

B

Background Checks

Peter T. Higgins
Higgins & Associates, International (HAI),
Washington, DC, USA

Synonyms

Credit check; Criminal history check; Criminal record search; Disclosure check; Personal information search; Preemployment screening; Vetting

Definitions

There are multiple types of background checks that all involve reviewing past, recorded behavior:

1. **Job Applicants:** When people apply for a position of trust (e.g., a school teacher, a lawyer, or a bank teller), a background check is part of the way of determining if the applicant is suitable – a positive result. These are known as applicant or civil background checks. In the USA:
 1. If there is a state or federal law requiring a national check, then applicant fingerprints (with minimal supporting biographic information) can be submitted to the Federal Bureau of Investigation (FBI) for a search.
 2. If the applicants are seeking federal employment, then their biographic data and fingerprints can be submitted to the FBI for a search.
 3. If the applicants are applying for a job not covered by a state or federal law, they are restricted to commercial background checking services – companies that have aggregated financial, court, motor vehicle, and other records.
2. **Applicants for Credit:** When people apply for credit cards or a large financial commitment (e.g., a mortgage), a background check is part of the way of determining if the applicant is suitable – a positive result. These are known as credit checks and are performed by commercial background checking services.
3. **Applicants for Government Benefits:** When people apply for a visa, passport, driver's license, Social Security, and other benefits, governments use varying levels of background checks to weed out fraud (e.g., multiple applications with different identities but for the same subject), previously denied persons, etc. Other than possible checks for visas, most of these checks say nothing about the suitability of a person for trustworthiness.
4. **Criminals:** In the criminal justice, community background checks are used when a person is arrested to determine if an arrestee already has a criminal record that they are hiding – a negative result that will be used in setting bail, sentencing, etc. In the USA.

5. Arrestee fingerprints (with minimal supporting biographic information) can be submitted to the FBI for a search.

Background checks are primarily based on textual information (e.g., name and date of birth) searches of bank, court, credit card issuer, and other files or textual searches and in some cases are combined with biometric-based (e.g., fingerprint) searches of criminal or undesirable persons (e.g., persons previously deported) records.

The ANSI/IAI 2-1988 American National Standard for Forensic Identification Glossary of Terms and Acronyms defines “criminal history check” as *A search of name indices and/or fingerprint files to determine whether or not a subject has a prior criminal record.*

The same American National Standard glossary defines “criminal history” as *A chronological summary of an individual’s criminal activity which may include the dates of the activity, the individual’s name, aliases and other personal descriptors, the identities of the reporting agencies, the arrest charges, dispositions, etc.*

The UK Criminal Records Bureau performs an Enhanced Disclosure Check (the same check as the standard disclosure but with a local police record check) to establish criminal backgrounds.

A credit check is an automated credit record search conducted through various major credit bureaus.

Introduction

Background checks became important to law enforcement about the time that large numbers of people started moving to cities as a by-product of the Industrial Revolution. Prior to that, few people ever ventured far from their birthplace – a place where they were known and their history was known. The need to link people to their criminal histories drove police forces in London, Paris, and Buenos Aires to examine identification methodologies such as fingerprint recognition and anthropometry in the late 1800s – the surviving approaches are now classified as members of the science called biometrics. Simon

Cole’s 2001 book provides a good history of criminal identification [1].

In the post-World War II era, international travel became far more common than before the war. A parallel can be drawn with the movement during the Industrial Age within countries – now criminals and terrorists were freely crossing borders – hoping to leave their criminal/terrorist records behind. Even if the world’s police records were all suddenly accessible over the Internet, they would not all be in the same character set. While many are in the Roman alphabet, others are in Cyrillic, Chinese characters, etc., this poses a problem for text search engines and investigators. Fortunately biometric samples are insensitive to the nationality or country of origin of a person. Thus, a search can be theoretically performed across the world using fingerprints or other enrolled biometric modalities. Unfortunately the connectivity of systems does not support such searches other than on a limited basis – through Interpol. If the capability to search globally were there, the responses would still be textual and not necessarily directly useful to the requestor. One response to the challenge of international travel has been that nations collect biometric samples, such as the United Arab Emirates does with iris recognition, overview, at their points of entry to determine if a person previously deported or turned down for a visa is attempting to reenter the country illegally.

A wide variety of positions of trust in both the public and private sectors require verification of suitability either as a matter of law or corporate policy. A person is considered suitable if the search for background impediments is negative. A position of trust can range from a police officer or teacher to a new corporate employee who will have access to proprietary information and possibly a business’s monetary assets or to an applicant for a large loan or mortgage. Certain classes of jobs are covered by federal and state/provincial laws such as members of the military and school teachers/staff.

A background check is the process of finding information about someone which may not be readily available. The most common way of conducting a background check is to look up

official and commercial records about a person. The need for a background check commonly arose when someone had to be hired for high-trust jobs such as security or in banking. Background checks while providing informed and less-subjective evaluations, however, also brought along their own risks and uncertainties.

Background checks require the “checking” party to collect as much information about the subject of the background check as is reasonably possible at the beginning of the process. Usually the subject completes a personal history form, and some official document (e.g., a driver’s license) is presented and photocopied. The information is used to increase the likelihood of narrowing the search to include the subject, but not too many others, with the same name or other attributes such as the same date and place of birth.

These searches are typically based on not only an individual’s name but also on other personal identifiers such as nationality, gender, place and date of birth, race, street address, driver’s license number, telephone number, and Social Security number. Without knowing where a subject really has lived, it is very hard for an investigation to be successful without broad access to nationally aggregated records. There are companies that collect and aggregate these records as a commercial venture.

It is important to understand that short of some biometric sample (e.g., fingerprints) the collected information is not necessarily unique to a particular individual. It is well known that name checks, even with additional facts such as height, weight, and DOB, can have varying degrees of accuracy because of identical or similar names and other identifiers. Reduced accuracy also results from clerical errors such as misspellings or deliberately inaccurate information provided by search subjects trying to avoid being linked to any prior criminal record or poor financial history.

In the USA, much of the required background information to be searched is publicly available but not necessarily available in a centralized location. Privacy laws limit access in some jurisdictions. Typically all arrest records, other than for juveniles, are public records at the police and courthouse level. When aggregated at the state

level, some states protect them while others sell access to these records. Other relevant records such as sex offender registries are posted on the Internet.

For more secure positions in the USA, background checks include a “National Agency Check.” These checks were first established in the 1950s and include a name-based search of FBI criminal, investigative, administrative, personnel, and general files. The FBI has a National Name Check Program that supports these checks. The FBI website [2] provides a good synopsis of the program:

- *Mission:* The National Name Check Program’s (NNCP’s) mission is to disseminate information from FBI files in response to name check requests received from federal agencies including internal offices within the FBI; components within the legislative, judicial, and executive branches of the federal government; foreign police and intelligence agencies; and state and local law enforcement agencies within the criminal justice system.
- *Purpose:* The NNCP has its genesis in Executive Order 10450, issued during the Eisenhower Administration. This executive order addresses personnel security issues and mandated National Agency Checks (NACs) as part of the preemployment vetting and background investigation process. The FBI is a primary NAC conducted on all US government employees. Since 11 September, name check requests have grown, with more and more customers seeking background information from FBI files on individuals before bestowing a privilege – whether that privilege is government employment or an appointment, a security clearance, attendance at a White House function, a green card or naturalization, admission to the bar, or a visa for the privilege of visiting our homeland. . . .
- *Function:* The employees of the NNCP review and analyze potential identifiable documents to determine whether a specific individual has been the subject of or has been mentioned in any FBI investigation(s) and if so, what (if any) relevant information may be disseminated to the requesting agency. It is important

to note that the FBI does not adjudicate the final outcome; it just reports the results to the requesting agency.

- *Major Contributing Agencies:* The FBI's NNCP Section provides services to more than 70 federal, state, and local governments and entities... The following are the major contributing agencies to the NNCP:
 - US Citizenship and Immigration Services – Submits name check requests on individuals applying for the following benefits: asylum, adjustment of status to legal permanent resident, naturalization, and waivers.
 - Office of Personnel Management – Submits name check requests in order to determine an individual's suitability and eligibility in seeking employment with the federal government.
 - Department of State – Submits FBI name check requests on individuals applying for visas... [2].

In the US government background checking process, a credit check *is included in most background investigations except the basic NACI investigation required of employees entering Non-Sensitive (Level 1) positions* [3].

Background checks were once done by the province of governments. Now commercial companies provide these services to the public, industry, and even to governments. These commercial checks rely on purchased, copied, and voluntarily submitted data from second and third parties. There are many commercial companies that accumulate files of financial, criminal, real estate, motor vehicle, travel, and other transactions. The larger companies spend substantial amounts of money collecting, collating, analyzing, and selling this information.

At the entry level, customers of these aggregators include persons “checking out” their potential roommates, baby sitters, etc. At the mid-level employers use these services to pre-screen employees. At the high end, the data is mined to target individuals for commercial and security purposes based on their background (e.g., financial and travel records). The profiling of persons based on background information is

disturbing in that the files are not necessarily accurate and rarely have biometric identifiers to identify people positively. For an example of the problem, there is no need to look further than the news stories about post 9–11 name-based screening that kept Senator Kennedy on the no-fly list because he shared a name with a suspected person – and that was a government maintained file.

Historically the challenge in background checking has been (1) when people usurp another person's identity that “checks out” as excellent, (2) when people make up an identity and it is only checked for negative records not for its basic veracity, and (3) when persons try to hide their past or create a new past using multiple identities to gain benefits or privileges they might otherwise not be entitled to receive. A second identity could be created by simply changing their date and place of birth; of course it would not have much “depth” in that a simple check would reveal no credit history, no driver's license, etc., yet for some applicants checking is only to determine if the claimed identity has a negative history or not – not to see if the person really exists. All of these challenges render many name or number-based (e.g., Social Security number) background checks ineffective.

Several countries, states, and provinces are undertaking one relatively simple solution to stolen identities. As more and more records become digital, governments can link birth and death records – so a person cannot claim to be a person who died at a very early age and thus having no chance of a negative record. People were able to use these stolen identities as seeds for a full set of identification documents. Governments and financial institutions are also requiring simple proof of documented residence such as mail delivered to an applicant from a commercial establishment to the claimed address and a pay slip from an employer. Denying people easy ways to shift identities is a critical step in making background checks more reliable.

The most successful way to deal with these challenges has been to link persons with their positive (e.g., driver's license with a clean record) and negative histories (e.g., arrest cycles) biometrically. The primary systems where this linkage

is being done are in the provision of government services (motor vehicle administration and benefits management) and the criminal justice information arena (arrest records and court dispositions). Currently, few if any financial records are linked to biometric identifiers, and the major information aggregators do not yet have biometric engines searching through the millions of records they aggregate weekly. The real reason they have not yet invested in this technology stems primarily from the almost total lack of access to biometric records other than facial images. This provides some degree of privacy for individuals while forcing credit bureaus to rely on linked textual data such as a name and phone number, billed to the same address as on file with records from a telephone company, with an employment record.

The inadequacy of name-based checks was re-documented in FBI testimony in 2003, regarding checking names of persons applying for visas to visit the USA. *Approximately 85 % of name checks are electronically returned as having “No Record” within 72 hours. A “No Record” indicates that the FBI’s Central Records System contains no identifiable information regarding this individual. . .*” This response does not ensure that the applicants are using their true identity but only that the claimed identity was searched against text-based FBI records – without any negative results.

The FBI also maintains a centralized index of criminal arrests, convictions, and other dispositions. The data is primarily submitted voluntarily by the states and owned by the states – thus limiting its use and dissemination. The majority of the 100 million plus indexed files are linked to specific individuals through fingerprints. The following information about the system is from a Department of Justice document available on the Internet [4].

This system is an automated index maintained by the FBI which includes names and personal identification information relating to individuals who have been arrested or indicted for a serious or significant criminal offense anywhere in the country. The index is available to law enforcement and criminal justice agencies through-

out the country and enables them to determine very quickly whether particular persons may have prior criminal records and, if so, to obtain the records from the state or federal databases where they are maintained. Three name checks may be made for criminal justice purposes, such as police investigations, prosecutor decisions, and judicial sentencing. In addition, three requests may be made for authorized noncriminal justice purposes, such as public employment, occupational licensing, and the issuance of security clearances, where positive fingerprint identification of subjects has been made.

Name check errors are of two general types: (1) inaccurate or wrong identifications, often called “false positives,” which occur when all three name checks of an applicant do not clear (i.e., it produces one or more possible candidates) and the applicant’s fingerprint search does clear (i.e., applicant has no FBI criminal record) and (2) missed identifications, often called “false negatives,” which occur when the three name checks of an applicant clear (i.e., produces no possible candidates) and the applicant’s fingerprint search does not clear (i.e., applicant has an FBI criminal record). Although errors of both types are thought to occur with significant frequency – based on the experience of state record repository and FBI personnel – at the time when this study was begun, there were no known studies or analyses documenting the frequency of such errors.

In contrast, fingerprint searches are based on a biometric method of identification. The fingerprint patterns of individuals are unique characteristics that are not subject to alteration. Identifications based on fingerprints are highly accurate, particularly those produced by automated fingerprint identification system (AFIS) equipment, which is in widespread and increasing use throughout the country. Analyses have shown that AFIS search results are 94–98 % accurate when searching good quality fingerprints.

Because of the inaccuracies of name checks as compared to fingerprint searches, the FBI and some of the state criminal record repositories do not permit name check access to their criminal history record databases for noncriminal justice purposes.

Where Do Biometrics Fit In?

When executing a background check, there are several possible ways that biometric data can be employed. As seen governments can collect large samples (e.g., all ten fingers) to search large criminal history repositories. The large sample is required to ensure the search is cost effective and accurate. The time to collect all these fingerprints and extract the features can be measured in minutes, possibly more than ten, while the search time must be measured in seconds to deal with the national workloads at the central site.

Other programs such as driver's license applicant background checks are sometimes run using a single facial image. These are smaller files than fingerprints, collected faster using less costly technology but have somewhat lower accuracy levels, thus requiring more adjudication by the motor vehicle administrators.

As companies (e.g., credit card issuers) start to employ biometrics for convenience or brand loyalty, they are very likely to use the biometrics not just for identity verification at the point of sale but to weed out applicants already "blacklisted" by the issuer. These biometric samples will need to be of sufficient density to permit identification searches and yet have a subset that is "lightweight" enough to be used for verification in less than a second at a point of sale.

Temporal Value of Background Checks

In the USA, under the best conditions, a vetted person will have "passed a background check" to include an FBI fingerprint search, an NAC, a financial audit, personal interviews, and door-to-door field investigation to verify claimed personal history and to uncover any concerns local police and neighbors might have had. This is how the FBI and other special US agencies and departments check their applicants. Unfortunately, this is not sufficient. Robert Hanssen, special agent of the FBI, was arrested and charged with treason in 2001 after 15 years of undetected treason and over 20 years of vetted employment.

Even more disturbing is a 2007 case where Nada Nadim Prouty pleaded guilty to numerous federal charges including unlawfully searching the FBI's Automated Case Support computer system. Ms. Prouty was hired by the FBI in 1999 and underwent a full background check that included fingerprints. In 2003 she changed employers, joining the CIA where she underwent some level of background check. Neither of these checks nor earlier checks by the then INS disclosed her having paid an unemployed American to marry her to gain citizenship.

Without being caught, criminals have the same clean record as everyone else, with or without biometrics being used in a background check. While FBI agent's fingerprints are kept in the FBI's AFIS system, those of school teachers and street cops are not. This means if any of them were arrested, only the FBI's employees' fingerprints would lead to notification of the subject's employer. RAP (allegedly short for Record of Arrests and Prosecutions) sheets are normally provided in response to fingerprint searches. A relatively new process called Rap-Back permits agencies requesting a background check to enroll the fingerprints such that if there is a subsequent arrest, the employer will be notified. Rap-Back and routine reinvestigations address part of the temporal problem, but in the end there is no guarantee that a clean record is not a misleading sign – just an indicator of no arrests, which is not always a sign of trustworthiness.

Privacy Aspects

Performing a complete and accurate background check can cause a conflict with widely supported privacy laws and practices. The conflicts come from most "privacy rights" laws being written to inhibit certain government actions not to uniformly limit commercial aggregation and sharing of even questionable data on a background-data-for-fee basis.

Robert O'Harrow's book [5] points out two serious flaws on the privacy side of the commercial background check process.

- “Most employees who steal do not end up in public criminal records. Dishonest employees have learned to experience little or no consequences for their actions, especially in light of the current tight labor market,” ChoicePoint tells interested retailers. “A low-cost program is needed so companies can afford to screen all new employees against a national theft database.” The database works as a sort of blacklist of people who have been accused or convicted of shoplifting [5].
- Among other things the law restricted the government from building databases of dossiers unless the information about individuals was directly relevant to an agency’s mission. Of course, that’s precisely what ChoicePoint, LexisNexis, and other services do for the government. By outsourcing the collection of record, the government doesn’t have to ensure the data is accurate or have any provisions to correct it in the same way it would under the Privacy Act [5].

These companies have substantially more information on Americans than the government. O’Harrow reports that ChoicePoint has data holdings of an unthinkable size:

- Almost a billion records added from TransUnion twice a year
- Updated phone records (numbers and payment histories) from phone companies – for over 130 million persons
- A Comprehensive Loss Underwriting Exchange with over 200 million claims recorded
- About 100 million criminal records
- Copies of 17 billion public records (such as home sales and bankruptcy records)

The United Nations International Labor Organization (ILO) in 1988 described “*indirect discrimination as occurring when an apparently neutral condition, required of everyone, has a disproportionately harsh impact on a person with an attribute such as a criminal record.*” [6] Thus, pointing out the danger of cases where criminal records “*include charges which were not proven, investigations, findings of guilt with non-conviction and convictions which were later quashed or pardoned. It also includes imputed*

criminal record. For example, if a person is denied a job because the employer thinks that they have a criminal record, even if this is not the case [7].”

This problem is recognized by the Australian government, which quotes the above ILO words in its handbook for employees. The handbook goes on to say, *The CRB “recognises that the Standard and Enhanced Disclosure information can be extremely sensitive and personal, therefore it has published a Code of Practice and employers’ guidance for recipients of Disclosures to ensure they are handled fairly and used properly”* [8].

Applications

Background checks are used for preemployment screening, establishment of credit, for issuance of visas, as part of arrest processes, in sentencing decisions, and in granting clearances. When a biometric check is included, such as a fingerprint-based criminal records search, there can be a higher degree of confidence in the completeness and accuracy of that portion of the search.

Seemingly secure identification documents such as biometric passports do not imply a background check of the suitability of the bearer – but only that the person it was issued to is a citizen of the issuing country. These documents permit positive matching of the bearer to the person the document was issued to – identity establishment and subsequent verification of the bearer.

It is unfortunately easy to confuse the two concepts: a clean background and an established identity. The US government’s new personal identity verification (PIV) card, on the other hand, implies both a positive background check and identity establishment. The positive background check is performed through a fingerprint-based records search. The identity is established when a facial image, name, and other identity attributes are locked to a set of fingerprints. The fingerprints are then digitally encoded and loaded on the PIV smart card,

permitting verification of the bearer's enrolled identity at a later date, time, and place.

Summary

Background checks are a necessary but flawed part of the modern world. Their importance has increased substantially since the terrorist attacks on 9/11 in the USA, 11-M in Spain, and 7/7 in London. Governments use them within privacy bounds set by legislatures but seem to cross into a less constrained world when they use commercial aggregators. Industry uses them in innumerable process – often with little recourse by impacted customers, employees, and applicants. Legislators are addressing this issue but technology is making the challenge more ubiquitous and at an accelerating rate.

Biometric attributes linked to records reduce the likelihood of them being incorrectly linked to a wrong subject. This is a promise that biometrics offers us – yet the possible dangers in compromised biometric records or systems containing biometric identifiers must be kept in mind.

Related Entries

- ▶ [Biometric Verification/Identification/Authentication/Recognition: The Terminology](#)
- ▶ [Fingerprint Matching, Automatic](#)
- ▶ [Fingerprint Recognition, Overview](#)
- ▶ [Fraud Reduction, Applications](#)
- ▶ [Fraud Reduction, Overview](#)
- ▶ [Iris Recognition at Airports and Border Crossings](#)
- ▶ [Law Enforcement](#)

References

1. S.A. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Harvard University Press, Cambridge, 2001). ISBN 0-6740-1002-7
2. <http://www.fbi.gov/hq/nationalnamecheck.htm>
3. *HHS Personnel Security/Suitability Handbook; SDD/ASMB 1/98*. U.S. Department of Health & Human Services

4. <http://www.ojp.usdoj.gov/bjs/pub/pdf/iince.pdf>
5. R. O'Harrow Jr., *No Place To Hide* (Free Press, New York, 2005), pp. 131, 137. ISBN 0-7432-5480-5
6. Committee of Experts on the Application of Conventions and Recommendations ILO, General survey of equality in employment and occupation, in *International Labour Conference*, Geneva (1988)
7. On the Record; Guidelines for the Prevention of Discrimination in Employment on the Basis of Criminal Record; November 2005; Minor Revision September 2007; Australian Human Rights and Equal Opportunity Commission
8. <http://www.crb.gov.uk/Default.aspx?page=310>

Back-of-Hand Vascular Recognition

Alex Hwansoo Choi

Techsphere Co., Ltd., Seoul, South Korea

Synonyms

Back-of-hand vascular pattern recognition; Hand vein identification; Hand vascular recognition; Hand vein verification

Definition

The back-of-hand vascular recognition is the process of verifying the identity of individuals based on their subcutaneous vascular network on the back of the hand. According to large-scale experiments, the pattern of blood vessels is unique to each individual, even among identical twins; thereby the pattern of the hand blood vessels on the back of the hand can be used as distinctive features for verifying the identity of individuals. A simple back-of-hand vascular recognition system is operated by using near-infrared light to illuminate on the back of the hand. The deoxidized hemoglobin in blood vessels absorbs more infrared rays than the surrounding tissues and causes the blood vessels to appear as black patterns in the resulting image captured by a camera, sensitive to near-infrared illumination. The image of back-of-hand vascular patterns is then preprocessed and compared

with the previously recorded vascular pattern templates in the database to verify the identity of the individual.

Introduction

Biometric recognition is considered as one of the most advanced security method for many security applications. Several biometric technologies such as fingerprint, face, and hand geometry have been researched and developed in recent years [1]. Compared with traditional security methods such as pass codes, passwords, or smart cards, the biometric security schemes show many priority features such as high level security and user convenience. Therefore, biometric recognition systems are being widely deployed in many different applications.

The back-of-hand vascular pattern is a relatively new biometric feature containing complex and stable blood vessel network that can be used to discriminate a person from the other. The back-of-hand vascular pattern technology began to be considered as a potential biometric technology in the security field in early 1990s. During this period, the technology became one of the most interesting topics in biometric research community that received significant attention. One of the first paper to bring this technology into discussion was published by Cross and Smith in 1995 [2]. The paper introduced the thermographic imaging technology for acquiring the subcutaneous vascular network of the back of the hand for biometric application. However, the thermographic imaging technology is strongly affected by temperature from external environment; therefore, it is not suitable to apply this technology to general outdoor applications.

The use of back-of-hand vascular recognition in general applications became possible when new imaging techniques using near-infrared illumination and low-cost camera have been invented [3]. Instead of using far-infrared light and thermographic imaging technology, this technology utilizes the near-infrared light to illuminate the back of the hand. Due to the difference in absorption rate of infrared radiation, the blood

vessels would appear as black patterns in the resulting image. The cameras to photograph the back-of-hand vascular pattern image can be any low-cost cameras that are sensitive to the range of near-infrared light.

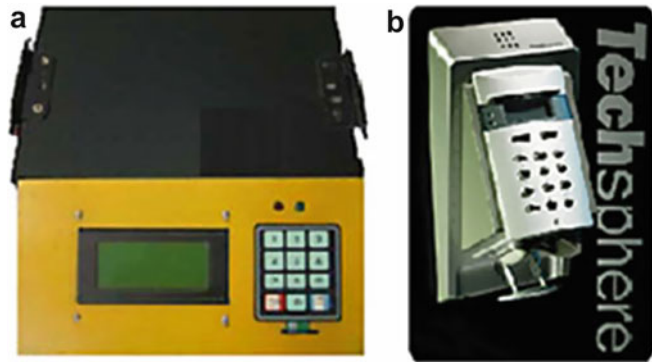
Although the back-of-hand vascular pattern technology is still an ongoing area of biometric research, it has become a promising identification technology in biometric applications. A large number of units deployed in many security applications such as information access control, homeland security, and computer security provide evidence to the rapid growth of the back-of-hand vascular pattern technology. Compared to the other existing biometric technologies, back-of-hand vascular pattern technology has many advantages such as higher authentication accuracy and better usability. Thereby, it is suitable for the applications in which high level of security is required. Moreover, since the back-of-hand vascular patterns lies underneath the skin, it is extremely difficult to spoof or steal. In addition, lying under skin surface, back-of-hand vascular pattern remains unaffected by inferior environments. Therefore, the back-of-hand vascular pattern technology can be used in various inferior environments such as factories, army, and construction sites where other biometric technologies have many limitations. Because of these advanced features, the back-of-hand vascular pattern technology is used in public places.

Development History of the Back-of-Hand Vascular Recognition

As a new biometric technology, back-of-hand vascular pattern recognition began to receive the attention from biometric community from 1990s. However, the launch of the back-of-hand vascular recognition system into the market was first considered from 1997. The product model named BK-100 was announced by BK Systems in Korea. This product was sold mainly in the local and Japanese market. In the early stage of introduction, the product had limitations for physical access control applications. More than 200 units have been installed in many access

Back-of-Hand Vascular Recognition, Fig. 1

Prototype of hand vascular recognition system; (a) BK-100 and (b) VP-II product



control points with time and attendance systems in both Korea and Japan. Figure 1a shows a prototype of the BK-100 hand vascular recognition system.

The first patent on the use of the back-of-hand vascular pattern technology for personal identification was published in 1998 and detailed in reference [4]. The invention described and claimed an apparatus and method for identifying individuals through their subcutaneous hand vascular patterns. Consecutively, other subsequent commercial versions, BK-200 and BK-300, have been launched in the market. During the short period of time from the first introduction, these products have been deployed in many physical access control applications.

The technology of back-of-hand vascular pattern recognition was continuously enhanced and developed by many organizations and research groups [5–11]. However, one of the organizations that made promising contributions to the development of the back-of-hand recognition technology is Techsphere Co., Ltd. in Korea. As the results from these efforts, a new commercial product under the name VP-II has been released. Many advanced digital processing technologies have been applied to this product to make it a reliable and cost-effective device. With the introduction of the new product, the scanner became more compact to make the product suitable to be integrated in various applications. The product also provided better user interface to satisfy user-friendly requirements and make the system highly configurable. Figure 1b shows a prototype of the VP-II product.

Various organizations and research groups are spending efforts to develop and enhance the back-of-hand vascular pattern technology. Thousands of back-of-hand products have been rapidly installed and successfully used in various applications. Researches and product enhancements are being conducted to bring more improvements to products. Widespread international attention from biometric community will make the back-of-hand vascular pattern technology as one of the most promising technologies in security field.

Underlying Technology of Back-of-Hand Vascular Recognition

To understand the underlying technology of the back-of-hand vascular recognition, the operation of a typical back-of-hand vascular recognition system should be considered. Similar to other biometric recognition system, the back-of-hand vascular recognition system often composes of different modules including image acquisition, feature extraction, and pattern matching. Figure 2 shows a typical operation of the back-of-hand vascular recognition system.

Image Acquisition

Since the back-of-hand vascular pattern lies underneath the skin, it cannot be seen by the human eye. Therefore, it cannot use the visible light that occupies a very narrow band (approx. 400–700 nm wavelength) for photographing the back-of-hand vascular patterns. The back-of-hand vascular pattern image can be captured under

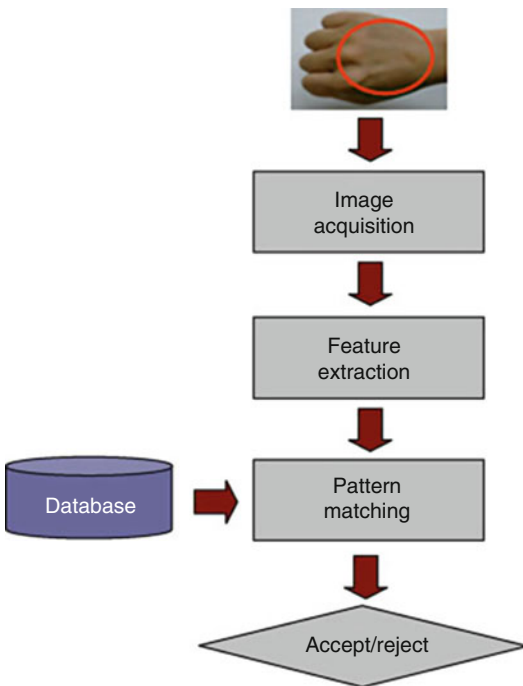
the near-infrared light (approx. 800–1,000 nm wavelength). The near-infrared light can penetrate into the human tissues to approximately 3 mm depth [10]. The blood vessels absorb more infrared radiation than the surrounding tissues and appear as black patterns in the resulting image. The camera used to capture the image of back-of-hand vascular pattern can be any low-cost camera that is sensitive to the range of near-infrared light. Figure 3 shows an example of images obtained by visible light and near-infrared light [12].

Pattern Extraction

One of the important issues in the back-of-hand vascular recognition is to extract the back-of-hand vascular pattern that can be used to distinguish an individual from the others. Pattern extraction module is to accurately extract the back-of-hand vascular patterns from raw images which may contain the undesired noises and other irregular effects. The performance of the back-of-hand vascular recognition system strongly depends on the effectiveness of the pattern extraction module. Therefore, the pattern extraction module often consists of various advanced image processing algorithms to remove the noises and irregular effects, enhance the clarity of vascular patterns, and separate the vascular patterns from the background. The final vascular patterns obtained by the pattern extraction algorithm are represented as binary images. Figure 4 shows the procedure of a typical feature extraction algorithm for extracting back-of-hand vascular patterns from raw images. After the pattern extraction process, there still could be salt-and-pepper-type noises. Thus, noise removal filters such as medial filters may be applied as a post-processing step.

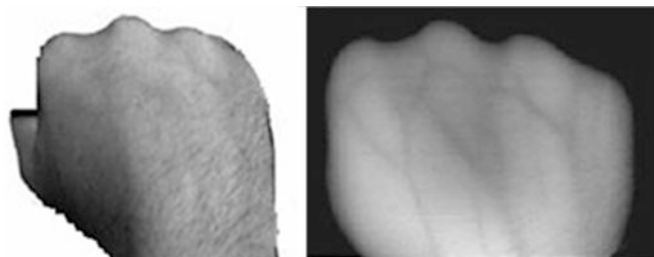
Pattern Matching

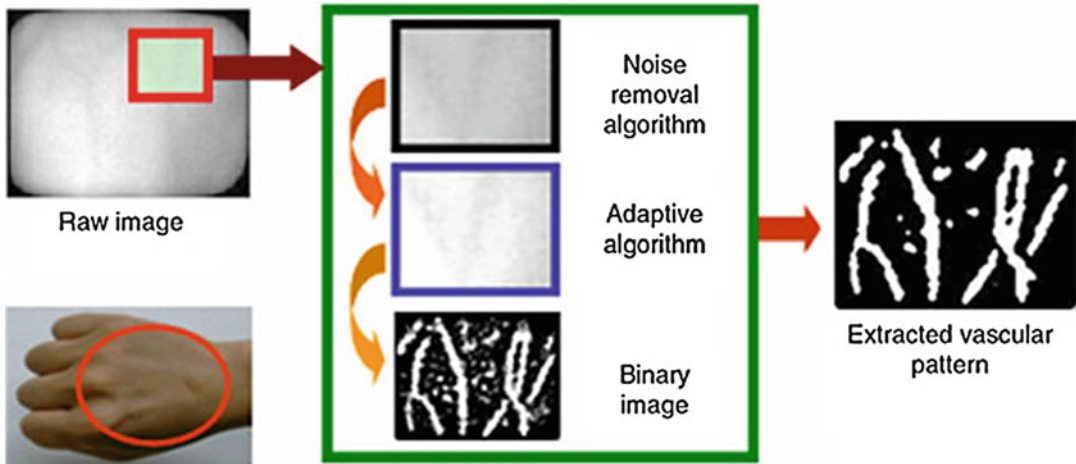
The operation of a back-of-hand vascular recognition system is based on comparing the back-of-hand vascular pattern of a user being authenticated against preregistered back-of-hand patterns stored in the database. The comparison step is often performed by using different type of pattern matching algorithms to generate a matching score. The structured matching algorithm is utilized if the vascular patterns are represented by collections of some feature



Back-of-Hand Vascular Recognition, Fig. 2 Operation of a typical back-of-hand vascular recognition system

Back-of-Hand Vascular Recognition, Fig. 3 The back-of-hand images obtained by visible light (left) and by infrared light (right)





Back-of-Hand Vascular Recognition, Fig. 4 The flow chart of a typical feature extraction algorithm

points such as line endings and bifurcations [13]. If the vascular patterns are represented by binary images, the template matching algorithm is also utilized [14]. The matching score is then used to compare with the predefined system threshold value to decide whether the user can be authenticated. For more specific performance figures for each algorithm, readers are referred to [4–7].

Applications of Back-of-Hand Vascular Recognition

The ability to verify identity of individuals has become increasingly important in many areas of modern life, such as electronic governance, medical administration systems, access control systems for secured areas, and passenger ticketing, etc. With many advanced features such as high level of security, excellent usability, and difficulty in spoofing, the back-of-hand vascular recognition systems have been deployed in a wide range of practical applications. The practical applications of the back-of-hand vascular recognition systems can be summarized as following:

Office Access Control and Time Attendance: The wide use of back-of-hand vascular recognition technology is physical access control and

identity management for time and attendance. The recognition systems utilizing the back-of-hand vascular technology are often installed to restrict the access of unauthorized people. The integrated applications with back-of-hand vascular recognition systems will automatically record the time of entering and leaving the office for each employee. Furthermore, the time and attendance record for each employee can be automatically fed to the resource management program of the organization. This provides a very effective and efficient way to manage the attendance and overtime payment at large-scale organizations.

Port Access Control: Due to the overwhelming security climate in recent years and fear of terrorism, there has been a surge in demand for accurate biometric authentication methods to establish a security fence in many ports. Airports and seaports are the key areas through which terrorists may infiltrate. Due to its high accuracy and usability, fast recognition speed, and user convenience, the back-of-hand vascular recognition systems are being employed for access control in many seaports and airports. For example, back-of-hand vascular recognition systems are being used in many places at Incheon International Airport and many airports in Japan [14]. In addition, major Canadian seaports (Vancouver and Halifax) are fully access-controlled by back-of-hand systems.

Factories and Construction Sites: Unlike other biometric features which can be easily affected by dirt or oil, the back-of-hand vascular patterns are not easily disturbed because the features lie under the skin of human body. Therefore, the back-of-hand vascular pattern technology is well accepted in applications exposed to inferior environments such as factories or construction sites. The strengths and benefits of the back-of-hand vascular pattern technology become more obvious when it is used in these applications because other existing biometric technologies show relatively low usability and many limitations when used in inferior environments.

Summary

The back-of-hand vascular pattern technology has been researched and developed in the recent decades. In a relatively short period, it has gained considerable attention from biometric community. The rapidly growing interest in the back-of-hand vascular pattern technology is confirmed by the large number of research attempts which have been conducted to improve the technology in recent years. Although the back-of-hand vascular pattern has provided a higher accuracy and better usability in comparison with other existing biometric technologies, more research need to be performed to make it more robust and tolerant technology in various production conditions. The future research should focus on development of higher-quality image capture devices, advanced feature extraction algorithms, and more reliable pattern matching algorithms to resolve pattern distortion issue.

Related Entries

- ▶ [Finger Vein](#)
- ▶ [Finger Vein Biometric Algorithm](#)
- ▶ [Finger Vein Pattern Imaging](#)
- ▶ [Finger Vein Reader](#)
- ▶ [Palm Vein Image Sensor](#)
- ▶ [Palm Vein](#)

References

1. A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric. *IEEE Trans. Circ. Syst. Video Technol.* **14**(1), 4–20 (2004)
2. J.M. Cross, C.L. Smith, Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification, in *IEEE 29th Annual International Carnahan Conference on Security Technology*, Sanderstead, Surrey, 1995, pp. 20–35
3. S.K. Im, H.M. Park, Y.W. Kim, S.C. Han, S.W. Kim, C.H. Kang, Biometric identification system by extracting hand vein patterns. *J. Korean Phys. Soc.* **38**(3), 268–272 (2001)
4. H.S. Choi, B.K. Systems, Apparatus and method for identifying individuals through their subcutaneous vein patterns and integrated system using said apparatus and method. US Patent 6301375 (2001)
5. S.K. Im, H.S. Choi, S.W. Kim, Design for an application specific processor to implement a filter bank algorithm for hand vascular pattern verification. *J. Korean Phys. Soc.* **41**, 461–467 (2002)
6. S.K. Im, H.S. Choi, A filter bank algorithm for hand vascular pattern biometrics, in *Proceedings of ICCARV'02*, Singapore, 2002, pp. 776–781
7. S.K. Im, H.S. Choi, S.W. Kim, A direction-based vascular pattern extraction algorithm for hand vascular pattern verification. *ETRI J.* **25**(2), 101–108 (2003)
8. S.K. Im, H.M. Park, S.W. Kim, C.K. Chung, H.S. Choi, Improved vein pattern extracting algorithm and its implementation, in *International Conference on Consumer Electronics*, Los Angeles, June 2000, pp. 2–3
9. T. Tanaka, N. Kubo, Biometric authentication by hand vein patterns, in *SICE 2004*, Sapporo, vol. 1, Aug 2004, pp. 249–253
10. Y. Ding, D. Zhuang, K. Wang, A study of hand vein recognition method, in *Proceedings of the IEEE International Conference on Mechatronics & Automation*, Niagara Falls, July 2005, pp. 2106–2110
11. A.M. Badawi, Hand vein biometric verification prototype: a testing performance and patterns similarity, in *International Conference on Image Processing, Computer Vision, and Pattern Recognition*, Las Vegas, 2006, pp. 3–9
12. L. Wang, G. Leedham, Near- and far-infrared imaging for vein pattern biometrics, in *IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS'06)*, Sydney, 2006, pp. 52–59
13. A. Kumar, K.V. Prathyusha, Personal authentication using hand vein triangulation, in *Proceedings SPIE Conference on Biometric Technology for Human Identification*, Orlando, vol. 6944, Mar 2008, pp. 69440E-69440E-13
14. A.H. Choi, C.N. Tran, *Handbook of Biometrics: Hand Vascular Pattern Recognition Technology* (Springer, New York, 2008)

BioAPI, Standardization

Raul Sanchez-Reillo¹ and Matthias Niesing²

¹GUTI (University Group for Identification Technologies), University Carlos III of Madrid, Leganes, Madrid, Spain

²Secunet Security Networks AG, Essen, Germany

Synonyms

ISO/IEC 19784; ISO/IEC 19784-1

Definition

BioAPI is the abbreviation for Biometric Application Programming Interface (API). It is an API to develop biometric-related applications and was created by the BioAPI Consortium. In 2005, BioAPI was published as an international standard under ISO/IEC 19784-1:2005 [1]. From that publication it has evolved by adding new functionalities, being now under a revision to create the new BioAPI 3.0.

Origins and Basic Specification

The use of standardized Application Programming Interface (API) is demanded for allowing interoperability among developers and removing the cost for adapting the biometric solution to the evaluation protocol. In Biometrics, the reference API for developing biometric-related applications is BioAPI. BioAPI was originated by the BioAPI Consortium [2]. The BioAPI Consortium first announced its formation and intent to develop a biometric API standard in April of 1998. By the end of the year, this group had developed a multi-level API architecture and begun defining the associated components.

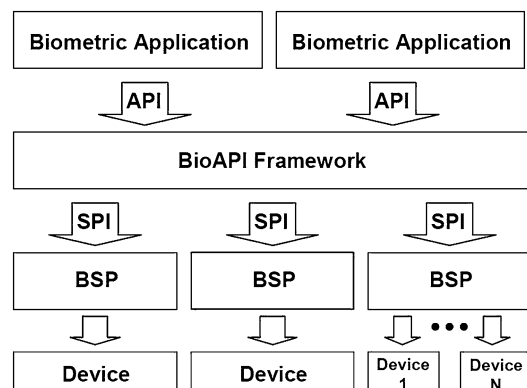
In March of 1999, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) and the US Biometric Consortium sponsored a unification meeting in

which the Human Authentication API (HA-API) working group (which had published a high level biometric API in 1997) agreed to merge their activities with the BioAPI Consortium. As part of this agreement, the BioAPI Consortium agreed to restructure their organization.

The reconstituted BioAPI Consortium completed its efforts to define the biometric API architecture and to solidify its organizational structure and operations by mid-1999. Version 1.0 of the Specification was released in March, 2000, and the Reference Implementation was released in September 2000. Version 1.1 of both the Specification and Reference Implementation were released in March 2001.

In February of 2002, BioAPI Version 1.1 was approved as an American National Standard through INCITS (ANSI/INCITS 358-2002). When ISO/IEC JTC1/SC37 was constituted, the US delegation offered that standard for adoption as an international standard through ISO/IEC, although it was decided that instead of adopting the standard directly, a new project would be started to improve the specification of BioAPI. This project led to the publication, in 2005, of the ISO/IEC 19784-1 standard [1], which is also known as BioAPI 2.0.

The basic idea of BioAPI is given in Fig. 1. It is based on a framework that serves as an interface between the application and those biometric units available. A biometric unit can be



BioAPI, Standardization, Fig. 1 BioAPI's API/SPI model [1]

understood as any element that can provide biometric-related services, such as capture devices, algorithms, or storage units. To communicate with any external application, the framework offers an API (set of functions) that works independently of the devices being developed. On the other hand, to communicate with the units, the framework offers another API (here called SPI), with all of the functions needed to access such units. Independent of the type of unit, they provide a component with the supported services to allow them to be accessed by the framework. Such a driver is called a Biometric Service Provider (BSP).

BSPs can have nearly any form. They can be related to just one physical device, more than one, or none (e.g., being an algorithm). Due to the functions provided by the SPI, BSPs can be dynamically loaded and unloaded from the framework. Any external application can use any of the BSPs loaded through the framework to allow any system complexity. Moreover, BSPs can communicate with the framework to access other loaded BSPs.

Having given this short introduction, a general idea on how BioAPI works could be perceived, but with the further improvements that came in the years following its publication, its implementation is far from being understood. Particularly it is difficult to understand not only how this idea can be implemented but also how could this be implemented without the need of a framework (i.e., it is called framework-free BioAPI). This entry presents an overview that tries to clarify the whole architecture, how this interacts with a Graphical User Interface (GUI), and the steps taken to implement a framework-free and a full-framework version of BioAPI. Future works in this area are outline.

BioAPI Architecture

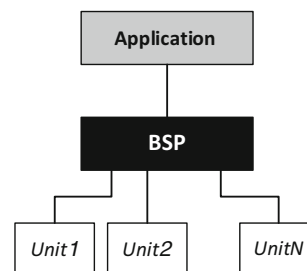
BioAPI is defined in a way that allows both structured development of applications and services, as well as interoperability between application and Biometric Service Providers (BSP) and among BSPs. In a few words, this API

has to allow the development of applications in a system based on a BioAPI Framework, as well as applications in a system where no framework is used (framework-free). Starting with the later, an application in a framework-free based system is developed using a BioAPI that allows the instantiation of a BSP, which is based on the instantiation of one or several BioAPI_Units. The BSP can host more than one BioAPI_Unit of each category, but when a session is attached, only up to a maximum of 1 BioAPI_Unit per category can be selected and, therefore, used.

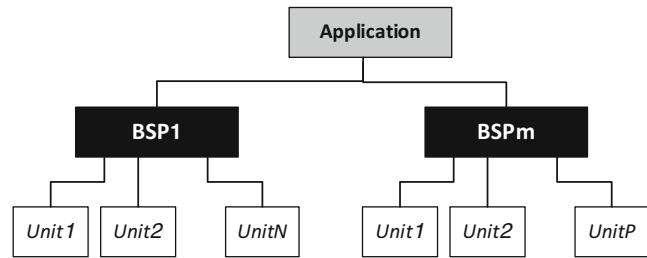
It is not allowed that the application access BioAPI_Units directly. Therefore this standard does not define a BioAPI_Unit interface, but only a hierarchical interface/class model that may ease the implementation of the BSP. The BSP shall inherit all public methods and data structures of the BioAPI_Units, and it is up to the implementation of the BSP developer to decide which of them are offered to the external world and which of them are only returning the lack of support of such method. This is represented in Fig. 2.

But a framework-free application may also be able to use several BSPs. Figure 3 represents how this can be implemented. As it can be seen, each BSP is used as a library to be used by the application. In such a case, if, for example, an application would like to use two different sensors and one processing and comparison BioAPI_Unit, then three BSPs can be used, one for each sensor and another for the Comparison and Processing BioAPI_Units.

Although the previous solution is fully valid, it may raise certain concerns in practical situations.



BioAPI, Standardization, Fig. 2 Framework-free application with a single BSP

BioAPI, Standardization,**Fig. 3** Framework-free application with multiple BSPs

The first concern is dealing with industry providing elements to be used in applications. It may happen that a provider is only providing sensors and would like to include support to all of its family of sensors as a single entity (e.g., a library). That provider may consider implementing that as a single BSP, but it may not be interested in providing monolithic methods (i.e., aggregated functionality such as Enrol, which performs in one single call the capture, the processing of the sample, the creation of the biometric reference, and even the archiving).

Therefore it will need to request these kinds of functions to be done at the application level, exchanging biometric information between the BSP and the application. Then, the application may forward that biometric data to another BSP to complete the action. So a possible solution for this inconvenience is to allow those sensors to directly interact with other BSPs, instead of using the application to do that. To achieve this, the biometric product provider may create an entity (e.g., a library) containing several BioAPI_Units of the same kind. This is called a Biometric Function Provider (BFP), which has mainly the following characteristics:

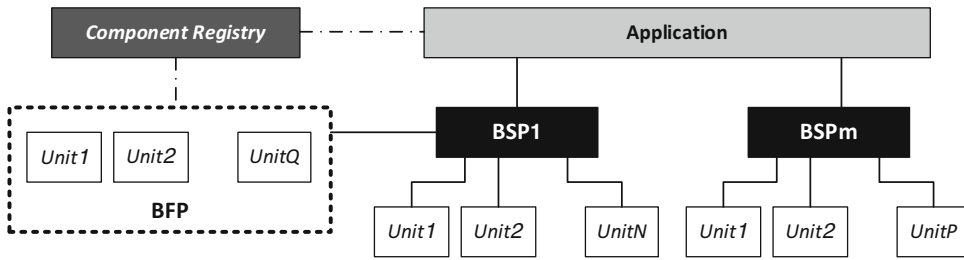
- The BFP shall only host BioAPI_Units of the same category.
- The BFP allows a BSP to be linked to one of its BioAPI_Units, in order to complete or adapt the functionality of the BSP.
- The BFP shall not provide functionality to the application, but only the link to the BSP. It is the BSP that provides functionality to the application.

The abovementioned situation also solves a problem from a developers' point of view, which deals with simplicity in developing

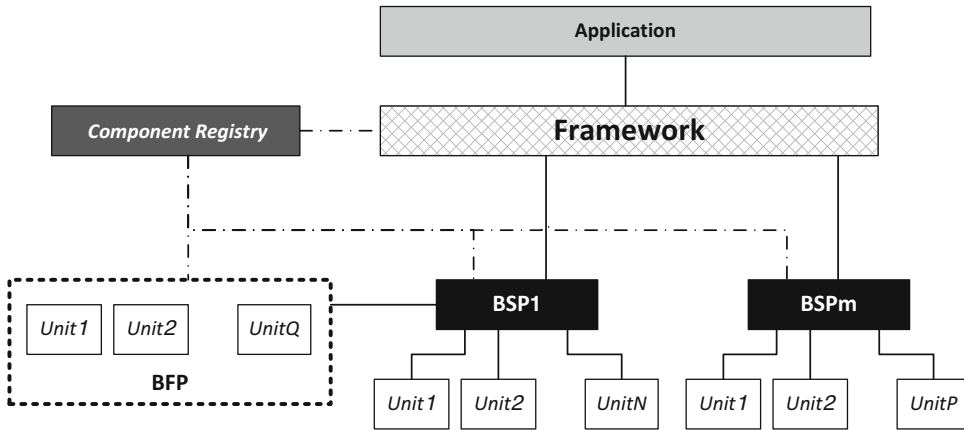
applications. If an application requires the use of BioAPI_Units from different providers (e.g., a sensor from one provider and processing, comparison, and archive BioAPI_Units from other provider), then it will have to load two different BSPs, calling each of the methods independently. As mentioned earlier, this has the inconvenience that it won't be possible to call a monolithic method, such as Verify(), which performs the data capture, the processing, extraction of the biometric reference from the database, the comparison, and taking the decision, all within the same single call. Therefore the application programmer will have to know which individual methods have to be called from each of the BSPs, in order to get the same functionality. By using a BSP that supports monolithic methods, and requesting the BSP to be linked to those BioAPI_Units for the BFPs of other product providers, once that link is established, the application can call those monolithic methods without taking into account that the functionality is provided by different vendors.

Last, but not least, there is a concern about security in certain operations. As biometric data is sensitive personal data, some clients may require that the biometric application won't directly access the user biometric data (i.e., the BIRs), avoiding the possibility of malware to tamper with such data. By using BFPs, all sensible data will be handled at the BSP level, and no Biometric Information Record (BIR) may be accessible to the application, not only simplifying the application development (by the use of monolithic methods) but also the security level achieved.

Figure 4 represents how a framework-free application is structured using BFPs.



BioAPI, Standardization, Fig. 4 Example of a framework-free application using BFPs



BioAPI, Standardization, Fig. 5 Generic structure of a framework-based application

The BFP is not accessed directly by the application. BioAPI calls are created to allow the application to know the BioAPI_Units that are contained in the BFPs so that the application may later request one BSP to attach one of those BioAPI_Units of the BFP.

All the above ideas are implemented in systems where the components to be used by the application (BSPs and BFPs) are known a priori, and only used by a single application (i.e., a static implementation of a biometric application, with the components chosen at time of compilation). But the same approach can be followed to allow the implementation of mechanisms for the dynamic selection of components to be used by the application, but with no a priori knowledge from the application developer. This is achieved by the inclusion of a common framework, which can be installed in the system where the application is expected to be running. In such a case, the application would request the framework the list of the BSPs and BFPs installed and select the BSPs

(with the requested attachment of BioAPI_Units from BFPs) to be instantiated dynamically by the framework. Then their methods and data structures would be accessed through the framework. The application would never be allowed to access the BSPs directly. This is depicted in Fig. 5.

In a framework-based system, BSPs may be accessed by several applications at the same time, and it may also happen that BioAPI_Units in the BFPs are also accessed by several BSPs at the same time. It is up to the implementation of the framework-based system as to how this is implemented (e.g., this may be done by queuing requests from the different sources or by responding to occurring events).

BioAPI Evolution and Adoption

From the basic specification given in ISO/IEC 19784-1:2005, additional specifications have been developed. This evolution includes different

parts of the ISO/IEC 19784 family of standards as specified in Biometric Technical Interface, Standardization. It includes further specifications on how to use the application Graphical User Interface (GUI), as well as providing further definition of the BFPs for each of the four categories of BioAPI_Units.

From the publication of version 1.1, BioAPI has been adopted by several companies for a variety of products. This can be seen in <http://www.bioapi.org/products.asp>. Since the publication of ISO/IEC 19784-1:2005, the adoption of BioAPI 2.0 has increased progressively, either by the development of brand-new BSPs and/or BFPs by major industrial players or by the adaptation of previous BioAPI 1.1 developments to a BioAPI 2.0 compliant version. The development of BioAPI versions in object oriented languages [3] is expected to help in the global adoption of this technology.

Summary

BioAPI is a comprehensive definition of an API for biometric-related applications, which can be adopted by any kind of application and under any kind of platform. Although defined in ANSI C language, there are also specifications in object-oriented languages, such as the specified family of standards ISO/IEC 30106 [3]. The basic specification is currently being revised as to build up a new 3.0 version that integrates all the evolutions that BioAPI has accomplished in the past years.

Related Entries

- ▶ [Biometric Technical Interface, Standardization](#)
- ▶ [Common Biometric Exchange Formats Framework Standardization](#)
- ▶ [Object-Oriented BioAPI Standard](#)

References

1. ISO/IEC JTC1/SC37, ISO/IEC 19784-1, Information technology – biometric application programming

interface – Part 1: BioAPI specification, 2005. Available at <http://www.iso.org/iso/home/store>. There is a revision in process (more information in <http://www.iso.org/iso/home/search.htm?qt=19784-1&sort=rel&type=simple&published=on>)

2. BioAPI Consortium webpage: <http://www.bioapi.org>
3. ISO/IEC JTC1/SC37, ISO/IEC 30106, Information technology – object oriented BioAPI. (Under development, more information in http://www.iso.org/iso/home/search.htm?qt=30106&published=on&active_tab=standards&sort_by=rel)

Biometric Algorithms

Yi Chen¹ and Jean-Christophe Fondeur²

¹Department of Computer Science and Engineering, Michigan State University, MI, USA

²Research & Technology, Morpho, Paris, France

Synonyms

Biometric Engines

Definition

Biometric algorithms are automated methods that enable a biometric system to recognize an individual by his or her anatomical/behavioral traits [1]. They consist of a sequence of automated operations performed by the system to verify or identify its ownership. These operations include quality assessment, enhancement, feature extraction, classification/indexing, matching and fusion, as well as compression algorithms, often used to reduce storage space and bandwidth.

Introduction

Biometric recognition is achieved by comparing the acquired biometric sample (the “query”) with one or more biometric samples that have been captured previously and stored in the system database (the “reference” or “gallery”).

The process of creating the database is called enrollment. The process of comparing samples is called verification if the query comes along with a claimed identity (in this case the “query” is compared to the biometric data of the claimed identity) or identification if no identity claim is made (in this case the “query” is compared to all the biometric data in the database).

The biometric sample is acquired by a biometric device and produces an electronic representation of high-dimensional signals (e.g., fingerprint or face images, signature dynamics) [2]. Most often, to avoid the “curse of dimensionality,” these high-dimensional signals are not directly compared; instead, a more compact representation of the signal – called “template” – is extracted from the raw signal and is used for the comparison. The various processes used to compare them are called biometric algorithms. These processes include assessing and enhancing the quality of the biometric signal, extracting and matching salient features, and information fusion at various stages. Compression and classification/indexing are also key components of biometric algorithms to optimize the resources needed (space and time).

Biometric techniques are effective to recognize people because the characteristics of biometric traits are distinct to each individual. In practice, however, variations (inherent in the biometric trait or how it is presented during acquisition) and noise, as well as intrinsic limitations of biometric sensing techniques can cause the accuracy of the system to drop significantly. It is necessary to develop biometric algorithms that are robust to these variations, namely, to extract salient and reproducible features from the input and to match these features efficiently and effectively with the templates in the database. Addressing all the problems requires the combination of various techniques to obtain the optimal robustness, performance, and efficiency, which is a key step in biometric algorithm design.

Compression

Many applications require storage or transmission of the biometric data (e.g., images).

These data can be large and it is often desirable to compress them to save storage space or transmission bandwidth. This compression can be either lossless or lossy. Lossless compression algorithms guarantee that every single bit of the original signal is unchanged after the data is uncompressed. Higher compression ratio can be achieved with lossy compression at the cost of altering the original signal. Artifacts introduced by lossy compression may interfere with subsequent feature extraction and degrade the matching results.

Biometric systems often use lossy compression, chosen in such a way that a minimal amount of critical information is lost during the compression, to achieve the best balance between data quality and representation size. Standardization bodies have defined compression protocols for each biometric so that any user of the system can reconstruct the original signal. They also specify the compression ratio that must be used to preserve the quality of the biometric data. As an example, standards currently exist for the compression of fingerprints (WSQ for 500ppi and JPEG-2,000 for 1,000ppi), facial images (JPEG-2,000), and voice data (CELP) [3,4].

Quality Assessment

Biometric quality refers to the usefulness of a biometric sample in terms of the amount of discriminatory information. Quality assessment is the algorithm that calculates and assigns a quantitative quality score to a biometric sample based on its character (e.g., inherent features), fidelity (e.g., signal-to-noise ratio), or utility (e.g., correlation with system performance) [5].

Quality measure can be used for various applications in a biometric system: (1) to provide quality feedback upon enrollment to improve the operational efficiency of biometric systems; (2) to improve the matching performance of biometric systems, e.g., local quality can be used to assist feature extraction and assign confidence to features during matching; and (3) to improve performance of multibiometric systems, e.g., quality

can be used to derive weights or statistical significance of individual sample or modality in fusion.

There are two main paradigms for quality assessment algorithms: a “bottom-up” approach reflecting character and fidelity and a “top-down” approach based on observed utility [5]. In the “bottom-up” approach, quality measure is used to determine a sample’s “improvability” (i.e., the improvement that can be gained by recapturing the biometric). If a sample does not inherently have many features, recapturing will not benefit the performance. On the other hand, if the signal-to-noise ratio is very high, recapturing may help obtain additional salient features. In the “top-down” approach, the utility of a sample is used to determine a performance estimate. This estimate can be used to disregard (emphasize) features that have strong (weak) correlation with utility.

Development of quality assessment algorithms and algorithms that use the estimated quality information is an active area of research in biometric community. The NIST biometric quality workshop [6] provides a forum for the community to share new research and development in biometric quality assessment. An open source software to measure fingerprint quality has also been developed and released by NIST [7]. Standards committees from around the world are working to incorporate the concept of quality into the biometric standards, e.g., ISO/IEC 29794 [8], with the aim of uniform interpretation and interoperability of quality scores.

Enhancement

Enhancement, in the context of biometrics, is the process of improving the signal quality with or without knowing the source of degradation (this definition includes restoration). The general goal is to increase the signal-to-noise ratio, although many interpretations of signal/noise can be applicable. Enhancement typically employs prior knowledge about the acquired signal to facilitate automatic feature extraction algorithms or to provide better visualization for manual processing.

The quality of a signal can be affected by environmental conditions, sensor noise,

uncooperative/untrained subjects, inherent low-quality biometrics, etc. In order to ensure that the performance of a biometric algorithm will be robust with respect to the quality of the acquired signal, additional algorithms/heuristics must be employed to improve the clarity of the desired traits in the signal. Different types of normalization (e.g., histogram equalization) or filtering approaches (e.g., Gabor wavelets) can be employed to separate noise from biometric signals [9]. Segmentation (i.e., detecting the meaningful part of the signal and discarding the background) is another example of enhancement that is classically used.

Feature Extraction

During feature extraction, the biometric data is processed to extract a set of salient and discriminatory features that represent the underlying biometric trait. These features can either have a direct physical counterpart (e.g., minutiae for fingerprints) or indirectly related to any physical trait (e.g., filter responses for iris images) [10]. The extracted set is commonly referred to as the template and is used as an input for matching and filtering (classification/indexing). Ideally, the extracted features are consistent for the same subject (small intraclass variation) and are distinct between different subjects (small interclass similarity). In practice, however, factors such as poor image quality and distortion can greatly affect the accuracy of feature extraction.

Feature extraction can be related to dimensionality reduction, where the raw input signal is often in high dimension, containing redundant and irrelevant information [2]. Feature extraction transforms the original data space into a lower dimension by retaining the most discriminatory information possible. In fact, standard dimensionality algorithms (e.g., PCA) are commonly employed to extract features for face images. Regardless of the trait, the feature extraction algorithm greatly controls the performance of matching [10]. If feature extraction can separate the subjects in the feature space, simple matching algorithms can be employed. If feature extraction

performs poorly, it may not be possible to design a matching algorithm that will provide sufficient accuracy.

For some applications, especially those where multiple systems need to work together, algorithms need to be interoperable. That is, in particular, the extracted features or templates are encoded in such a way that they can be used by any matching system that follows the same encoding standard. This is crucial for large-scale applications, such as biometric passport, especially when the template storage space is small. Once again, standardization bodies play an important role in defining common formats to store the biometric templates. The Minutiae Interoperability Exchange Test (MINEX) [11], conducted by NIST, quantified the impact on system performance to use fingerprint minutiae standards in comparison to proprietary formats.

Matching

A matching algorithm compares the features extracted from the query with the stored templates in the database to produce scores that represent the (dis)similarity between the input and template. A matching algorithm must cope with variations of the extracted features [12]. These variations may be the result of modification (e.g., scar, aging, disease), occlusion (e.g., beard, glasses), presentation (pose, displacement, nonlinear distortion), and noise (lighting, motion blur) of the biometric trait. Variations resulting from the presentation of the biometric are typically handled through the use of invariant features or by trying to “align” the two templates. A common approach to alleviate some variations is to introduce certain flexibility (or tolerance) in the matching of individual features (local matching) and obtain an accumulated probability value (global matching) for computing the final match score. In many cases, this approach is shown to exhibit some complementary nature, increasing robustness to errors while preserving high accuracy. Integration (fusion) of various feature representations in a matching algorithm or combining different matching

algorithms seems to be the most promising way to significantly improve the matching accuracy.

In the final stage, matching must provide a decision, either in the form of validating a claimed identity or providing a ranking of the enrolled templates to perform identification. The biometric matching algorithms range from simple nearest neighbor algorithms to sophisticated methods such as support vector machines. Thresholding techniques are used to decide if the distance of the claimed identity (in verification) or first rank (in identification) is sufficient for authentication.

In large systems, such as countrywide ID or law enforcement systems, when throughput is high or when matching decision has to be determined online in real time (e.g., border crossing), the time of an individual match must be very small. This imposes strong constraints on the design of the matching algorithm. In order to achieve both high accuracy and speed, multistage matching techniques are often used. Furthermore, biometric algorithms can often be implemented in a parallel architecture, and the processing of matching can be distributed over many CPUs.

Filtering (Classification/Indexing)

With the rapid proliferation of large-scale databases, one-to-one matching of the query with each template in the database would be computationally expensive. A filtering process is, hence, usually employed to reduce the number of candidate hypotheses for matching operation. Filtering can be achieved by two different approaches: classification and indexing [10].

Classification algorithms, or classifiers, partition a database into a discrete set of classes. These classes can be explicitly defined based on the global features of the biometric data, e.g., “Henry classes” for fingerprints [13], or implicitly derived based on data statistics [10]. General biometric classification algorithms can be divided into rule-based, syntactic-based, structural-based, statistical-based and neural network-based and multi-classifier methods. Sometimes, a single-level classification is not efficient enough as data may be unevenly distributed among these classes.

For example, more than 90% of fingerprints belong to only three classes (left loop, right loop, and whorls). To continue narrowing down the search, some classes can be further divided into more specific categories, also known as subclassification. Once templates in a database are classified, matching time can be greatly reduced by comparing the query only with templates belonging to the same class assigned to the query.

Indexing algorithms [10], on the other hand, provide a continuous ordering of the database. This process is also often referred as continuous classification, where biometric data are no longer partitioned into disjoint classes, but associated with numerical vector representations of its main features. This can also be regarded as an extremely fast matching process, where feature vectors can be created through a similarity-preserving transformation and the matching is performed by comparing the query only with those in the database whose vector representation are close to that of the query in the transformed space.

Because they can be extremely fast, filtering techniques are often used as a first stage in multistage matching. Indexing is often preferred over classification, since it enables to avoid classifying ambiguous data (e.g., by adjusting the size of the neighborhood considered for matching) and can be designed to be virtually error free.

Fusion

Biometric systems can be designed to recognize a person based on information acquired from multiple biometric sources. Such systems, also known as multibiometric systems, offer substantial improvement with regard to enrollment and matching accuracy over traditional (uni) biometric systems [12, 14]. The algorithm that combines the multiple sources of information in a multibiometric system is called fusion.

Biometric fusion can be performed at four different levels of information, namely, sensor, feature, match score, and decision levels [12, 14]. Fusion algorithms can be used to integrate

primary biometric traits (e.g., fingerprint and face) with soft biometric attributes (e.g., gender, height and eye color). Besides improving recognition accuracy, information fusion also increases population coverage (by avoiding “failure to enroll”) and deters spoof attacks in biometric systems [14].

Related Entries

- ▶ [Biometric Applications, Overview](#)
- ▶ [Biometric Sample Acquisition](#)

References

1. A. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol.* **14**(1), 4–20 (2004)
2. R. Duda, P. Hart, D. Stork, *Pattern Classification*, 2nd edn. (Wiley, New York, 2000)
3. C. Brislawn, The FBI fingerprint image compression specification, in *Wavelet Image and Video Compression*, ed. by P. Topiwala (Kluwer Academic, Boston, 1998), pp. 271–288
4. C. Brislawn, M. Quirk, Image compression with the JPEG-2000 standard, in *Encyclopedia of Optical Engineering*, ed. by R. Driggers (Marcel Dekker, New York, 2003), pp. 780–785
5. INCITS Biometric Sample Quality Standard Draft, M1/06–0948 (2006), http://www.incits.org/tc_home/m1htm/2006docs/m1060948.pdf
6. NIST Biometric Quality Workshop (2006), <http://www.itl.nist.gov/iad/894.03/quality/workshop07/index.html>, 2007
7. E. Tabassi, C. Wilson, C. Watson, Fingerprint image quality, NIST research report NISTIR7151, 2004
8. ISO/IEC Biometric Sample Quality Standard, ISO/IEC 29794 (2009), http://www.iso.org/iso/iso_catalogue/catalogue_detail.htm?csnumber=43583
9. L. Hong, Y. Wan, A. Jain, Fingerprint image enhancement: algorithms and performance evaluation. *IEEE Trans. Pattern Anal. Mach. Intell.* **20**(8), 777–789 (1998)
10. D. Maltoni, D. Maio, A. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition* (Springer, New York, 2003)
11. P. Grother, M. McCabe, C. Watson, M. Indovina, W. Salamon, P. Flanagan, E. Tabassi, E. Newton, C. Wilson, MINEX: performance and interoperability of the INCITS 378 fingerprint template. NIST MINEX Evaluation Report, 2006

12. A. Jain, P. Flynn, A. Ross, *Handbook of Biometrics* (Springer, New York, 2008)
13. E. Henry, *Classification and Uses of Finger Prints* (Routledge, London, 1900)
14. A. Ross, K. Nandakumar, A. Jain, *Handbook of Multibiometrics* (Springer, New York, 2006)

Biometric and User Data, Binding of

Peng Li¹, Jie Tian², Xin Yang¹, and Sujing Zhou¹

¹Institute of Automation, Chinese Academy of Sciences, Beijing, People's Republic of China
²Center for Biometrics and Security Research & The Key Laboratory of Complex System and Intelligence Science Chinese Academy of Sciences, Institute of Automation Zhingguancun Donglu, Beijing, China

Synonyms

Key binding; Secure biometrics; Template protection

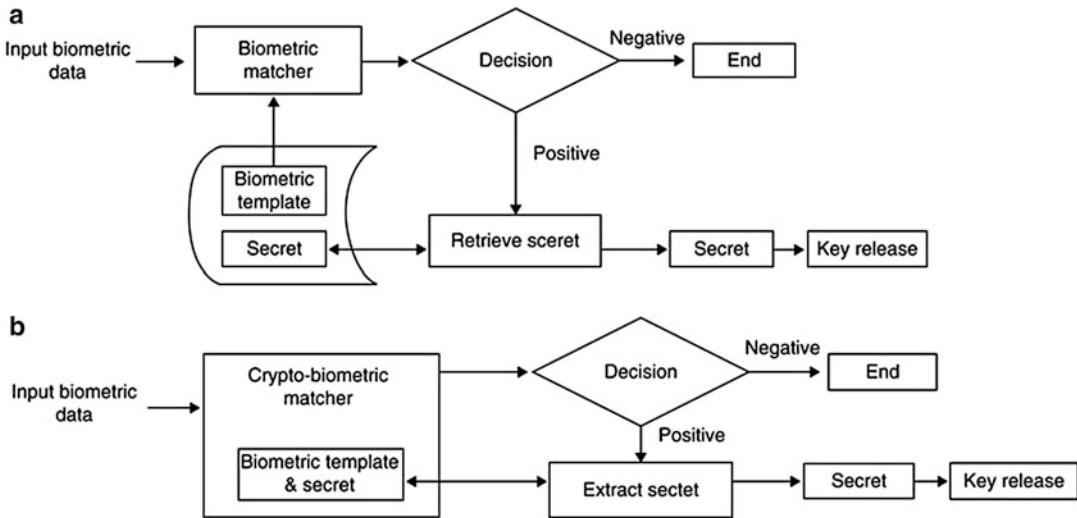
Definition

“User data” stands for the private information of the biometric system user, for example, identity number, e-mail address, or any other significant or insignificant character string, which can be transformed into ASCII code in computer systems. Binding of biometric and user data is a method which aims to solve the issues of security and privacy involved with biometric system. As an important method of biometric encryption, binding of biometric and user data has two main functions: one is protecting the biometric template from attacks, where cancelable biometric templates can be generated, and the other is embedding user data into the biometric template, where user data will be reproduced if and only if biometric matching succeeds.

Introduction

As an identity authentication method, biometrics bases recognition on an intrinsic aspect of the human being, and the use of biometrics requires the person to be authenticated as physically present at the point of the authentication [1]. With more and more application examples, biometrics recognition system exposes some intrinsic defects; the most serious is the security and privacy issue involved with raw biometric data [2]. Biometric data is difficult to cancel in case it is lost or obtained by an attacker. The lost biometric may be used for cross-matching between different databases and can bring disastrous results to user data. Because of this kind of hidden danger, people resort to a more secure biometric system, called Biometric Encryption or Biometric Cryptosystems [3]. Among the various methods of Biometric Encryption, binding of biometric and user data is the most practical and promising one, which is named Key Binding Method. This is different from the other key-related method: Key Release (Fig. 1).

The commonly collected user data includes name, any form of ID number, age, gender, e-mail address, etc. The user data which is bound with biometric in the algorithm layer, say e-mail address or social security ID, should be protected from being stolen by the attackers, while the nonsensitive data can be open. In the enrollment stage of the Biometric Encryption system, the biometric feature extraction procedure is the same as in the traditional system. After the feature is obtained, it will be bound with user data (e.g., identity number, password, etc.) in some way, thus yielding a cancelable biometric template, which will be stored as a private template and used to match the query samples. In the matching stage, the user provides his/her biometric and the user-specific data to the biometric system. Then, the same feature extraction and binding procedure will be conducted inside the system. The two private templates are compared in the traditional manner in which the biometric system works and a matching score or YES/NO decision is given. In some algorithms, famous



Biometric and User Data, Binding of, Fig. 1 (a) Key release. (b) Key binding (Reprinted with permission from Jain et al. [4] ©2006 IEEE)

fuzzy vault algorithm, for instance, if matching succeeds, the user-specific key is reproduced and released. The key can be used in different conventional cryptographic circumstances.

Challenges

The difficulty of binding biometric and user data lies mostly in how the fuzziness of biometrics and the exactitude of user data (key) are bridged.

Fuzziness of Biometrics

Unlike the password-based identity authentication system, biometric signals and their representations (e.g., fingerprint image and its computer representation) of a person vary dramatically depending on the acquisition method, acquisition environment, and user's interaction with the acquisition device [2].

Acquisition condition variance: The signal captured by a sensor varies with the identifier as well as the acquisition equipment. For example, fingerprint images are usually captured with contacting sensors, e.g., capacitive sensor, inductive sensor, and optical sensor. The mechanism of imaging fingerprint is mapping a three-dimensional object to a two-dimensional

plane. Since the fingertip is nonrigid and the mapping procedure cannot be controlled precisely, the captured fingerprint images change in minute details from time to time, but are still within a certain metric distance of intra-class difference. When the sensor's surface is not large enough or the user provides only part of the finger to the sensor, the acquired image area does not cover the whole finger. Different fingerprint images from the same finger may include different parts of the finger. In addition, translation and rotation are very common in different samples from the same finger. Another good example to show the acquisition condition variance is facial image acquisition. Illumination change influences the captured facial image in real circumstances. Moreover, the greatest variance is in the facial expression, including the kinds of modalities used to express different emotions. Almost all kinds of biometric modalities have to bear this variance.

Circumstances and time variance: Change in outer circumstances may also cause the captured biometric signal to vary more or less. While taking the fingerprint, for example, environmental temperature and humidity may render the finger too dry or too damp to be captured. Low-quality fingerprint images are very common

in real application systems, and enhancing (i.e., preprocessing) them is a challenging research direction in the traditional fingerprint recognition field. Generally, the fingerprint does not change with time because the skin on the fingertip may not change much with age. But many modalities cannot resist the temporal change, e.g., face, gait, palm, voice, and so on. In particular, the face varies greatly with age; facial images captured from the same person at different ages differ vastly. How one estimates the aging model of a person also makes an important research issue in the face recognition field. In addition, there are other factors which can influence the captured biometric signal for some specific modality.

Feature extraction variance: Almost all the feature extraction algorithms are based on signal processing or image processing methods. They are not exact when processing different biometric samples. Noise is often introduced in the extraction procedure, especially of the low-quality samples.

All the above factors can make the samples from the same subject seem different and the ones from different subjects quite similar. Large intra-class differences and small inter-class differences will be the result due to these reasons. However, a cryptosystem requires exact computing and operation. A tiny change in input may cause an enormous difference in output, for example, for the hash function. So bridging the fuzziness of biometrics and the exactness of cryptography becomes the greatest challenge in the binding of biometric and user data.

Encrypted Template Alignment

The second challenging problem is how to align the encrypted biometric templates. One of the purposes of binding biometric and user data is to conceal raw biometric data. Thus original features cannot be used for alignment after binding to prevent the original template from being stolen. Nevertheless, the alignment stage has to be conducted to locate the various biometric samples in the same metric space and to ensure the authentication accuracy. So the feature used in the alignment stage must satisfy two conditions:

(1) it will not reveal original biometric data and (2) it must assure alignment accuracy to some extent. The concept of Helper Data satisfying these conditions was proposed [5]. Taking the case of the fingerprint as an example, the points with maximum local curvature around the core are detected and used for alignment without leaking the minutiae information. Theoretically, the system security can be estimated according to information theory from the information published by Helper Data [6].

Theory and Practice

The theories of Secure Sketch [6] and fuzzy extractor [6] lay the foundation for the binding of biometric and user data and give some significant theoretic results from the point of view of information theory. In the various binding methods of biometric and user data, Bioscrypt [7], Biohashing [8], fuzzy commitment [9], and fuzzy vault [10] are the most representative to address the problem of security and privacy. These algorithms will be described in detail in the next section.

Fuzzy Commitment Scheme

Fuzzy commitment scheme [9] is one of the earliest methods of binding biometric and user data. It is actually an ordinary commitment scheme (a primitive in cryptography) taking biometric templates as private keys and employing error correcting codes to tackle the fuzziness problem of biometric templates.

As an ordinary cryptographic commitment, the fuzzy commitment scheme has two procedures: committing and decommitting. To commit a bit string x , first generate a codeword c from x according to a prespecified error correcting code, then apply some cryptographic hash function (or one-way function) to c , the ultimate commitment is $(h(c), w + c)$, where w is a biometric template-related string with the same length of c . To decommit a commitment, the user has to provide a biometric template-related string w' which is close to that in the committing procedure; the verifier uses it to decode the correct codeword c ,

then checks whether the hash value of c equals the stored hash value in the commitment, and accepts the commitment if they are equal, rejects otherwise. The fuzzy commitment scheme is essentially a Secure Sketch as observed by Dodis et al. [6].

Secure Sketch

A Secure Sketch is a primitive component proposed by Dodis et al. [6] to extract helper data from the input biometric sample and to reconstruct the original sample according to the helper data without storing the raw biometric template. A Secure Sketch consists of two procedures. The first procedure outputs a bit string (called helper data) from the enrolled biometric template and stores the bit string while discarding the enrolled biometric template. In the second procedure, the query sample is inputted. The biometric template could be reconstructed according to the query and the helper data if the distance between the query and the template is less than a specified threshold in terms of some metric space.

The security of a Secure Sketch is estimated as the loss of the min-entropy of the enrolled biometric template between the sketch values before and after the bit string is provided; the less the loss, the better. In case the distance between the two biometric templates is measured by the number of positions in which the two binary represented biometric templates differ, e.g., in Hamming metric space, two basic constructions based on error correcting codes are known: code-offset construction and syndrome construction. In case the distance between the two biometric templates is measured by the number of elements that occur only in one of the two duplicate-free set represented biometric templates, e.g., in set difference metric space, the construction is called a PinSketch. In case the distance between two biometric templates is measured by the smallest number of character insertions and deletions required to change one biometric template into another one, e.g., in edit metric space, the metric space is first transformed into another metric space that is easy to handle by embedding injections with some distortion that is tolerable and then treated as in the transformed metric space.

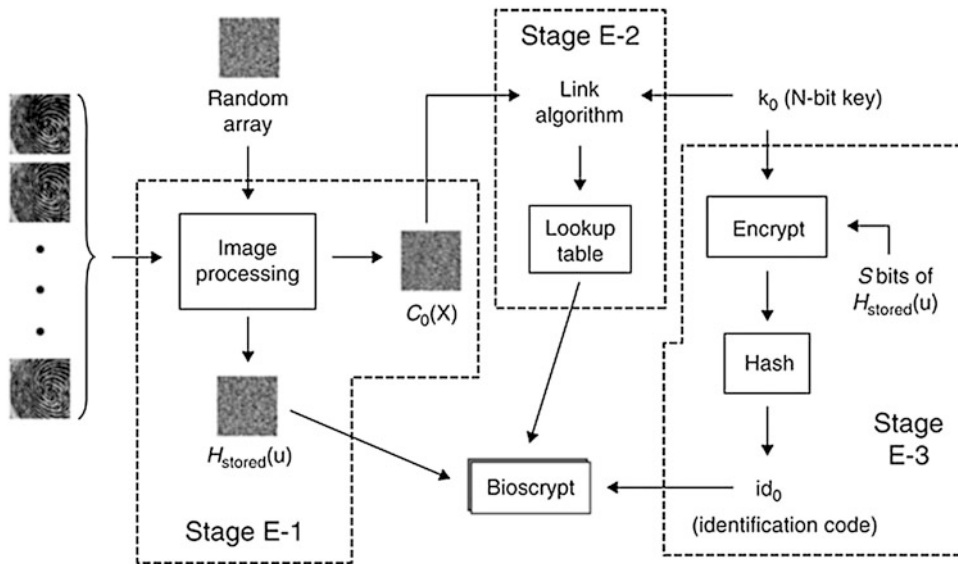
A Secure Sketch can be used to construct a fuzzy extractor. Fuzzy vault and fuzzy commitment in this context are essentially Secure Sketches in Hamming metric space and set difference metric space, respectively.

Fuzzy Extractor

A fuzzy extractor is a primitive component proposed by Dodis et al. [6] to obtain a unique bit string extracted from the biometric template provided in enrollment whenever the query biometric template is close enough to the enrolled biometric template. The random bit string can be further used as a private key of the user.

A fuzzy extractor consists of two procedures. The first procedure outputs a bit string and a helper data from the enrolled biometric template and stores the helper data while it discards the bit string and the enrolled biometric template. The second procedure outputs the bit string from the first procedure if the distance between the query biometric template and the enrolled biometric template is less than a specified parameter, given a query biometric template and helper data from the first procedure.

The security of a fuzzy extractor is estimated as the statistics distance between the bit string and a uniform random distribution when the helper data is provided; the closer, the better. A fuzzy extractor can be constructed easily from any Secure Sketch. A fuzzy extractor itself is also an important primitive component in biometric-based cryptosystems. Fuzzy extractors with robustness [6] are considered to protect against a kind of active attack, i.e., an adversary might intercept and change the helper data in a way to obtain biometric template-related private information of the user who blindly applied his biometric template on the fraud helper data. Fuzzy extractor with reusability [6] is also considered to secure against a kind of active attack, i.e., a collusion attack from multiple application servers to which a user is enrolled by the same fuzzy extractor scheme, each server obtaining a different helper data, and by collusion, there exists the risk of exposure of private user data, e.g., biometric template.



Biometric and User Data, Binding of, Fig. 2 Overview of the enrollment process for Biometric Encryption (Reprinted with permission from [6])

Bioscrypt

Bioscrypt [7], a method of binding biometric and user data, is the first practical Biometric Encryption algorithm to the authors' knowledge. The binding is based on performing a Fourier Transform of a fingerprint.

In the enrollment stage (Fig. 2), several fingerprint images, denoted by $f(x)$, are inputted, and Fourier Transformation and other operations are performed to result in $H(u)$. $H(u)$ composes two components: magnitude $|H(u)|$ and phase $e^{i\phi} H(u)$. The magnitude component $|H(u)|$ is discarded, and the phase $e^{i\phi} H(u)$ is preserved. A random array is generated according to RNG (Random Number Generator), denoted by R . The phase components of R , denoted by $e^{i\phi} R(u)$, are used to multiply with $e^{i\phi} H(u)$ and results stored in $H_{\text{stored}}(u)$. In addition, $c_0(x)$ is produced from the Fourier Transform of the number of fingerprints and stored into a lookup table together with an N-bit key k_0 , where k_0 and $c_0(x)$ are linked with a link algorithm. On the other hand, k_0 is used to encrypt S bits of $H_{\text{stored}}(u)$, and then the result will be hashed to obtain an identification code id_0 . After the above procedure, $H_{\text{stored}}(u)$, the lookup table, and the

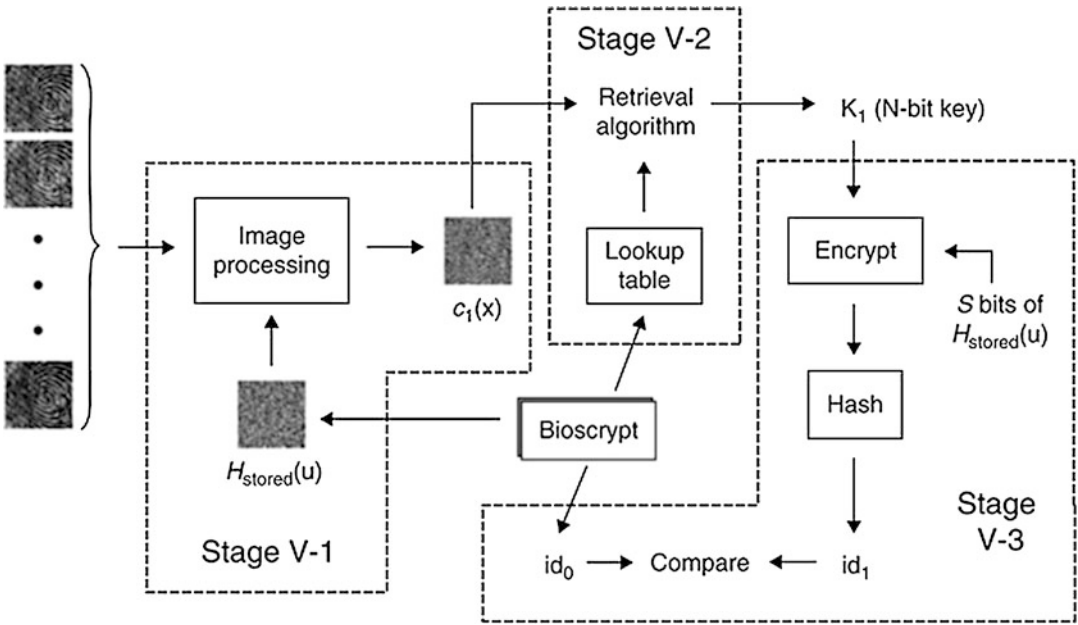
identification code id_0 are stored together in a template (called Bioscrypt by the authors).

In the verification stage (Fig. 3), after inputting the query fingerprint sample and the Fourier Transform operation, the identification code $c_1(x)$ is computed according to the $H_{\text{stored}}(u)$ in the Bioscrypt. Through the link algorithm, a key k_1 is released from the lookup table in the Bioscrypt. id_0 is released synchronously to be used for comparing in the next step. S bits of $H_{\text{stored}}(u)$ is encrypted with k_1 , and the result is hashed to result in id_1 . id_1 is compared to id_0 , and if they are identical, the identification succeeds, otherwise fails.

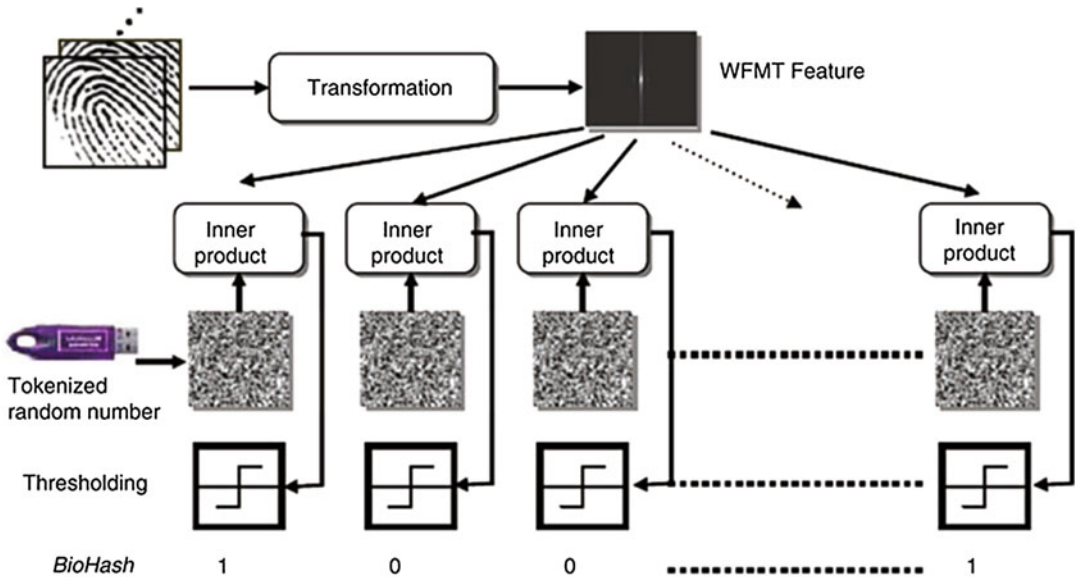
Biohashing

Biohashing [8] is also a typical Biometric Encryption algorithm binding biometric and user data. In the beginning, it uses the fingerprint, followed by facehashing [11], palmhashing [12], and so on.

Toeh et al. [8] proposed the two-factor identity authentication method combining fingerprint and tokenized random number (i.e., user data). The Wavelet Fourier Mellin Transform (WFMT) feature of fingerprint is employed (Fig. 4), and



Biometric and User Data, Binding of, Fig. 3 Overview of the verification process for Biometric Encryption (Reprinted with permission from [6])

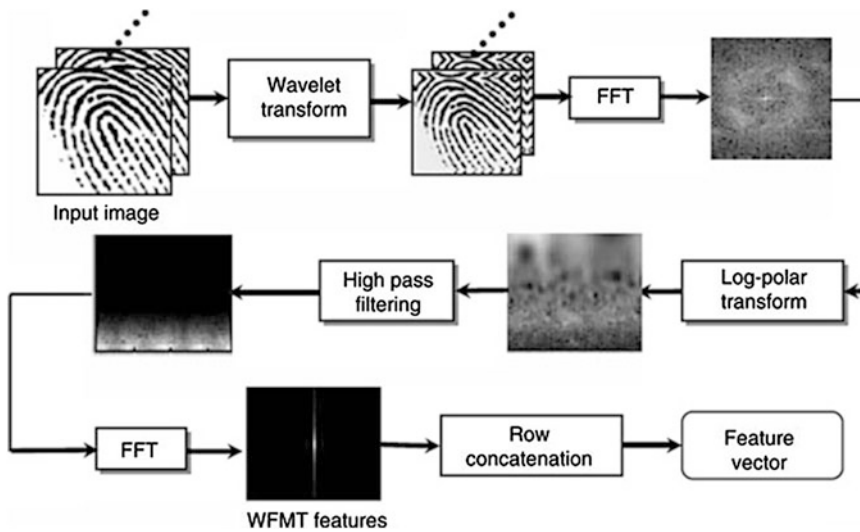


Biometric and User Data, Binding of, Fig. 4 The flowchart of WFMT generation (Reprinted with permission from [7])

iterative inner product operations are performed on WFMT and the user-specific pseudo-random number stored in the user's token (Fig. 5). Quantization is then conducted on the inner product value according to the preset threshold. Thus,

from a fingerprint image, a bit string can be obtained, which is used for matching in terms of Hamming distance.

However, the authentication performance of bihashing will decrease greatly if the token



Biometric and User Data, Binding of, Fig. 5 Flowchart of iterative inner product operation (Reprinted with permission from [7])

(i.e., the user data) is stolen by the attacker, which is called the token-stolen scenario. Related experiments have confirmed this point. That is to say, tokenized random number plays a more important role than the biometric itself in the biohashing algorithm.

Some subsequent work has focused on improving the performance in the token-stolen scenario, e.g., Lumini and Nanni's work [13], which are briefly described below. They improved the performance by dramatically increasing the length of the biohashing output. The following are the specific solutions leading to the reported improvement:

1. *Normalization*: Normalizing the biometric vectors by their module before applying the biohashing procedure, such that the scalar product $\langle x | or_i \rangle$ is within the range $[-1, 1]$
2. τ *Variation*: Instead of using a fixed value for τ , using several values for τ and combining with the "SUM rule" the scores obtained by varying τ between τ_{\max} and τ_{\min} , with p steps of $\tau_{\text{step}} = (\tau_{\max} - \tau_{\min}) / p$
3. *Spaces augmentation*: Since the dimension of the projection space m cannot be increased at will, using more projection spaces to generate more BioHash codes per user. Let k be the selected number of projection spaces to be

used; the Biohashing method is iterated k times on the same biometric vector in order to obtain k bit vectors b_i , $i = 1, 2, \dots, k$. Then the verification is carried out by combining the classification scores obtained by each bit vector (BioHash code). The random generation can be performed in an iterative manner, thus requiring a single Hash key K : in such a way that the random generator is not reinitialized by a new key until the complete generation of the k bases is not performed.

4. *Features permutation*: Another way to generate more BioHash codes, without creating more projection spaces, is to use several permutation methods of the feature coefficients in x during the projection calculation: using q permutations of x obtained by round-shifting the coefficients of a fixed amount, thus obtaining q bit vectors. As above the verification is carried out by combining the classification scores obtained by each bit vector.

Fuzzy Vault

The fuzzy vault algorithm [10] is a practical method of binding biometric and user's private key. It consists of the following two steps:

1. A user Alice places a secret (K) in the vault and locks it with an unordered set A .

2. Another user Bob tries to access the secret (K) with another unordered set B (i.e., unlock the vault).

Bob can access the secret (K) if and only if the two unordered sets B and A overlap substantially.

Specifically, the fuzzy vault can be depicted as follows:

1. *Encoding the Vault*: A user Alice selects a polynomial p of variable x encoding K , then computes the project $p(A)$ of the unordered set A on the polynomial p ; thus $(A, p(A))$ can construct a finite point set. Some chaff points are then randomly generated to form R with the point set $(A, p(A))$; R is the so-called Vault. The chaff point set is vital to hide the secret K , and the point numbers in it are more than the real point set.
2. *Decoding the Vault*: Another user Bob tries to access the secret (K) with another unordered set B . If the elements in B and the ones in A overlap substantially, then many points in B will lie in the polynomial p . So Bob can use correction code technology to reconstruct p and consequently access the secret K . However, if a large proportion of points in B and A do not overlap, due to the difficulty of reconstructing the polynomial, it is almost infeasible to attain p over again.

The security of fuzzy vault scheme is based on the polynomial reconstruction problem. This scheme is highly suitable for hiding biometric data, because it works with unordered sets (e.g., fingerprint minutiae) and can tolerate difference (element number or kind or both) between the two sets A and B to some extent.

The idea of “fuzzy fingerprint vault” [14] and “fuzzy vault for fingerprint” [5] are also proposed aiming to solve the problems of fingerprint template protection. Fuzzy vault for face [15] and iris [16] have also been proposed recently.

Performance Evaluation

Performance evaluation of the binding of biometric and user data should be conducted based mainly on two aspects: accuracy and security.

Accuracy reflects the effect after binding of biometric and user data as an enhanced identity authentication way, and security can provide information on the probability that the system will be attacked successfully.

1. **Accuracy**: The accuracy of biometric-like identity authentication is due to the genuine and imposter distribution of matching. The overall accuracy can be illustrated by Receiver Operation Characteristics (ROC) curve, which shows the dependence of False Reject Rate (FRR) on False Accept Rate (FAR) at all thresholds. When the parameter changes, FAR and FRR may yield the same value, which is called Equal Error Rate (EER). It is a very important indicator to evaluate the accuracy of the biometric system, as well as binding of biometric and user data.
2. **Security**: The security of the binding of biometric and user data depends on the length of user data, which is converted to binary 0/1 expression. It assumes the attacker has full knowledge about the binding method, but can only mount brute-force attack on the system. So the system security is weighed by bit length of the user data. Typically, the security of the iris binding system is 140 bits and that of fingerprint is 128 bits. However, typical face binding algorithm holds only 58-bit security [3].

Summary

Binding of biometric and user data is a kind of technique to tackle the issues of security and privacy arising frequently in traditional biometric systems. It may decrease the accuracy performance to some extent, but generally, the security and privacy of the system are enhanced.

Related Entries

- ▶ [Privacy Issues](#)
- ▶ [Security Issues, System Design](#)

References

1. D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition* (Springer, New York, 2003)
2. U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain, Biometric cryptosystems: issues and challenges. *Proc. IEEE*. **92**(6), 948–960 (2004)
3. http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf
4. A Jain et al., Biometrics: a tool for information security. *IEEE Trans. Inf. Forensics Secur.* **1**(2), 125–143 (2006)
5. U. Uludag, A. Jain, Securing fingerprint template: fuzzy vault with helper data, in *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshop*, New York, 2006, p. 163
6. Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractor, in *Security with Noisy Data*, ed. by P. Tuyls, B. Skoric, T. Kevenaar (Springer, London, 2008)
7. C. Soutar, D. Roberge, S.A. Stojanov, R. Gilroy, B.V.K.V. Kumar, Biometric encryption, in *Proceedings of ICSA Guide to Cryptography*, ed. by R.K. Nichols (McGraw-Hill, New York, 1999)
8. A.B.J. Teoh, D.C.L. Ngo, A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognit.* **37**(11), 2245–2255 (2004)
9. A. Juels, M. Wattenberg, A fuzzy commitment scheme, in *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, Singapore, 1999, pp. 28–36
10. A. Juels, M. Sudan, A fuzzy vault scheme, in *Proceedings of IEEE International Symposium on Information Theory*, Lausanne, 2002, p. 408
11. D.C.L. Ngo, A.B.J. Toeh, A. Goh, Eigenface-based face hashing, in *Proceedings of International Conference on Biometric Authentication*, Hong Kong, 2004, pp. 195–199
12. T. Connie, A. Teoh, M. Goh, D. Ngo, PalmHashing: a novel approach for cancelable biometrics. *Inf. Process. Lett.* **93**(1), 1–5 (2005)
13. A. Lumini, L. Nanni, An improved biohashing for human authentication. *Pattern Recognit.* **40**(3), 1057–1065 (2007)
14. T.C. Clancy, N. Kiyavash, D.J. Lin, Secure smartcard-based fingerprint authentication, in *Proceedings of ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, Berkley, 2003, pp. 45–52
15. D. Nyang, K. Lee, Fuzzy face vault: how to implement fuzzy vault with weighted features, in *Proceedings, Part I of Fourth International Conference on Universal Access in Human-Computer Interaction, UAHCI 2007, Held as Part of HCI International 2007*, Beijing (Springer, Heidelberg, 2007), pp. 491–496
16. Y.J. Lee, K. Bae, S.J. Lee, K.R. Park, J. Kim, Biometric key binding: fuzzy vault based on iris images, in *Proceedings of the Second International Conference on Biometrics*, Soul (Springer, Heidelberg, 2007), pp. 800–808

Biometric Applications, Overview

David Day

International Biometric Group, New York,
NY, USA

Synonyms

Biometrics

Definition

A biometric application is the sum of the functionality, utilization, and role of a biometric technology in operation. Biometric technologies such as fingerprint, face recognition, and iris recognition are utilized in a range of applications that vary in terms of performance requirements, operational environment, and privacy impact. Biometric technology selection – which modality to utilize and what hardware and software to deploy – is typically driven in large part by the application. Biometric applications can be generalized into four categories. The first application category is controlling access to data, such as logging into a device, PC, or network. The second application category is controlling access to tangible materials or areas, such as physical access control. The third application category is to validate a claimed identity against an existing credential, such as in a border control environment. The fourth application is to register or identify individuals whose identities need to be established biometrically, most often using centralized or distributed databases. Beyond this high-level decomposition, an application taxonomy can be defined that spans 12 distinct

biometric applications. This taxonomy takes into account factors such as the user's motivation and incentive, the location of biometric data storage and matching, the nature of the data or materials that the biometric is protecting, and the role of non-biometric authentication and identification techniques.

Introduction

The need for secure, reliable identity validation and confirmation has driven the adoption of biometric technologies in a diverse range of applications. Biometric applications can be generalized into four categories. The first application category is controlling access to data, such as logging into a device, PC, or network. The second application category is controlling access to materials or areas, such as physical identity against an existing credential, such as in a border control environment. The fourth is to register or identify individuals whose identities need to be established by biometric means, most often using centralized or distributed databases. Law enforcement and military uses of biometrics are primary examples of this fourth application category.

Though the four generalized functionalities provide an overview of how biometrics can be applied, a more detailed taxonomy is required to capture the full breadth of biometric application. The large majority of biometric utilization and deployment can be grouped into one of 12 applications:

- *Law Enforcement (Forensics):* Biometric technologies have long been utilized as a secure means to identify alleged criminals. In this particular application, an individual's fingerprints are used to determine or confirm an identity against a central record store. The FBI currently holds one of the largest biometric databases, comprised of tens of millions of civil and criminal fingerprint records.
- *Background Checks:* Biometric technologies are used to execute background checks as a condition of employment for many government and commercial professions. While background checks may be executed against the same databases used in criminal searches, the applications differ in that background check or "civil" records are typically not retained – they are discarded after the result is returned to the querying agency.
- *Surveillance:* Biometric technologies are deployed, locate, track, and identify persons in a field of view (i.e., in a given space or area). Historically, surveillance applications required laborious and monotonous monitoring of cameras. Biometrics automates the process through the utilization of face-recognition technology; biometric surveillance systems can be configured to alert officials to the presence of individuals of interest.
- *Border Control:* The ever-increasing volume of international travel necessitates implementation of technologies that can automate, streamline, and expedite border crossing. Driven by international standards for biometric-enabled passports, as well as ad hoc regional efforts, countries utilize fingerprints, iris, and face-recognition technologies in border control applications ranging from localized to nationwide. Deployed properly, biometrics can ensure that screening resources are routed toward travelers whose risk profile is unknown.
- *Fraud Reduction:* Biometric technology can be deployed in public-sector applications to prevent individuals from claiming benefits under multiple identities. Government agencies have utilized iris and fingerprint recognition as a means to deter "double dipping" at the state and federal levels.
- *Trusted Traveler:* This application enables users to traverse security checkpoints with reduced likelihood of rigorous security inspections. Iris recognition and fingerprint are the leading technologies in this high-profile biometric application.
- *Physical Access Control:* Physical access control is the use of biometrics to identify or verify the identity of individuals before permitting access to an area. Companies and government agencies deploy technologies such as

fingerprint, hand geometry, and iris recognition to control key entry and exit points.

- *Time and Attendance: Biometrics can serve as a commercial application to assist in employee management. In this particular application, devices are used to track employee attendance. Hundreds of commercial deployments utilize hand geometry and fingerprint recognition to ensure the integrity of work hours and payroll.*
- *Consumer Recognition: This application refers to the confirmation of one's identity in order to execute a commercial transaction. Conventional authentication methods have utilized keycards, PIN numbers, and signatures to ensure the validity of a given transaction. Biometrics can reduce reliance on tokens and passwords and can provide consumers with a sense of assurance that their transactions are secure. Fingerprint recognition is a common technology deployed in this application.*
- *Remote Authentication: Biometrics provide a secure method of authentication for remote access to important information by allowing mobile device users to be accurately identified. Previous deployments have utilized fingerprint and voice recognition.*
- *Asset Protection: This application describes the need to protect digital information and other sensitive materials from unauthorized users. One common application is the use of fingerprint recognition on safes to protect sensitive documents. Biometrics also serves to compliment already in-place security methods such as passwords and user identification on computer workstations.*
- *Logical Access Control: Biometrics is used to control access to systems and/or devices based on physical characteristics. It is commonly used to control access to centralized databases, healthcare information, or financial records. Many deployments have utilized fingerprint recognition due to its proven reliability, ease of use, and accuracy.*

As seen by the aforementioned application descriptions, biometric technology is typically used

in applications where it can improve security, increase efficiency, or enhance convenience. Additionally, biometrics allow users to forego the responsibility of creating passwords and carrying keycards while maintaining a level of security that meets, and in some cases surpasses, that of conventional authentication methods.

Discussion

Each application utilizes biometrics as a solution to an identified authentication problem. There exist, however, key differentiating factors that help to distinguish one application from another. Some of these distinctions include the environment in which biometrics has been implemented, the purpose that biometrics is intended to serve, and the methods in which biometrics is utilized to serve its purpose.

The application of biometrics in law enforcement has utilized fingerprint recognition as a reliable means to identify criminals. Biometrics enable officials to conduct automated searches; compare biometric information of suspects against local, state, and national databases; and process mug shot-database comparisons [3]. A typical deployment would utilize a live-scan system, AFIS technology including matching hardware and software, and face-recognition software. Though such a scenario is common for law enforcement-related applications, recent trends have begun to push for mobile biometric devices in order to identify individuals in the field without the need to retain suspects for extended periods of time. Law enforcement applications of biometrics are unique in that they implement widely adopted standards for imaging, data transmission, and file formats. These standards allow jurisdictions to share fingerprint and face data in an interoperable fashion, even when biometric hardware and software are sourced from different suppliers. Increasingly, law enforcement biometric systems are deployed to search suspected terrorist data as well as data collected in military applications.

Background checks utilize biometric systems to determine the identity of an individual and to retrieve his or her historical records. Biometric

background check systems collect high-quality fingerprints for submission to state or federal systems that determine whether a given set of fingerprints is linked to criminal or other derogatory records. For example, some government agencies require individuals to submit biometric data for employment purposes. Fingerprint recognition technology is primarily used due to the extensive collection of fingerprint images currently held by government officials.

Surveillance applications utilize biometric technology, primarily face recognition, to locate and identify individuals without their awareness. Such applications are designed to collect biometric data without an explicit, direct presentation. By contrast, fingerprint and vein recognition technologies require individuals to voluntarily submit biometric measurement to the device. Surveillance application can, however, measure one's biometrics from a distance. A typical deployment would be to implement biometrics into already-existing security cameras or to install customized cameras whose resolution and performance characteristics are sufficient for acquisition of enrollable face images. In the future, gait recognition is envisioned as a surveillance technology capable of operating at greater distances than face recognition [2]. The technology could then notify officials to the presence of specific individuals in highly trafficked areas such as airport terminals. One challenge facing biometric surveillance is individual movement. Previously deployed systems have shown that quick and sudden actions can cause recognition performance to decrease. Some implementers have attempted to overcome this challenge by installing cameras in locations in which movement is limited such as entrances and staircases.

Border control focuses upon the management of international borders at targeted locations. At busy points of entry, it can be a difficult process to accurately and efficiently identify individuals. A common solution is to compliment conventional security protocols, such as identification cards, with biometric security methods such as fingerprint devices. This allows for 1:1 biometric matches that can reduce the time required to confirm the user's

identity. There are some complications, however, when implementing biometrics into border management. One challenge typically faced is the assurance of cross-jurisdictional interoperability. It can prove to be difficult to have bordering nations to agree upon a single standard.

Biometric technology can provide a considerable financial benefit to both the government and general public. Biometric systems are deployed in public service applications for fraud reduction, detecting and deterring the use of multiple identities to receive entitlements such as welfare payments. If a previously enrolled individual attempts to claim another identity, the biometric system recognizes this, and officials are alerted. Past deployments have utilized stationary fingerprint or iris recognition systems that have been installed within government facilities.

The trusted traveler application enables frequent travelers to bypass extensive and time-consuming security checkpoints after their initial enrollment. At enrollment, passengers submit their identification information and biometric data, which is then used to conduct a background check. Once the individual has been cleared as nonthreatening and their identity is verified, the agency can then distribute a specialized traveler's smart card that contains the traveler's information and biometric data [3]. With this smart card, the traveler can utilize specialized security checkpoints to gain access to airport terminals quickly and conveniently. Terminals install automated systems that determine whether to deny or grant access to the traveler based on their biometric information. Typical trusted traveler systems utilize gated entry points to prevent forced entry, smart cards that store biometric templates, and face, fingerprint, or iris recognition technology to verify the individual's identity. The commercial benefits of trusted traveler programs accrue when a critical mass of registrants is reached, as well as when additional programs are incorporated into the "trusted" framework.

Biometric physical access control deployments are most often implemented to control employee access to secure or protected areas. Typically, the biometric reader is installed as

a stationary system in which the user must verify his or her identity against a card-based, reader-based, or centralized template. Physical access control is one of the most well-established biometric applications, with hundreds of devices on the market ranging from inexpensive, standalone fingerprint readers to highly automated iris recognition devices. Fingerprint, face recognition, hand geometry, and vein recognition are also commonly deployed for physical access control.

Aside from maintaining a high level of security, biometric applications can help to serve the commercial sector for financial benefits. Biometrics used for time and attendance confirm the presence of an individual at a specific time, date, and location. Because of the potential difficulty of tracking the hours of thousands of employees at larger facilities, time and attendance applications allow management to automatically eliminate the possibility of “buddy punching”, tardiness, or absence without their knowledge. Automating this process can also lead to time savings with payroll management. Hand geometry recognition and fingerprint are the most frequently deployed biometric technologies in this application. Deployers often need to overcome the learning curve associated with device acclimation and the challenge of end-user acceptance.

Biometrics are deployed in financial sector applications to provide convenience and security for the consumer. Numerous banks have deployed fingerprint and vein recognition technology at ATMs as a method to enhance identification and security. The use of biometric technology bypasses the need for users to carry identification cards and to remember lengthy PIN numbers. Another possible application of biometric technology within the financial sector is to use biometrics in customer service call centers. This specific example utilizes voice recognition technology to bypass the need for customers to provide their identification details and verify their information. Instead, voice recognition technology automates the customer authentication process and allows representatives to immediately aid the consumer, saving time and increasing productivity.

Remote authentication utilizes biometrics to verify individuals in different locations and allows for unsupervised secure authentication. Web-based financial transactions without biometrics typically consist of an extended identification number, PIN number, and/or user information to verify an individual as authorized. This single factor authentication, however, can be easily replicated. Biometric technologies such as voice recognition or mobile fingerprint recognition [1] can provide an added layer of security to reduce customer fraud.

Biometric logical access control applications allow authorized users to gain access to systems or devices containing highly sensitive information such as healthcare information and financial records. A common approach would be to utilize inexpensive fingerprint peripherals (for workstations) or integrated fingerprint devices (for laptops). The user must provide his or her biometric information in order to gain access to sensitive device or system. It can be a challenge to deploy biometrics for logical access control because end users may feel uncomfortable with supplying such personal information to gain access to information. It would be crucial to provide sufficient lead time for users to become accustomed with the device and aware of what information is being recorded and not recorded.

Summary

Biometric technologies are currently deployed in a wide range of mission-critical government and commercial applications. Due to its wide range of functionality, biometric technology can be utilized in a number of applications to provide an added level of security and convenience beyond that of conventional security methods. Additionally, biometrics can be implemented in parallel with legacy systems to enable a gradual transition from conventional security systems to enhanced biometric security. As seen from previous deployments, some biometric modalities better serve one application than another; limiting factors include environment, size, and end-user compliance. Though each application serves its own purpose, applying biometrics achieves the

overarching goal of accurately identifying or verifying an individual's identity while enhancing security, efficiency, and/or convenience.

Related Entries

- ▶ [Access Control, Logical](#)
- ▶ [Access Control, Physical](#)
- ▶ [Law Enforcement](#)
- ▶ [Surveillance](#)
- ▶ [Time and Attendance](#)

References

1. C. Lee, S. Lee, J. Kim, S. Kim, Preprocessing of a fingerprint image captured with a mobile camera. Biometrics Engineering Research Center, Korea, 2005
2. H. Lu, K. Plataniotis, A. Ventsanopoulos, Uncorrelated multilinear discriminant analysis with regularization for gait recognition. The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, Canada (2007)
3. M. Arnold, C. Busch, H. Ihmor, *Investigating Performance and Impacts on Fingerprint Recognition Systems* (United States Military Academy, New York, 2005)
4. H. Sellahewa, S. Jassim, Wavelet based face verification for constrained platforms, in *Proceedings of SPIE 5779*, Florida, 2005

Biometric Data Interchange Format, Standardization

Christoph Busch^{1,2} and Greg Cannon³

¹Fraunhofer-IGD, Darmstadt, Germany

²Gjøvik University College, Gjøvik, Norway

³Cross Match Technologies, Palm Beach Gardens, FL, USA

Synonyms

Biometric data interchange format; Biometric data interchange record (BDIR); Biometric reference

Definition

Biometric data interchange formats define an encoding scheme according to which biometric data is stored in a **biometric reference**. In most cases the stored data will be used in future comparisons with biometric data stemming from the same or different subjects. Encoded data should contain not only a digital representation of a **biometric characteristic** (e.g., fingerprint image, face image) but also relevant metadata that impacted the capturing process (e.g., resolution of the fingerprint sensor). Standardized data interchange formats are a fundamental precondition to implement open systems where biometric data can be processed with components of different suppliers.

Introduction

Biometric systems are characterized by the fact that essential functional components are usually dislocated. While the enrolment may take place as part of an employment procedure in a personal office or at a help desk, the biometric verification often takes place at different location and time. This could occur when the claimant (the data subject) approaches a certain physical access gate or requests logical access to an IT system. No matter whether the recognition system operates in verification or identification mode, it must be capable to compare the probe biometric data captured from the subject with the stored reference data. Applications vary in the architecture, especially with respect to the storage of the **biometric reference**. Some applications store the reference in a database (either centralized or decentralized), while other applications utilize token-based concepts like the ePassport [1] in which subjects keep control of their personal biometric data as they decide themselves whether and when they provide the token to the controlling instance [2].

Given the expected complexities in system architecture, the use of open standardized formats is highly recommended as a best practice. While closed systems that are dedicated to specific applications – say access control to

a critical infrastructure – could be designed on proprietary format standards, any open system implementation requires the use of an interoperable, open standard to allow for enrolment and recognition components to be supplied from different vendors. The selection of a proprietary technology from one single vendor could add significant risk, where multiple issues (either technology or economic) could cause system failure to guarantee service. The Indian UIDAI is a good example for the benefits of standards to a large-scale biometric deployment process. Furthermore, sometimes it is desired that the same **biometric reference** could be used in different applications: It may serve as a trusted traveler document or as ID for eGovernment applications. Applications that may be quite different in nature will require the biometric data to be encoded in one harmonized record format. Due to the nature of the different **biometric characteristics** being observed, an extensive series of standards is required. Some biometric systems measure stable biological characteristics of the individual that reflect anatomical and physiological structures of the body. Examples of these types are facial or hand characteristics. Other biometric systems measure dynamic behavioral characteristics, usually by collecting measured samples over a given time span. Examples are signature/sign data that is captured with digitizing tables or advanced pen systems or voice data that is recorded in speaker recognition systems. The ISO/IEC JTC1/SC37 series of standards known as ISO/IEC IS 19794 (or the 19794 family) meets this need. This multipart standard includes currently 14 parts and covers a large variety of biometric modalities ranging from finger, face, iris, signature, hand geometry, 3D face, voice to DNA data.

A data package containing biometric data that claims to be in the form conformant to ISO/IEC 19794 is considered as a **biometric data interchange record (BDIR)**. Several applications such as the ICAO ePassport encapsulate the BDIR furthermore in a data container, the Common Biometric Exchange Format Framework (CBEFF) [3]. In this case the BDIR is denoted as a **Biometric Data Block (BDB)** and its concept is described

in the CBEFF standard. CBEFF containers provide additional functionality such as integrity protection of the data through digital signatures or the storage of multiple recordings from various **biometric characteristics** in one data record. Thus, the CBEFF container is also appropriate to represent data for multimodal biometric systems. The CBEFF standard is a component of the SC37 layered set of data interchange and interoperability standards.

Format Structures

The prime purpose of a **biometric reference** is to represent a **biometric characteristic**. This representation must allow a good biometric performance when being compared to a probe sample as well as allowing a compact coding as the storage capacity for some applications (e.g., the RFID token with 72 KB) may be limited. A further constraint is that the encoding format must fully support the interoperability requirements. Thus, encoding of the **biometric characteristic** with a two-dimensional digital representation of, for example, a fingerprint image, face image, or iris image is a prominent format structure for many applications. The image itself is stored in standardized formats that allow high compression ratio. Facial images are stored according to JPEG, JPEG2000. For fingerprint images a Wavelet Scalar Quantization (WSQ) has been proven to be a highly efficient encoding. It can be shown that a 300 KB image can be compressed to a 10 KB WSQ file without compromising the biometric performance [4]. Compression formats such as JPEG2000 furthermore can encode a specific region of interest in higher quality using limited compression and more aggressively compress the remainder background image. A good example is the encoding of the iris in high resolution, while all other areas of the image such as the lids may essentially be masked out. In such a case images can be compressed down to 2,5 KB and still yield an acceptable performance [5].

Nonetheless, smart card-based systems such as the European Citizen Card [6] or the US PIV Card [7] require not only a further reduction of

the format size but also a good computational preparation of the comparison step especially in environments with low computational power. On-card comparison is an efficient concept to realize privacy protection: The relevant concept is that the **biometric reference** is not disclosed to the potentially untrusted recognition system. Hence, the probe sample is provided to the card and comparison and decision are performed by the trusted smart cards. Samples are encoded in template format, as a vector of individual features that were extracted from the captured biometric sample. This process is quite transparent as, for example, in the fingerprint analysis: The essential features of a fingerprint are minutia locations (ridge endings and ridge bifurcations) and directions and potentially extended data such as ridge count information between minutia points. This data is relevant information for almost every fingerprint comparison subsystem, and standardizing a minutia format was a straightforward process [8].

These feature-based format standards encode the structured information only – none of the various concepts and algorithms that extract minutia points have been included in the standardization work. Many approaches for these tasks have been published in the academic literature; nevertheless, solutions in products are considered as intellectual property of the suppliers and are therefore usually not disclosed.

Furthermore, it became necessary to cope with different cultures in identifying minutia points. Thus, minutia definitions based on ridge ending versus definitions based on valley skeleton bifurcations became subtypes of the standard. While these ambiguities cover the variety of approaches of industrial implementations, an impressive interoperability can still be achieved, as it was proven in two independent studies [9, 10].

Requirements from biometric recognition applications are quite diverse: Some applications are tuned on high biometric performance (low error rates) in an identification scenario. Other applications are tuned to operate with a low capacity token in a verification scenario. Where database systems are designed, the record format subtype is the appropriate encoding. In other applications

the token capacity may be extremely limited and thus the card format subtype that exists in ISO/IEC IS 19794 for the fingerprint data formats in Part 2, 3, and 8 is the adequate encoding. Other parts such as 19794-10, which specifies the encoding of the hand silhouette, have been designed to serve implementations that are constrained by storage space. In general the concept of compact encoding with the card format is to reduce the data size of a BDIR down to its limits. This can be achieved when necessary parameters in the metadata are fixed to standard values, which makes it obsolete to store the header information along with each individual record.

For all data interchange formats, it is essential to store along with the representation of the **biometric characteristic** essential information (metadata) on the capturing processing and the generation of the sample. Note that in the case of the card format subtype, fixed values may be required as discussed above. Metadata that is stored along with the biometric data (the biometric sample at any stage of processing) includes information such as size and resolution of the image (e.g. a fingerprint image) but also relevant data that impacted the data capturing process: Examples for such metadata are the Capture Device Type ID that identifies uniquely the device that was used for the acquisition of the biometric sample and also the impression type of a fingerprint sample, which could be a plain live scan, a rolled live scan, non-live scan, or stemming from a swipe sensor.

For biometric systems, the quality of the biometric sample is essential information that estimates how useful the data is for future recognition tasks. Quality information must be encoded in the metadata. Biometric systems utilize quality for a number of different reasons. Quality is used to improve captured biometric characteristics, especially when giving rapid feedback to users to help them cooperate for better capture. Quality is utilized to improve biometric fusion for multimodal systems. Quality is measured to provide metrics for capture system maintenance, operator training, and user habituation. In general an overall assessment of the sample quality is stored on a scale from

0 to 100, while some formats allow additional local quality assessment such as the fingerprint zonal quality data or minutia quality in various fingerprint encoding standards [8, 11]. The rationale behind this quality recording is to provide information that might weigh into a recapture decision or to drive a failure to acquire decision. A biometric system may need to exercise quality control on biometric samples, especially enrollment, to assure strong performance, especially for identification systems. Multimodal comparison solutions can utilize quality to weight the decisions from the various comparison subsystems to improve biometric performance. Details on how to combine and fuse different information channels can be found in the ISO/IEC technical report on multibiometric fusion [12]. A local quality assessment may also be very meaningful as environmental factors such as different pressure, moisture, or sweat may locally degrade the image quality of a fingerprint and thus degrade biometric performance.

According to ISO/IEC 19794-1:2011 [13], the metadata in an ISO/IEC data interchange format is subdivided into information related to the entire record which is stored in the general header and specific information related to one individual representation (i.e., a view for a fingerprint system), which is stored in the representation

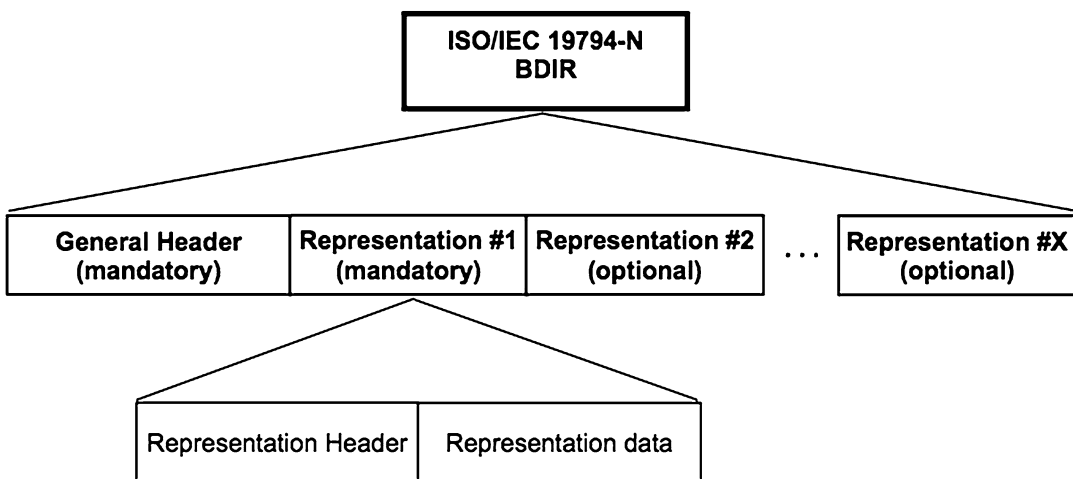
header. The existence of multiple representations is of course dependent on the application and the respective modality used. In the case of a fingerprint recognition system, it is a common approach – in order to achieve a higher recognition performance – to store multiple representations such as right and left index finger together as separate representation in one BDIR.

The general structure of ISO/IEC data interchange format standards is:

1. General header
2. Representation 1 (mandatory)
 - (a) Representation header
 - (b) Representation data
3. Representations 2 to N (optional)
 - (a) Representation header
 - (b) Representation data

This structure was not implemented in all parts of ISO/IEC 19794 in the first generation (G1) that was issued back in the year 2005. But harmonization in this regard was achieved in the revision process of these standards, which was completed in 2011 leading to the second generation (G2) of these standards (Fig. 1).

Common elements of the general header are the format identifier, the version number of the standard, the length of the record, the number of representations in the record, and the certification flag. The purpose of the flag is to indicate whether



Biometric Data Interchange Format, Standardization, Fig. 1 Example structure of a multiple-representation BDIR (Source: ISO/IEC 19794-1:2011)

the following representation headers will contain information about certification of the capture device that generated the sample.

Elements of the representation header are dependent on the modality in use. Mandatory elements such as representation length, capture data and time in Coordinated Universal Time (UTC), and the capture device technology identifier shall indicate the class of capture device technology used to acquire the captured biometric sample (e.g., for fingerprint systems one class is *white light optical TIR*). Typical additional represented information for a biometric fingerprint sample includes the finger position (right thumb, right index finger, ..., left index finger, ..., left little finger), the representation number (in the record), impression type (Live-scan plain, Live-scan rolled, etc.), finger quality, and number of minutia.

Often, the mere specification for the encoding of the biometric data and the metadata is not enough to assure interoperability. For some biometric modalities, the context of the capture process is also important, and best practices for the capture procedures of the **biometric characteristics** are described in the standards. The capture of face images suitable for biometric comparison is described in an informative Annex to ISO/IEC IS 19794-5:2011 [14]. This amendment provides suitable constraints for illumination, backgrounds, and how to avoid shadows on the subject's face. Other standards include similar information.

Published Standards

After the international committee for biometric standardization, SC37, was founded in 2002 (ISO/IEC JTC 1 on Information Technology Subcommittee 37 on Biometrics (<http://www.jtc1.org>)), the first standards were already published after an extremely short preparation period in the summer of 2005. These standards are named first generation (G1) and do cover the most common modalities (Fig. 2).

The second generation of data interchange formats was developed in 2007 in order to achieve

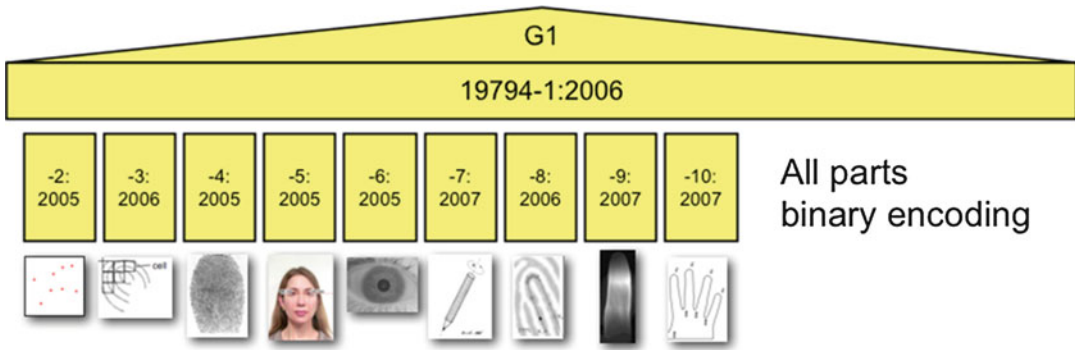
better harmonization among parts and also to cover more modalities and innovative encoding schemes such as XML (Fig. 3).

Standardization in the field of information technology is pursued by a Joint Technical Committee (JTC) formed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). An important part of the JTC1 SC37 subcommittee's activities is the definition of data interchange formats in its Working Group 3 (WG3) as described in the previous section. WG3 has concentrated on the development of the ISO/IEC 19794 family, which includes currently the following 14 parts:

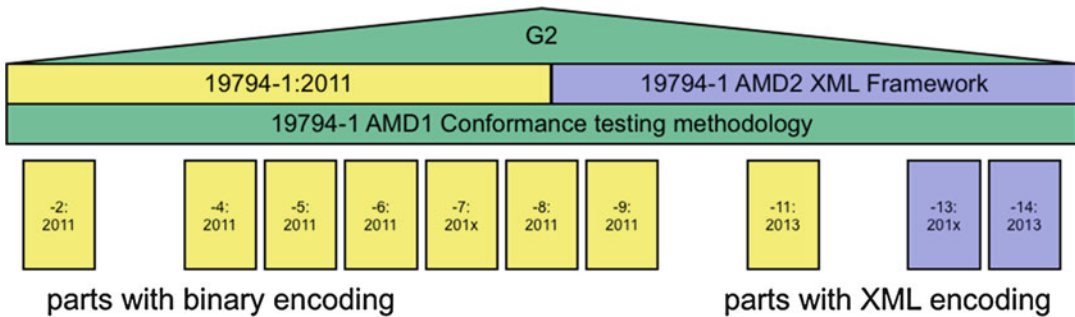
- Part 1: Framework (IS)
- Part 2: Finger minutiae data (IS)
- Part 3: Finger pattern spectral data (IS)
- Part 4: Finger image data (IS)
- Part 5: Face image data (IS)
- Part 6: Iris image data (IS)
- Part 7: Signature/sign time series data (IS)
- Part 8: Finger pattern skeletal data (IS)
- Part 9: Vascular image data (IS)
- Part 10: Hand geometry silhouette data (IS)
- Part 11: Signature/sign processed dynamic data (WD)
- Part 12: – Void –
- Part 13: Voice data (WD)
- Part 14: DNA data (WD)
- Part 15: Palm line image data (new project)

The first part [13] includes relevant information that is common to all subsequent modality-specific parts such as an introduction of the layered set of SC37 standards and an illustration of a general biometric system with a description of its functional subsystems, namely, the capture device, signal processing subsystem, data storage subsystem, comparison subsystem, and decision subsystem. Furthermore, this framework part illustrates the functions of a biometric system such as enrolment, verification, and identification and explains the widely used context of biometric data interchange formats in the CBEFF structure.

Part 2 to Part 15 then detail the specification and provide modality-related data interchange formats for both image interchange and template interchange on feature level. The 19794 family



Biometric Data Interchange Format, Standardization, Fig. 2 First generation of biometric data interchange formats



Biometric Data Interchange Format, Standardization, Fig. 3 Second generation of biometric data interchange formats

gained relevance, as the International Civil Aviation Organization (ICAO) adopted image-based representations for finger, face, and iris for storage of **biometric references** in electronic passports [14–16]. Thus, the corresponding ICAO standard 9303 includes a normative reference to ISO/IEC 19794 [17].

Another relevant standard for the global exchange of biometric data has been developed by the National Institute of Standards and Technology (NIST) as American National Standard [18]. This data format is the de facto standard for the interchange of fingerprint and facial information for forensic purposes among criminal police institutions. It is also intended to be used in identification or verification processes. This standard supports fingerprint images, fingerprint minutia, iris images, face images, as well as support for any CBEFF encapsulated biometric data.

The American and Japanese standardization committees are developing national standards

in parallel to the SC37 international standards. Many of the projects inside SC37 had been initiated by and received significant support from national standard developments. However, with the full constitution of SC37 as one of the most active and productive committees inside the JTC1, many national standardization committees – and essentially all European countries – have stopped the development of pure national standards. Most of the available resources are now focused and invested in the development and procurement of international standards with the JTC1.

Interoperability and Future Needs

With the current set of data format standards open, biometric systems can be developed, which can provide interoperability among suppliers. However, as the prime purpose

of a biometric system is to achieve a good recognition performance, a core objective is to achieve a good interoperability performance, e.g., the performance associated with the use of a generator and comparison subsystems from different suppliers. This goal of good interoperability performance can be achieved when conformance of each supplier to the data form standard is reached. The concept of conformance testing supports customers and suppliers. A conformance testing protocol verifies that data records generated by an implementation are compliant to the standard. Testing can be subdivided in three levels:

1. Data format conformance: Proof that data fields specified in a data format standard do exist and are filled in a consistent manner. The result of this test indicates whether all fields are included and values in those fields are in the defined range. This check is conducted on a field-by-field and byte-by-byte operation and is often referred to as “level 1 conformance testing.”
2. Internal consistency checking: In the second level of conformance Testing, the data record is tested for internal consistency, such as relating values from one field of the record to other parts or fields of the record are conformant. This test is often referred to as “level 2 conformance testing.”
3. Semantic conformance: In the third level of conformance testing, the values in the data fields are investigated whether or not they are faithful representation of the **biometric characteristic**, e.g., for a fingerprint image whether minutia points identified are indeed bifurcation or end points of papillary ridges. The test requires standardized sample data on the one hand and elaborated semantic conformance tests on the other that are yet in an early state and not maturely developed.

Along with the definition of conformance testing standards, the standardization of sample quality standards is the most important and pressing work to be solved in SC37. The standardization or calibration of quality scores is important as it

allows for increased interoperability of reference data. The system that utilizes a **biometric reference** enrolled under a different quality policy may still be able to leverage that reference if it can understand and make use of the quality information relevant to that **biometric reference**. Thus, the quality standards and technical reports provide guidance to assure interoperability. The technical reports provide guidance about what is relevant to comparability that should be measured for a given **biometric characteristic**. Currently, quality standardization exists for an overall framework, along with guidance for fingerprint images and face images.

The SC37 standards community also currently amends the G2 standards with an encoding scheme for XML, which allows more flexible encoding and is required by manifold applications.

Related Entries

- ▶ [Biometric System Design, Overview](#)
- ▶ [Common Biometric Exchange Formats Framework Standardization](#)
- ▶ [Finger Data Interchange Format, Standardization](#)
- ▶ [Hand Data Interchange Format, Standardization](#)
- ▶ [Iris Image Data Interchange Formats, Standardization](#)
- ▶ [Speaker Recognition, Overview](#)
- ▶ [Conformance Testing Methodologies for Biometric Data Interchange Formats, Standardization of](#)
- ▶ [Vascular Image Data Format, Standardization](#)

References

1. International Civil Aviation Organization, *Machine Readable Travel Documents – Volume I*. Document 9303, 6th edn. (International Civil Aviation Organization, Montreal, 2006)
2. EU-Council Regulation No 2252/2004 – of 13 December 2004 on standards for security features and

biometrics in passports and travel documents issued by Member States

3. ISO/IEC JTC 1 SC 37, ISO/IEC 19785-1, Information technology – common biometric exchange formats framework – part 1: data element specification (2006)
4. F. Funk, M. Arnold, C. Busch, A. Munde, Evaluation of image compression algorithms for fingerprint and face recognition systems, in *Proceedings from the Sixth IEEE Systems, Man Cybernetics (SMC): Information Assurance Workshop of Systems, Man and Cybernetics*, West Point (IEEE Computer Society, 2005), pp. 72–78
5. J. Daugman, C. Downing, Effect of severe image compression on iris recognition performance. Technical report, no. 685, University of Cambridge, 2007. ISSN 1476-2986
6. European Citizen Card, CEN TC 224 WG 15: identification card systems
7. National Institute of Standards and Technology, Biometric Data Specification for Personal Identity Verification. NIST Special Publication 800-76-1 (2007), http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf
8. ISO/IEC JTC 1 SC 37, ISO/IEC IS 19794-2:2011, Information technology – biometric data interchange formats – part 2: finger minutia data (2011)
9. National Institute of Standards and Technology, MINEX – performance and interoperability of the INCITS 378 fingerprint template (2006), http://fingerprint.nist.gov/minex04/minex_report.pdf
10. The Minutia Template Interoperability Testing Project MTIT (2007) <http://www.mtitproject.com>
11. ISO/IEC JTC 1 SC 37, ISO/IEC IS 19794-8:2011, Information technology – biometric data interchange formats – part 8: finger pattern skeletal data (2011)
12. ISO/IEC JTC 1 SC 37, ISO/IEC TR 24722, Multimodal and other multibiometric fusion (2007)
13. International Standards ISO/IEC IS 19794-1:2011, Information technology – biometric data interchange formats – part 1: framework (2011)
14. ISO/IEC JTC 1 SC 37, ISO/IEC IS 19794-5:2011, Information technology – biometric data interchange formats – part 5: face image data (2011)
15. ISO/IEC JTC 1 SC 37, ISO/IEC IS 19794-6:2011, Information technology – biometric data interchange formats – part 6: iris image data (2011)
16. ISO/IEC JTC 1 SC 37, ISO/IEC IS 19794-4:2011, Information technology – biometric data interchange formats – part 4: finger image data (2011)
17. International Civil Aviation Organization, Supplement to Doc9303-part 1, 6th edn. (2006)
18. National Institute of Standards and Technology, ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290, American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136

Biometric Identity Assurance Services

Kevin Mangold¹ and Matthew Swayze²

¹National Institute of Standards and Technology, Gaithersberg, MD, USA

²Daon, Inc., Reston, VA, USA

Synonyms

BIAS

Definition

Biometric Identity Assurance Services, or BIAS, is a collaborative standards project between the International Committee for Information Technology Standards (INCITS), Technical Committee M1-Biometrics and the Organization for the Advancement of Structured Information Standards (OASIS). BIAS provides an open framework for deploying and invoking biometric-based identity assurance capabilities that can be readily accessed using services-based frameworks. BIAS services provide basic biometric identity assurance functionality as modular and independent operations that can be assembled in many different ways to perform and support a variety of business processes.

Introduction

In reviewing the current biometric-related standards portfolio and service-oriented architecture (SOA) references, it became apparent that a gap exists in the availability of standards related to biometric services. There are several existing biometric-related standards describing how to format either biometric data specifically or transactions containing identity information (including biometric information) for use in a particular application domain. However, these standards do not readily fit into an SOA. As enterprise architectures are increasingly built on SOA models and standards, biometric

applications, such as those that perform biometric capture functions, require a consistent set of services to access other biometric-based resources. In this context, a biometric resource could be a database with biometric information, a one-to-many search engine, or a system that performs one-to-one verifications. BIAS seeks to fill the gap by standardizing a set of biometric-based identity assurance capabilities that applications can invoke remotely across a services-oriented framework in order to access these biometric resources.

Scope

Although focused on biometrics, BIAS recognizes that there are nonbiometric elements to an identity. While the services have been built around biometric-related operations, nonbiometric information can be referenced in several of the service calls. BIAS services do not prescribe or preclude the use of any specific biometric type. BIAS is primarily focused on remote service invocations, and therefore, it does not deal directly with any local biometric devices. Recognizing the need for vendor independence, BIAS attempts to be technology, framework, and application domain independent.

BIAS establishes an industry-standard set of predefined and reusable biometric identity management services that allow applications and systems to be built upon an open-system standard rather than implementing custom one-off solutions for each biometric resource. BIAS defines basic biometric-related business-level operations, including associated data definitions, without constraining the application or business logic that implements those operations. The basic BIAS services can be assembled to construct higher-level, composite operations that support a variety of business processes.

INCITS and OASIS Collaboration

The development of the BIAS standard requires expertise in two distinct technology domains:

biometrics, with standards leadership provided by INCITS M1 [1], and service architectures, with standards leadership provided by OASIS [2]. The two groups are collaborating to produce two associated standards. The INCITS M1 standard [3] defines biometric services used for identity assurance, which are invoked over a services-based framework. It is intended to provide a generic set of biometric (and related) functions and associated data definitions to allow remote access to biometric services. The related OASIS standard [4] specifies a set of patterns and bindings for the implementation of BIAS operations (which are defined in the INCITS M1 standard) using Web services and service-oriented methods within XML-based transactional Web services and service-oriented architectures.

Existing standards are available in both fields, and many of these standards provide the foundation and underlying capabilities upon which the biometric services depend. The INCITS standard leverages the existing biometric and identity-related standards and formats. The OASIS standard leverages known information exchange and assurance patterns (such as message reliability acknowledgments), and functions (such as repository use and calls) arising in service-oriented systems, and potentially leverages those functions and features that are already embedded in existing SOA methods and standards.

Currently, the INCITS M1 standard has been published as INCITS 442. The OASIS standard, which depends on the INCITS M1 standard, is still in draft form in the OASIS technical committee and is expected to be finalized in 2009.

Architecture [5, 6]

The BIAS architecture consists of the following components: BIAS services (interface definition), BIAS data (schema definition), and BIAS bindings. The BIAS services expose a common set of operations to external requesters of these operations. These requesters may be an external system, a Web application, or an intermediary. The BIAS services themselves are platform and language independent. The BIAS services may be

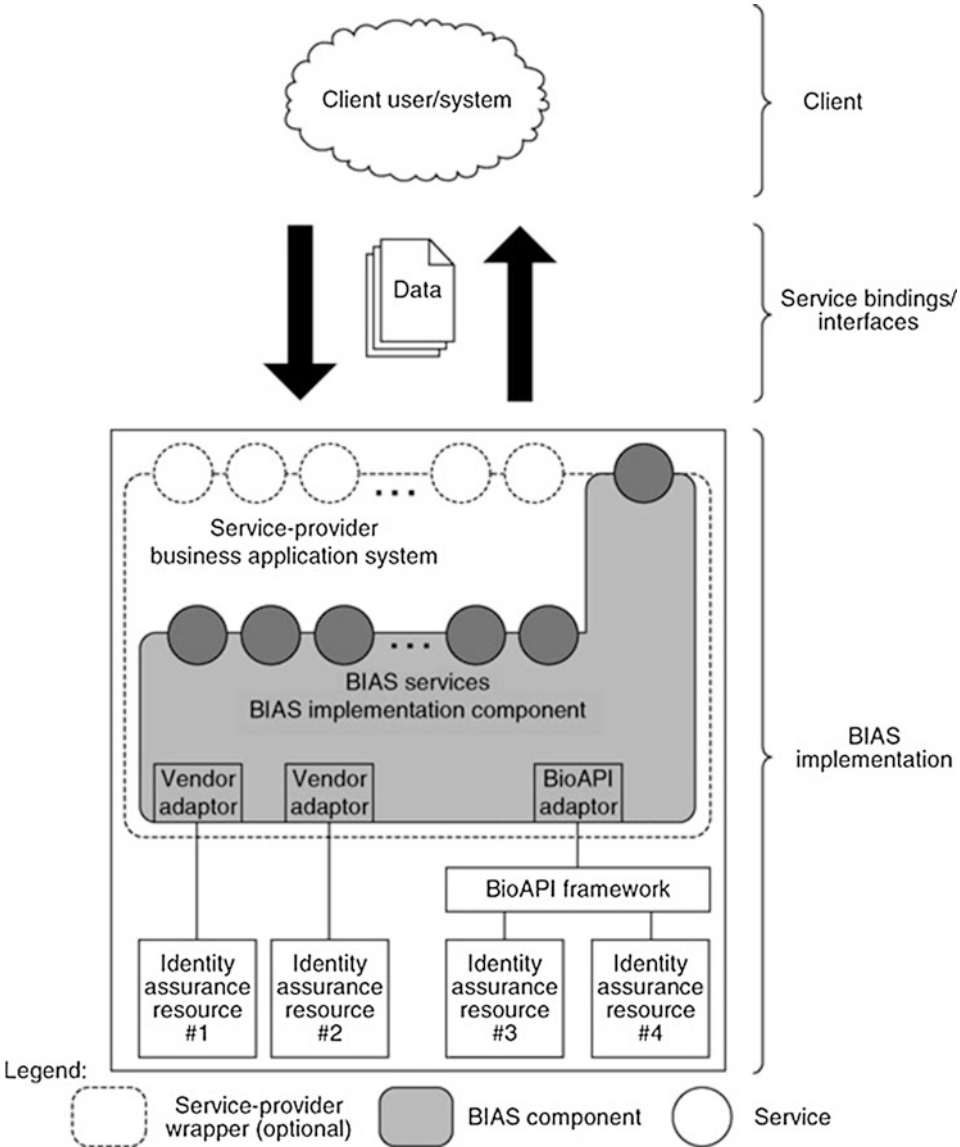
implemented with differing technologies on multiple platforms. For example, OASIS is defining Web services bindings for the BIAS services.

Figure 1 depicts the BIAS services within an application environment. BIAS services provide basic biometric functionality as modular and independent operations that can be publicly

exposed directly and/or utilized indirectly in support of a service-provider’s own public services.

Services

BIAS defines two categories of services: primitive and aggregate. Primitive services are basic,



Biometric Identity Assurance Services, Fig. 1 BIAS application environment. ITIC. This material is reproduced from INCITS 422-2008 with permission of the American National Standards Institute (ANSI) on behalf of the Information Technology Industry Council (ITIC). No part of this material may be copied or reproduced

in any form, electronic retrieval system or otherwise, or made available on the Internet, a public network, by satellite, or otherwise without the prior written consent of the ANSI. Copies of this standard may be purchased from the ANSI, 25 West 43rd Street, New York, NY 10036, (212) 642-4900, <http://webstore.ansi.org>

B

lower-level operations that are used to request a specific capability. Aggregate services operate at a higher level, performing a sequence of primitive or other operations in a single request. An example of an aggregate service would be where a one-to-many search (identify), which results in a “no match,” is immediately followed by the addition of the biometric sample into that search population (enroll).

BIAS provides primitive services for the following areas:

1. Manage subject information: adding or deleting subjects or associating multiple subjects into a single group
2. Managing biographic information: adding, updating, deleting, or retrieving biographic information on a particular subject
3. Managing biometric information: adding, updating, deleting, or retrieving biometric information on a particular subject
4. Biometric searching/processing: performing biometric one-to-one or one-to-many searches, checking biometric quality, performing biometric fusion, or transforming biometric data from one format to another

BIAS also defines several aggregate services. The intent of BIAS is to standardize the service request; organizational business rules will determine how the service is actually implemented. The standard aggregate services include enroll, identify, verify, and retrieve information.

Summary

The BIAS standard represents the first collaboration between INCITS M1 and OASIS, bringing these two organizations together to define a set of standardized biometric services that can be invoked within a services-oriented framework. The services are defined at two levels and correspond to basic biometric operations. BIAS is technology and vendor independent, and therefore, it may be implemented with differing technologies on multiple platforms.

References

1. INCITS M1 – Biometrics, http://www.incits.org/tc_home/m1.htm. Last Accessed 02 Apr 2009
2. OASIS, <http://www.oasis-open.org/home/index.php>. Last Accessed 02 Apr 2009
3. ANSI INCITS 442-2008, Biometric Identity Assurance Services (BIAS), May 2008, <http://www.incits.org>. Last Accessed 02 Apr 2009
4. OASIS BIAS SOAP Profile (Draft), <http://www.oasis-open.org/committees/bias>
5. Service-oriented architecture: beyond web services. Java Dev. J. http://java.sys-con.com/read/44368_p.htm. Accessed Feb 2006
6. Reference model for service-oriented architecture 1.0, OASIS, <http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf>. Accessed Feb 2007

Biometric Interfaces

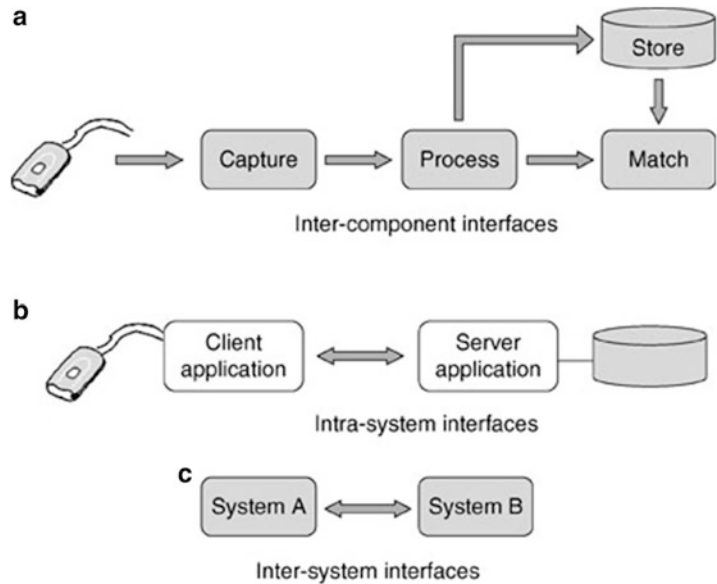
Catherine J. Tilton
Standards & Technology, Daon, Reston,
VA, USA

Definition

Biometric interfaces comprise the methods by which one biometric system component communicates with another. These components may be devices, software, or entire systems. Implied in this definition is the exchange of information – generally that of biometric data. Interfaces are key elements of biometric system architecture and design and provide the basis for interoperability.

Introduction

Biometric systems are composed of subsystems and components, the configuration and inter-relationship of which describe the system architecture. For the system to function, these components must interact with one another across intrasystem interfaces. The system itself may be a part of a larger “system of systems” in which

Biometric Interfaces,**Fig. 1** Interface types and levels

intersystem interfaces also exist. In a biometric (or biometrically enabled) system, the interface involves the exchange of biometric data or the invocation of biometric services.

Biometric interfaces exist at a variety of levels – from low-level internal interfaces within a capture device, for instance, to intersystem messaging interfaces, such as between law enforcement systems in different countries (Fig. 1).

The biometric process involves a series of steps, including data collection (capture), processing (feature extraction), storage, and matching depending on the operation (i.e., enrollment, verification, or identification). Biometric data may be transferred between components performing these operations or to an application controlling or using the results of the operation. A biometric interface exists whenever biometric data is transferred from one system component to another, internally or externally. The following sections describe data interchange, device interfaces, application programming interface and communications, and messaging interfaces.

Data Interchange

Biometric data may exist in a variety of forms – “raw” biometric sample data captured by a sensor

device, partially processed data (e.g., a biometric sample that has undergone a degree of image processing), or a fully processed biometric reference template or recognition sample suitable for matching. Likewise, this data may be formatted and encoded in different ways. An image, for example, can be compressed or uncompressed. Biometric data may exist as a single sample or be packaged together with other like or unlike samples from the same individual. It may exist in a proprietary format or in a standard format, with or without associated metadata.

Whenever data is exchanged between components or systems, the format and encoding of that data must be understood by both the sending and the receiving entities. This implies that the format information is defined in a document of some type. If both ends of the interface are owned/controlled by the same entity (e.g., a device manufacturer), then the definition may be less formal or be contained within some larger specification. As the relationship between the end points becomes more loosely coupled, more formal and rigorous data definitions are needed.

In a closed system, the data format can be whatever works. It can be highly customized and proprietary. In open systems, however, data formats need to be standardized so that they can be understood by a wide variety of producers and

consumers of biometric data. Today, data interchange format standards exist for most modalities, although at the raw/image levels. Standard template formats exist only for fingerprint biometrics.

In addition to the biometric data itself, standards exist for encapsulating (“packaging”) that data. This includes defined structures, standard metadata headers, and security information. Examples of such standards are the Common Biometric Exchange Formats Framework (CBEFF) and ANSI/NIST ITL1-2007 [1,2].

More information on data interchange standards can be found in the chapter on Standardization.

Device Interfaces

Biometric sensor devices capture biometric data and sometimes provide additional capabilities to process, store, and/or match it. For an application to integrate a biometric device, an interface to that device must exist and be defined. This includes the physical interface, the communications protocol, and the data/message exchange.

Physical interfaces to biometric devices generally utilize industry standards which define both the physical interface and communications protocols. Because biometric data samples (especially raw data such as images) can be very large, an interface that provides adequate speed and bandwidth is desirable. In the early days of electronic fingerprint scanners, IEEE 1284 parallel interfaces were the norm. Today, the Universal Serial Bus (USB) or IEEE 1394 (“FirewireTM”) are more commonly used. Some biometric sensors are commodity items such as cameras, microphones, or signature pads.

A common software interface for devices is TWAIN, whose purpose is to provide and foster a universal public standard which links applications and image acquisition devices. It supports image acquisition from a scanner, digital camera, or another device and imports it directly into an application. Many commodity devices provide TWAIN-compliant device drivers.

To interface to a biometric device from a software application, operating system (OS) support is required. This is generally accomplished via a “device driver.” Most devices provide WindowsTM device drivers; however, support for other platforms (such as Linux, Unix, OS2, etc.) is a bit more spotty.

In addition to the device drivers, biometric device manufacturers usually provide software developer kits (SDKs) to control and access the functionality of their device. Applications interface to SDKs via a defined application programming interface (API) as described in the following.

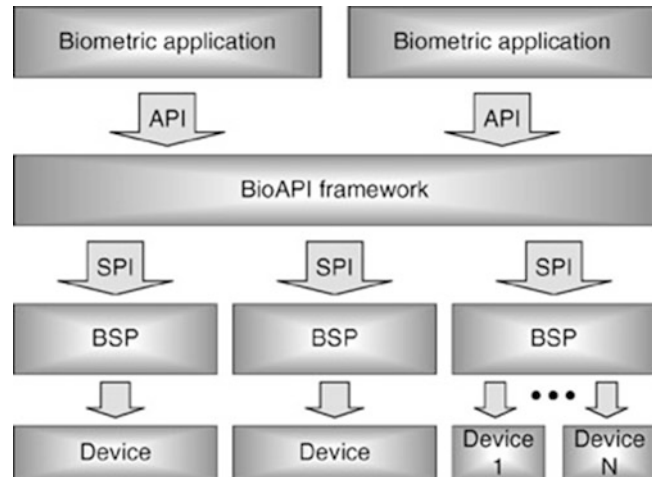
Software Interfaces

Biometric software modules are components that provide a set of biometric functions or capabilities via a software interface. This includes biometric processing and matching algorithms or control of a biometric device. Reusable software packages are called SDKs. Biometric SDKs with standardized interfaces are called biometric service providers (BSPs).

APIs can be either “high level” or “low level”. In terms of biometrics, a high-level API provides a set of more abstract, generalized functions (e.g., “Enroll”), whereas a lower-level API provides more specific, atomic functions (e.g., “Capture Fingerprint Image” or “Set Contrast”). The lower the level, the more modality- and even vendor/device-specific it is. An example of a low-level biometric API standard is the Speaker Verification API (SVAPI) developed in the mid-1990 and championed by Novell [3].

A software application interfaces to an SDK or BSP via an API. The first biometric SDKs appeared in the mid-1990. Most SDK APIs are vendor specific. They are defined by the manufacturer to be highly tailored to the features and capabilities of their product. The advantage of such APIs is that they can be very efficient and provide sophisticated controls. Standard biometric APIs also exist, which define a common interface definition for a category of services. This allows an application to be written once

Biometric Interfaces,
Fig. 2 BioAPI architecture



to the standard API and utilize any biometric SDK/BSP that conforms to the standard.

Early APIs were defined using “C” language constructs. However, more recently, the trend is to define object-oriented interfaces in terms of Java, .NET, or COM in order to be more easily integrated into object-oriented applications.

The most well-known biometric API is the BioAPI. This standard was originally developed by a group of over 100 organizations from industry, government, and academia and published in 2000 as an open systems industry specification [4]. Subsequently, version 1.1 was published as an American National Standard (INCITS 358) and version 2.0 as an international standard (ISO/IEC 19784) [5,6].

The BioAPI interface defines a set of functions (and associated data structures), including biometric, database, and unit (device) operations; component management functions; utility functions; and data handle, callback, and event operations. High-level biometric operations such as enroll, verify, and identify are provided as well as more primitive operations such as capture, create template, process (feature extraction), verify match, identify match, and import. Conformance categories identify which functions and options are required for a given product class.

To perform module management functions, a BioAPI framework component is included as part of the API/SPI (service provider interface) architecture. This allows dynamic insertion and

control of BSPs and devices as well as a discovery mechanism (Fig. 2).

BioAPI is defined as a “C” interface, though a Java version is in progress. The version 1.1 framework has been ported to Win32, Linux, Solaris, and WinCE platforms, and a variety of wrappers (e.g., JNI, C#) have been developed.

Another “standard” biometric API is BAPI. This API was developed by I/O Software and later licensed to Microsoft, who included it in their XP Home Edition as the interface to their fingerprint device. This API originally provided three levels of interface – a high level similar to BioAPI, a mid-level, and a lower (device)-level interface. BAPI has not been made publicly available or formally standardized.

More recently, the Voice Extensible Markup Language (VoiceXML) was created for creating voice user interfaces that use automatic speech recognition (ASR) and text-to-speech synthesis (TTS). It was developed by the VoiceXML Forum and published by the W3C. “VoiceXML simplifies speech application development by permitting developers to use familiar Web infrastructure, tools and techniques. VoiceXML also enables distributed application design by separating each application’s user interaction layer from its service logic.” [7] An extension to VoiceXML called Speaker Identification and Verification (SIV) is in progress [8].

In addition to group-developed APIs, there have been biometric APIs developed

by application and middleware vendors. The latter standardize an interface to their particular product or product line. In this case, the application/middleware vendor defines an interface such that any biometric technology vendor wishing to be integrated (or resold) with that application must conform to the application vendor's API. It may be a biometric-specific API or a more general "authentication method" API. While this has been successful to some extent, the drawback is that the technology vendors must provide different flavors of their SDK for each such application, which may become difficult to maintain.

Communications and Messaging Interfaces

When biometric information is passed between systems or subsystems, a communications or messaging interface may be used. This is generally defined in terms of message content and protocol. The best known are those used by the justice community. The FBI's Electronic Fingerprint Transmission Specification (EFTS) and the Interpol Implementation (INT-I) both utilize the ANSI/NIST ITL1-2000 standard to define transactions (request and response messages) with their respective systems [2, 9, 10] (note that the EFTS and ANSI/NIST standards have recently been revised; however, at the time of this article, they had not yet been implemented. Interpol is expected to follow suit) [11, 12].

ANSI/NIST ITL1-2000/2007 defines the content, format, and units of measurement for electronically encoding and transmitting fingerprint, palmprint, facial/mugshot, and SMT images and associated biographic information. It consists of a series of "record types," each containing a particular type and format of data. For example, a Type-4 record contains a high-resolution grayscale fingerprint image, a Type-9 record contains minutiae data, a Type-10 facial or SMT images, a Type-14 variable-resolution tenprint images, etc. An XML version of the 2007 standard was recently released [13].

EFTS and INT-I define transactions in terms of these records and further define the content of "user-defined fields." For example, EFTS defines a type of transaction (TOT) called a CAR (Criminal Tenprint Submission, Answer Required) that "contains ten rolled and four plain impressions of all ten fingers, as well as information relative to an arrest or to custody or supervisory status and optionally may include up to 4 photos of the subject." [8] It nominally consists of a Type 1 (header), a Type 2 (descriptive text), 14 Type-4, and 0-4 Type-10 records.

Services Interfaces

Today's biometric systems are being built upon what is commonly referred to as a "service-oriented architecture (SOA)." In an SOA, requesting applications/systems are decoupled from those systems which provide biometric services and allow biometric operations to be invoked and resources to be accessed remotely, usually across an open or closed network, including the Internet. These service interfaces may be customized or standardized.

The most often used protocols for such services are XML over Hypertext Transmission Protocol (HTTP) or Simple Object Access Protocol (SOAP) over HTTP. SOAP services are defined in terms of Web Services Definition Language (WSDL) and frequently utilize a set of existing web service standards. Service providers may post their WSDL to a directory which can be read by potential users or, in closed systems, may be provided directly to known requesters.

A service provider offers a set of remote biometric services such as biometric data storage and retrieval, 1:1 face verification, or 1:N iris or fingerprint search/match. The requester invokes the operation by sending a service request with the associated data to the service provider. The service provider accepts the request, performs the operation, and returns the results as a service response (Fig. 3).

Although today most service interfaces are system specific, a project known as Biometric Identity Assurance Services (BIAS) is in progress

Biometric Interfaces,**Fig. 3** Biometric web services using BIAS

to standardize a set of generic biometric Web services. (See BIAS section of the Standardization chapter for more information.)

Summary

Biometric interfaces provide a means to exchange biometric data, perform data transactions, and invoke biometric services. This can occur at several different levels and between different types of biometrics and system components. All biometric interfaces involve transfer of biometric data and must be specified in some way. An interface definition may be proprietary, as is frequently done in closed systems, or standardized. Biometric interfaces are key aspects of the overall biometric system architecture and design.

Related Entries

- ▶ [BioAPI, Standardization](#)
- ▶ [Biometric Sensor and Device, Overview](#)
- ▶ [Biometric System Design, Overview](#)
- ▶ [Biometric Technical Interface, Standardization](#)

References

1. Common Biometric Exchange Formats Framework (CBEFF), INCITS 398-2008 and ISO/IEC 19785-1:2006
2. American National Standards Institute and National Bureau of Standards, ANSI/NIST ITL1-2000: Data Format for the Interchange of Fingerprint, Facial, and SMT Information
3. Speaker Verification API (SVAPI), SVAPI Working Group, originally published in 1997 with latest version 2004. <http://developer.novell.com/wiki/index.php/SRAPI> and SVAPI Source Code. [Note

also article by J. Markowitz Introduction to SVAPI at <http://www.jmarkowitz.com/downloads.html>.]

4. BioAPI Consortium website: <http://www.bioapi.org>
5. BioAPI Consortium, American National Standards Institute (ANSI) and International Council on Information Technology Standards: The BioAPI Specification, Ver. 1.1, INCITS 358-2002, Feb 2002
6. ISO/IEC 19784-1: Information technology – Biometric application programming Interface – Part 1: BioAPI specification, Ver. 2.0, 1 May 2005
7. VoiceXML Forum website: <http://www.voicexml.org>
8. W3C website: <http://www.w3.org/voice>
9. Federal Bureau of Investigation: Electronic Fingerprint Transmission Specification (EFTS), IAFIS-DOC-01078-7.1, May 2, 2005
10. Interpol AFIS Expert Group: Interpol Implementation of ANSI/NIST ITL1-2000, Version No. 4.22b, Oct 28, 2005
11. American National Standards Institute and National Bureau of Standards, ANSI/NIST ITL-1-2007: Data Format for the interchange of Fingerprint, Facial, and other Biometric Information – Part 1, Apr 2007
12. Federal Bureau of Investigation: Electronic Biometric Transmission Specification (EBTS), IAFIS-DOC-01078-8.1, Nov 2008
13. American National Standards Institute and National Bureau of Standards, ANSI/NIST ITL2-2008: Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information – Part 2: XML version, Aug 2008

Biometric Sample Acquisition

Dale Setlak

AuthenTec, Inc., Melbourne, FL, USA

Synonyms

Biometric data acquisition; Biometric data capture; Biometric front end; Biometric sensing; Fingerprint capture; Fingerprint reading; Fingerprint scan; Image capture; Iris capture; Iris scan

Definition

Biometric sample acquisition is the process of capturing information about a biological attribute of the subject, as it exists within a specific time frame. The objective is to measure data that can be used to derive unique properties of the subject that are stable and repeatable over time and over variations in acquisition conditions.

Typically, the capture process measures a physical property that is affected by the biological characteristic of interest and converts the measured data into a format that is suitable for analysis – typically a digital electronic format compatible with computerized analysis.

For simplicity, in this discussion, it is assumed that behavioral biometrics are biological attributes that have a temporal dimension and are included in the discussion as such.

In classic biometric systems such as criminology systems, there is a definitive separation (in both time and space) between biometric sample acquisition and the processing and matching of that sample. For example, an arresting officer may collect a suspect's fingerprints at a booking station in the sheriff's office. The fingerprints may then be sent to the FBI for processing and matching against a fingerprint repository. In contrast, real-time biometric ID verification systems, such as those used for log-in on a laptop computer, do not have that clear separation. In laptop computers, for example, the sample processing and matching will begin operating, while sample acquisition is still in progress. Information from those analyses can then be used to optimize the sample acquisition in real time, significantly improving the overall performance of the system, but blurring the separation between sample acquisition and the subsequent processes.

Introduction

This article will start out by examining the high-level requirements that apply generally to many types of biometric sample acquisition. The biometric sample acquisition process will then be

decomposed into its essential elements and each of those discussed briefly. It then examines how each of the essential elements is applied, using the fingerprint ridge pattern as the example biological property, and also examines the real-world implementation embodied in the recently popular fingerprint log-in systems on laptop computers. The article then reviews some of the new requirements imposed on biometric sample acquisition systems when they become essential elements of the secure, trusted computing, and communication systems that are needed by applications such as mobile commerce and mobile banking.

Generalized Requirements for Biometric Sample Acquisition

The fundamental requirements for the biometric sample acquisition process are driven by the needs of the biometric matching process. At the conceptual level, these requirements boil down to the following two:

- To be able to distinguish a large number of people from each other, a biometric property must contain a large amount of information entropy. In state space terms, the property must have a very large number of distinguishable states. As a result, most biometric characteristics are complex properties represented as arrays of information such as 2- or 3-dimensional images of biological structures (e.g., fingerprints) or segments of time series data (e.g., speech segments). Biometric sample acquisition then becomes the task of making a large number of measurements that have well-known interrelationships in space and/or in time, with sufficient resolution and accuracy to develop the required large measurement state space.
- To avoid failing to recognize a previously enrolled person, the biometric matching process needs repeatable detail among all the samples of the biometric property data. The key is minimizing sample variability. Ideally, the biometric sample acquisition system should capture the same biometric property data across the full range of conditions in which

it is used. This can become a significant challenge given the wide variability in the biological structures being measured across the human population and the wide range of environmental conditions in which some biometric systems must function.

Sample variability can come from a variety of sources including:

- Intrinsic biological variability
- Environmental variability
- Sample presentation variability
- Biological target contamination
- Acquisition losses, errors, and noise

Good biometric sample acquisition systems minimize the effects of these sources of variability.

Process Decomposition

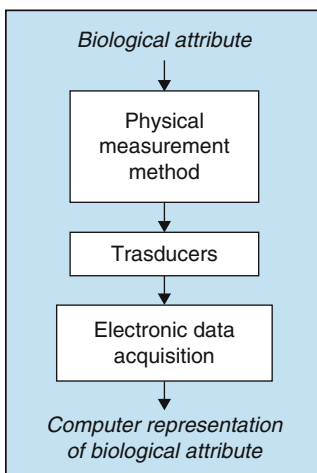
For our discussion here, the sample acquisition process can be decomposed into three parts:

1. The measurement physics
2. The transducers
3. The electronic data acquisition

Figure 1 illustrates this decomposition.

The Measurement Physics

Starting with a biological attribute of interest, a physical sensing method is selected, usually



Biometric Sample Acquisition, Fig. 1 Biometric sample acquisition process decomposition

involving an energy flow that originates from or has been modified by the biological attribute to be measured.

Different physical sensing mechanisms may be more or less sensitive to the biological attribute of interest. A key element in selecting the sensing mechanism is the intrinsic signal to noise ratio. A mechanism that has high sensitivity to the attribute of interest and low sensitivity to other influences is likely to have a favorable signal to noise ratio [1].

The Transducers

The energy flow associated with a sensing method may be measurable by several different types of transducers. Transducers convert the energy associated with a physical measurement into a representative electronic signal. Different transducers may be more or less effective in extracting the biological information from the energy flow.

The Electronic Data Acquisition

Electronic data acquisition equipment converts the transducer output signal into a standardized form that can be manipulated by digital computers [2]. This digitized data becomes the input to the feature extraction and pattern-matching processes.

The data acquisition process typically involves [3]:

- Generating excitation energy and applying it to the biological structures to be measured and/or to the transducers
- Amplifying the transducer signals
- Multiplexing the signals from a multitude of transducers to a small number of signal processing nodes
- Canceling or filtering noise in the transducer signals
- Time-sampling the transducer signals
- Digitizing the (typically analog) transducer signals
- Assembling the digitized signals into a formatted data stream for delivery to a microprocessor for further processing [4]

An Example Biometric Sample Acquisition Process

For example, select the fingerprint ridge pattern as the biological attribute to be measured.

Example Sensing Physics and Transducers

The fingerprint ridge pattern is able to generate or influence several different types of energy and, hence, may be amenable to several different measurement methods. Each type of energy can be measured by several types of transducers. Designing the biometric sample acquisition system then involves finding the optimum combination of measurement methods and transducer type for the application [5].

Pressure

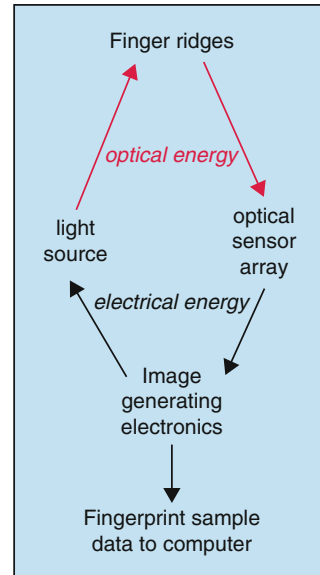
Fingerprint ridges and valleys can apply different amounts of pressure to a contact surface. A wide variety of transduction methods can detect such spatial pressure variations. These span the range from arrays of tiny nano-switches to the legacy inkpad and card systems used with fax-machine-like card scanners.

Optical Energy

Fingerprint ridges and valleys differ in their abilities to reflect light, absorb light, and diffuse light. When one of the various forms of optical energy has been applied to the fingerprint region of the skin, camera-like image capture devices can then capture the fingerprint patterns from the resulting light. Figure 2 illustrates the energy conversions involved in a typical optical fingerprint reader.

Electrical Energy

The fingerprint ridge and valley pattern can affect the movement of electrical energy in several different ways, and electrical energy can be measured by several different types of transducers. Arrays of electrical transducers then measure the patterns in the electrical energy flow to develop a 2-dimensional image of the fingerprint pattern that can be very



Biometric Sample Acquisition, Fig. 2 Example of optical fingerprint sample acquisition process

similar to the images produced by optical measurements.

Acoustical and Thermal Energy

Both acoustical energy and thermal energy propagate more efficiently through the fingerprint ridges than through the air spaces in the valleys between the ridges. Arrays of acoustical and thermal transducers then can detect the pattern of ridges in contact with the array and generate images similar to those produced by the optical and electrical methods discussed above.

Example Electronic Data Acquisition

Arrays of all the above types of transducers can be fabricated today on the top surfaces of silicon integrated circuits [6]. The transducers can then be connected directly to silicon electronic circuits that perform the data acquisition tasks described in the previous section of this article. The integration of arrays of transducers with data acquisition circuitry on a single silicon chip has reduced the size and cost of biometric sample acquisition systems by a factor of over 100 within the 10 years between 1997 and 2007, enabling

a wide variety of new biometric identity verification applications that had previously been cost prohibitive.

Real-World Implementation: Biometric Sample Acquisition Systems in Widespread Use Today

If you have a laptop computer purchased in 2007 or later, there is a good chance that it has a biometric sample acquisition system built into it – in the form of a small fingerprint sensor integrated into the keyboard. The fingerprint sensor can be used as a convenient alternative to passwords when you log on to your computer or when you access a password-protected website. Figure 3 is a photograph of a laptop computer with a built-in fingerprint sensor.

The fingerprint sensors integrated into laptop computers use tiny bits of electrical energy as discussed above to detect the fingerprint pattern of a finger when you slide your finger across the sensor. There are two types of sensing physics in common use in today's laptops. One type uses electrical energy to measure differences in electrical capacitance between pixels near a fingerprint ridge and pixels near a valley. The other type uses small radio frequency signals to detect the fingerprint shape in the conductive layer of skin just beneath the surface. Both types of sensors



Biometric Sample Acquisition, Fig. 3 Fingerprint sensor in a laptop computer

are fabricated as silicon devices, with integrated transducers and data acquisition electronics.

New Requirements for Security in Biometric Sample Acquisition

Biometric sample acquisition systems have begun to take a roll in user identity verification in mobile computing and communication systems. Examples include the previously discussed fingerprint-enabled laptops and biometrically secured cell phones as well. This is a different type of role than that played by biometric systems in the forensic and criminology worlds, because these new systems operate in unsupervised and usually insecure situations. This section examines some of the implications of that new role for biometric sample acquisition and the new requirements imposed on biometric sample acquisition by that role.

Using Biometric Data in Trustworthy Identity Verification

While biometric verification is often used as a replacement for passwords, biometric methods when applied to identity verification function more like a handwritten signature and less like a password. This is not surprising, since a handwritten signature is considered as a form of biometric identity verification.

It can be argued that biometric sample data of any kind cannot be considered secret; hence Trustworthy Biometric Identity Verification in unsupervised situations requires the biometric sample acquisition system to function as a kind of trusted agent [7], essentially certifying (to some reasonable degree of confidence) the validity of the biometric sample that it generates. The role is somewhat analogous to that of a notary in handwritten signature situations. This new role imposes new requirements on the biometric sample acquisition system that do not exist in the heavily supervised biometric acquisition processes associated with criminology and forensics.

While it is not the intention here to discuss the full scope of trusted biometric identity verification systems, the biometric sample acquisition

part of that system inherits certain requirements that can be discussed in this context. Thus, for biometric sample acquisition systems designed to function within unattended identity verification systems, the added requirements include resistance to a number of attack vectors that could be used to falsify the biometric sample that the system delivers.

Trusted Biometric Sample Acquisition Systems

A trusted biometric sample acquisition system inherits at least the following requirements:

- Resistance to fake biometric target presentation.
- This capability is also called Biometric Spoof Prevention. It provides an appropriate degree of protection against attacks like the use of a face mask to fool a face recognition system or movie hero James Bond's use of molded latex rubber finger coverings to fool a fingerprint reader.
- Resistance to acquisition system tampering.
- The requirement here is to prevent an attacker from accessing the internal operation of the biometric sample acquisition system, where he could force it to output different information than it is actually measuring. This requirement may impose hardened packaging requirements on the biometric sample acquisition system.
- Resistance to device/system substitution.
- The system as a whole should be able detect if an alternate device has been substituted for all or any portion of the biometric sample acquisition system. This typically imposes cryptographic capabilities on the biometric sample acquisition system.
- Resistance to communications attacks (e.g., man-in-the-middle and replay).
- The acquired biometric sample must be securely delivered to the subsequent processing stages either by a physically inaccessible data channel or by cryptographic methods.

All these requirements are designed to enhance the trustworthiness of the biometric sample capture event. When a trusted biometric sample acquisition system is integrated into an

overall trusted biometric system (e.g., a sealed local biometric identity verification system), unsupervised biometric identity verification can be performed with reasonable levels of confidence, without concern that biometric properties are intrinsically not secret.

Related Entries

- ▶ [Biometric Applications, Overview](#)
- ▶ [Biometrics, Overview](#)
- ▶ [Biometric Sensor and Device, Overview](#)
- ▶ [Security and Liveness, Overview](#)

References

1. J. Fraden, *Handbook of Modern Sensors – Physics, Designs, and Applications*, 3rd edn. (Springer, Heidelberg, 2004)
2. H. Austerlitz, *Data Acquisition Techniques Using PCs* (Academic, London, 2003)
3. J.G. Webster, *The Measurement Instrumentation and Sensors Handbook* (CRC, Boca Raton, 1998)
4. S. Ball, *Analog Interfacing to Embedded Microprocessor Systems*, 2nd edn. (Newnes, Oxford, 2003)
5. N. Ratha, R. Bolle, *Automatic Fingerprint Recognition Systems* (Springer, Heidelberg, 2003)
6. J.S. Wilson, *Sensor Technology Handbook* (Newnes/Elsevier, Oxford, UK, 2005)
7. S. Pearson, *Trusted Computing Platforms: TCPA Technology in Context*. HP Professional Series (Prentice Hall, Upper Saddle River, 2003)

Biometric Sample Quality

Elham Tabassi and Patrick Grother
National Institute of Standards and Technology,
Gaithersburg, MD, USA

Synonyms

Biometric quality evaluation; Performance of biometric quality measures

Definition

The intrinsic characteristic of a biometric signal may be used to determine its suitability for further

processing by the biometric system or assess its conformance to preestablished standards. The quality score of a biometric sample signal is a scalar summary of the sample's quality.

Quality measurement algorithm is regarded as a black box that converts an input sample to an output scalar. Evaluation is done by quantifying the association between those values and observed matching results. For verification, these would be the false match and nonmatch rates. For identification, the matching results would usually be false match and nonmatch rates [1], but these may be augmented with rank and candidate-list length criteria. For a quality algorithm to be effective, an increase in false match and false nonmatch rates is expected as quality degrades.

Introduction

Biometric quality measurement algorithms are increasingly deployed in operational biometric systems [2, 3], and there is now international consensus in industry [4], academia [5], and government [6] that a statement of a biometric sample's quality should be related to its recognition performance. That is, a quality measurement algorithm takes a signal or image, \mathbf{x} , and produces a scalar, $q = Q(\mathbf{x})$, which is predictive of error rates associated with the verification or identification of that sample. This entry formalizes this concept and advances methods to quantify whether a quality measurement algorithm (QMA) is actually effective.

What is meant by quality? Broadly a sample should be of good quality if it is suitable for automated matching. This viewpoint may be distinct from the human conception of quality. If, for example, an observer sees a fingerprint with clear ridges, low noise, and good contrast, then he or she might reasonably say it is of good quality. However, if the image contains few minutiae, then a minutiae-based matcher would underperform. Likewise, if a human judges a face image to be sharp, but a face recognition algorithm benefits from slight blurring of the image, then the human statement of quality is inappropriate. Thus,

the term quality is not used here to refer to the fidelity of the sample, but instead to the utility of the sample to an automated system. The assertion that performance is ultimately the most relevant goal of a biometric system implies that a quality algorithm should be designed to reflect the sensitivities of the matching algorithm. For fingerprint minutiae algorithms, this could be the ease with which minutiae are detected. For face algorithms, it might include how readily the eyes are located.

Quality evaluation methods should not rely on the manual annotation of a data set because this is impractical for all but small data sets, not least because human examiners will disagree in this respect. The virtue of relating quality to performance is that matching trials can be automated and conducted in bulk. The essay notes further that quality algorithms that relate to human perception of a sample quantify performance only as much as the sensitivities of the human visual system are the same as those of a biometric matcher.

One further point is that performance-related quality evaluation is agnostic on the underlying technology: it would be improper to force a fingerprint quality algorithm to produce low-quality values for an image with few minutiae when the target matching algorithm is nonminutia based, as is the case for pattern-based methods [7].

Evaluation of quality measurement algorithms should be preferably done in large-scale offline trials, which offer repeatable, statistically robust means of evaluating core algorithmic capability.

Prior work on quality evaluation, and of sample quality analysis generally, is limited. Quality measurement naturally lags recognition algorithm development, but has emerged as it realized that biometric systems fail on certain pathological samples. Alonso et al. [8] reviewed five algorithms and compared the distributions of the algorithms' quality assignments, with the result that most of the algorithms behave similarly. Finer-grained aspects of sample quality can be addressed. For instance, Lim et al. [9] trained a fingerprint quality system

to predict the accuracy of minutia detection. However, such methods rely on the manual annotation of a data set, which as stated above is impractical.

Properties of a Quality Measure

This section gives needed background material, including terms, definitions, and data elements, to support quantifying the performance of a quality algorithm. Throughout this entry, low-quality values are used to indicate poor sample properties.

Consider a data set D containing two samples, $d_i^{(1)}$ and $d_i^{(2)}$, collected from each of $i = 1, \dots, N$ individuals. The first sample can be regarded as an enrollment image, the second as a user sample collected later for verification or identification purposes. Suppose that a quality algorithm Q can be run on the i th enrollment sample to produce a quality value

$$q_i^{(1)} = Q(d_i^{(1)}), \quad (1)$$

and likewise for the authentication (use-phase) sample

$$q_i^{(2)} = Q(d_i^{(2)}). \quad (2)$$

Thus, it has been suggested that these qualities are scalars, as opposed to vectors, for example. Operationally, the requirement for a scalar is not necessary: a vector could be stored and used by some application. The fact that quality has historically been conceived of as scalar is a widely manifested restriction. For example, BioAPI [10] has a signed single byte value, BioAPI_QUALITY; and the headers of the ISO/IEC biometric data interchange format standards [11] have five-byte fields for quality with only one byte allocated for quality score. This entry does not further address the issue of vector quality quantities other than to say that they could be used to specifically direct reacquisition attempts (e.g., camera settings), and if considered, their practical use would require application of a discriminant function.

The discussion now formalizes the premise that biometric quality measures should predict performance. A formal statement of such requires an appropriate, relevant, and tractable definition of performance. Consider K verification algorithms, V_k , that compare pairs of samples (or templates derived from them) to produce match (i.e., genuine) similarity scores

$$s_{ii}^{(k)} = V_k(d_i^{(1)}, d_i^{(2)}), \quad (3)$$

and similarly nonmatch (impostor) scores

$$s_{ij}^{(k)} = V_k(d_i^{(1)}, d_j^{(2)}) \quad i \neq j. \quad (4)$$

Now, to posit that two quality values can be used to produce an estimate of the genuine similarity score that matcher k would produce on two samples,

$$s_{ii}^{(k)} = P(q_i^{(1)}, q_i^{(2)}) + \epsilon_{ii}^{(k)}, \quad (5)$$

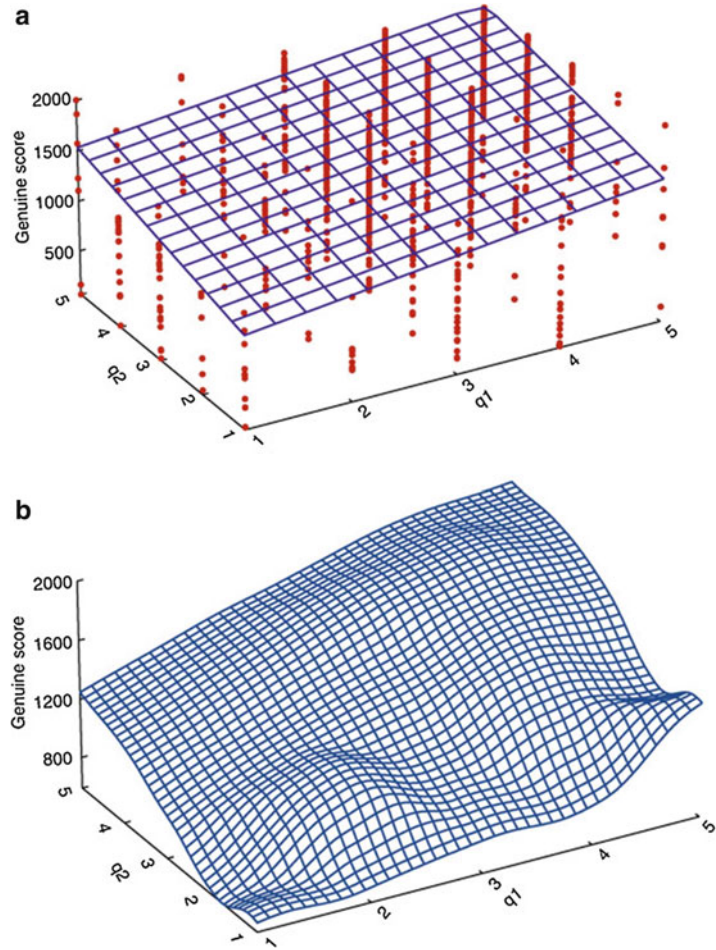
where the function P is some predictor of a matcher k 's similarity scores and ϵ_{ii} is the error in doing so for the i th score. Substituting (1) gives

$$s_{ii}^{(k)} = P(Q(d_i^{(1)}), Q(d_i^{(2)})) + \epsilon_{ii}^{(k)}, \quad (6)$$

and it becomes clear that together P and Q would be perfect imitators of the matcher V_k in (3), if it was not necessary to apply Q to the samples separately. This separation is usually a necessary condition for a quality algorithm to be useful because at least half of the time (i.e., enrollment) only one sample is available. The obvious consequence of this formulation is that it is inevitable that quality values will imprecisely map to similarity scores, i.e., there will be scatter of the known scores, s_{ii} , for the known qualities $q_i^{(1)}$ and $q_i^{(2)}$. For example, Fig. 1 shows the raw similarity scores from a commercial fingerprint matcher versus the transformed integer quality scores from NIST fingerprint image quality (NFIQ) algorithm [6, 12], where NFIQ native scores are mapped to $Q =$

Biometric Sample Quality, Fig. 1

Dependence of raw genuine scores on the transformed NFIQ qualities of the two input samples



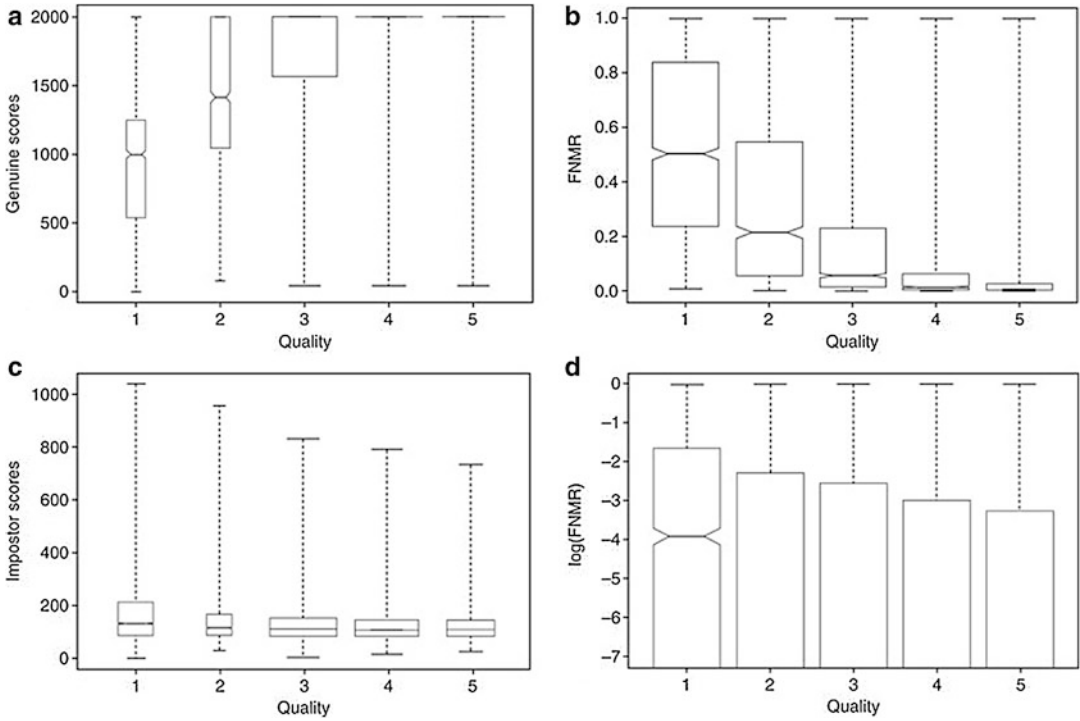
6 – NFIQ (so that higher-quality values indicate good “quality”). Figure 1a also includes a least squares linear fit, and Fig. 1b shows a cubic spline fit of the same data. Both trend in the correct direction: worse quality gives lower similarity scores. Even though the residuals in the spline fit are smaller than those for the linear, they are still not small. Indeed even with a function of arbitrarily high order, it will not be possible to fit the observed scores perfectly if quality values are discrete (as they are for NFIQ). By including the two fits of the raw data, it is not asserted that scores should be linearly related to the two quality values (and certainly not locally cubic). Accordingly, it is concluded that it is unrealistic to require quality measures to be linear predictors of the similarity scores; instead, the scores should be a

monotonic function (higher-quality samples give higher scores).

Evaluation

Quality measurement algorithms are designed to target application-specific performance variables. For verification, these would be the false match rate (FMR) and false nonmatch rate (FNMR). For identification, the metrics would usually be FNMR and FMR [1], but these may be augmented with rank and candidate-list length criteria. Closed-set identification is operationally rare and is not considered here.

Verification is a positive application, which means samples are captured overtly from users who are motivated to submit high-quality



Biometric Sample Quality, Fig. 2 Boxplots of genuine scores, FNMR, impostor scores, and FMR for each of five transformed NFIQ quality levels for scores from a commercial matcher. Each quality bin, q , contains scores from comparisons of enrollment images with quality $q^{(1)} \geq q$ and subsequent use-phase images with $q^{(2)} = q$, per

the discussion in section “[Rank-Ordered Detection Error Tradeoff Characteristics.](#)” The boxplot notch shows the median; the box shows the interquartile range, and the whiskers show the extreme values. Notches in (d) are not visible because the medians of FMRs are zero and therefore outside the plot range

samples. For this scenario, the relevant performance metric is the false nonmatch rate (FNMR) for genuine users because two high-quality samples from the same individual should produce a high score. For FMR, it should be remembered that false matches should occur only when samples are biometrically similar (with regard to a matcher) as, for example, when identical twins’ faces are matched. So, high-quality images should give very low impostor scores, but low-quality images should also produce low scores. Indeed, it is an undesirable trait for a matching algorithm to produce high impostor scores from low-quality samples. In such situations, quality measurement should be used to preempt submission of a deliberately poor sample.

For identification, FNMR is of primary interest. It is the fraction of enrollee searches that do not yield the matching entry on the candidate list.

At a fixed threshold, FNMR is usually considered independent of the size of the enrolled population because it is simply dependent on one-to-one genuine scores. However, because impostor acceptance, as quantified by FMR, is a major problem in identification systems, it is necessary to ascertain whether low- or high-quality samples tend to cause false matches.

For a quality algorithm to be effective, an increase in FNMR and FMR is expected as quality degrades. The plots in Fig. 2 show the relationship of transformed NFIQ quality levels to FNMR and FMR. Figure 2a, c is boxplots of the raw genuine and impostor scores for each of the five NFIQ quality levels. The scores were obtained by applying a commercial fingerprint matcher to left and right index finger impressions of 34,800 subjects. Also shown are boxplots of FNMR and FMR. The

result, that the two error rates decrease as quality improves, is expected and beneficial. The FMR shows a much smaller decline. The nonoverlap of the notches in plots of Fig. 2a, b demonstrates “strong evidence” that the medians of the quality levels differ [13]. If the QMA had more finely quantized its output, to $L > 5$ levels, this separation would eventually disappear. This issue is discussed further in section “Measuring Separation of Genuine and Impostor Distributions.”

Rank-Ordered Detection Error Tradeoff Characteristics

A quality algorithm is useful, if it can at least give an ordered indication of an eventual performance. For example, for L discrete quality levels, there should notionally be L DET characteristics. In the studies that have evaluated performance measures [1, 5, 12, 14–16], DETs are the primary metric. It is recognized that DETs are widely understood, even expected, but note three problems with their use: being parametric in threshold, t , they do not show the dependence of FNMR (or FMR) with quality at fixed t , they are used without a test of the significance of the separation of L levels, and partitioning of the data for their computation is underreported and nonstandardized.

This entry examines three methods for the quality-ranked DET computation. All three use N paired matching images with integer qualities $q_i^{(1)}$ and $q_i^{(2)}$ on the range $[1, L]$. Associated with these are N genuine similarity scores, s_{ii} , and up to $N(N - 1)$ impostor scores, s_{ij} , where $i \neq j$, obtained from some matching algorithm. All three methods compute a DET characteristic for each quality level k . For all thresholds s , the DET is a plot of $\text{FNMR}(s) = M(s)$ versus $\text{FMR}(s) = 1 - N(s)$, where the empirical cumulative distribution functions $M(s)$ and $N(s)$ are computed, respectively, from sets of genuine and impostor scores. The three methods of partitioning differ in the contents of these two sets. The simplest case uses scores obtained by comparing authentication and enrollment samples whose qualities are both k . This procedure

(see, e.g., [17]) is common but overly simplistic. By plotting

$\text{FNMR}(s, k)$

$$= \frac{\left[\left\{ s_{ii} : s_{ii} \leq s, \quad q_i^{(1)} = q_i^{(2)} = k \right\} \right]}{\left[\left\{ s_{ii} : s_{ii} < \infty, \quad q_i^{(1)} = q_i^{(2)} = k \right\} \right]}$$

$\text{FMR}(s, k)$

$$= \frac{\left[\left\{ s_{ij} : s_{ij} > s, \quad q_i^{(1)} = q_j^{(2)} = k, \quad i \neq j \right\} \right]}{\left[\left\{ s_{ij} : s_{ij} > -\infty, \quad q_i^{(1)} = q_j^{(2)} = k, \quad i \neq j \right\} \right]}, \quad (7)$$

the DETs for each quality level can be compared. Although a good QMA will exhibit an ordered relationship between quality and error rates, this DET computation is not operationally representative because an application cannot usually accept only samples with one quality value. Rather, the DET may be computed for verification of samples of quality k with enrollment samples of quality greater than or equal to k :

$\text{FNMR}(s, k)$

$$= \frac{\left[\left\{ s_{ii} : s_{ii} \leq s, \quad q_i^{(1)} \geq k, \quad q_i^{(2)} = k \right\} \right]}{\left[\left\{ s_{ii} : s_{ii} < \infty, \quad q_i^{(1)} \geq k, \quad q_i^{(2)} = k \right\} \right]},$$

$\text{FMR}(s, k)$

$$= \frac{\left[\left\{ s_{ij} : s_{ij} > s, \quad q_i^{(1)} \geq q_j^{(2)} = k, \quad i \neq j \right\} \right]}{\left[\left\{ s_{ij} : s_{ij} > -\infty, \quad q_i^{(1)} \geq q_j^{(2)} = k, \quad i \neq j \right\} \right]}, \quad (8)$$

The situation is modeled in which the enrollment samples are at least as good as the authentication (i.e., user-submitted) samples. Such a use of quality would lead to failures to acquire for the low-quality levels.

If instead performance across *all* authentication samples is compared against enrollment samples of quality greater than or equal to k ,

$$\begin{aligned}
 & \text{FNMR}(s, k) \\
 &= \frac{\left[\left\{ s_{ii} : s_{ii} \leq s, q_i^{(1)} \geq k \right\} \right]}{\left[\left\{ s_{ii} : s_{ii} < \infty, q_i^{(1)} \geq k \right\} \right]}, \\
 & \text{FMR}(s, k) \\
 &= \frac{\left[\left\{ s_{ij} : s_{ij} > s, q_i^{(1)} \geq k, i \neq j \right\} \right]}{\left[\left\{ s_{ij} : s_{ij} > -\infty, q_i^{(1)} \geq k, i \neq j \right\} \right]}. \tag{9}
 \end{aligned}$$

The situation where quality control is applied only during enrollment is modeled. If repeated enrollment attempts fail to produce a sample with quality above some threshold, a failure-to-enroll (FTE) would be declared. This scenario is common and possible because enrollment, as an attended activity, tends to produce samples of better quality than authentication.

The considerable differences between these three formulations are evident in the DETs of Fig. 3 for which the NFIQ algorithm [6] for the predicting performance of a commercial fingerprint system was applied to over 61,993 genuine and 121,997 impostor comparisons (NFIQ native scores were transformed to $Q = 6 - \text{NFIQ}$). In all cases, the ranked separation of the DETs is excellent across all operating points. It is recommended that (8), as shown in Fig. 3b, be used because it is a more realistic operational model.

However, as relevant as DET curves are to expected performance, revisited here is a very important complication. Because DET characteristics quantify the separation of the genuine and impostor distributions and combine the effect of quality on both genuine and impostor performance, the separate effects of quality on FNMR and FMR are lost sight of.

In any case, it is concluded that DETs, while familiar and highly relevant, confound genuine and impostor scores. The alternative is to look at the specific dependence of the error rates on quality at some fixed threshold. Indeed for verification applications, the variation in FNMR with quality is key because the majority of transactions are genuine attempts. For negative identification systems (e.g., watchlist applications) in which

users are usually not enrolled, the variation of FMR with quality is critical. This approach is followed in the next section.

Error Versus Reject Curves

It is proposed to use error versus reject curves as an alternative means of evaluating QMAs. The goal is to state how efficiently rejection of low-quality samples results in improved performance. This again models the operational case in which quality is maintained by reacquisition after a low-quality sample is detected. Consider that a pair of samples (from the same subject), with qualities $q_i^{(1)}$ and $q_i^{(2)}$, are compared to produce a score $s_{ii}^{(k)}$, and this is repeated for N such pairs.

Thresholds u and v are introduced that define levels of acceptable quality and define the set of low-quality entries as

$$R(u, v) = \left\{ j : q_j^{(1)} < u, q_j^{(2)} < v \right\}. \tag{10}$$

The FNMR is the fraction of genuine scores below threshold computed for those samples *not* in this set:

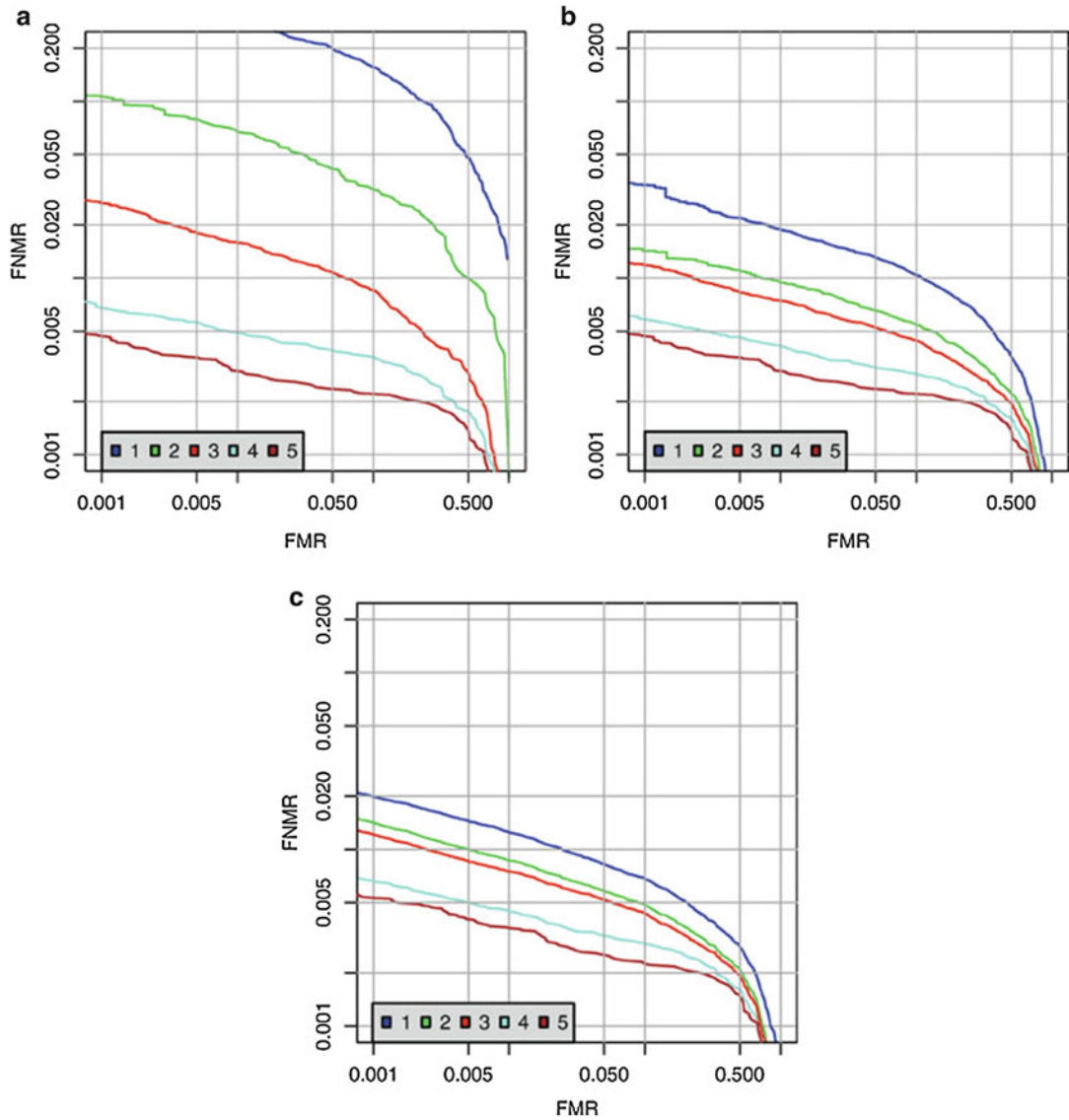
$$\text{FNMR}(t, u, v) = \frac{\left| \left\{ s_{jj} : s_{jj} \leq t, j \notin R(u, v) \right\} \right|}{\left| \left\{ s_{jj} : s_{jj} < \infty \right\} \right|}. \tag{11}$$

The value of t is fixed (note that any threshold may be used. Practically it will be set to give some reasonable false nonmatch rate, f , by using the quantile function the empirical cumulative distribution function of the genuine scores, $t = M^{-1}(1 - f)$), and u and v are varied to show the dependence of FNMR on quality.

For the one-dimensional case, when only one quality value is used, the rejection set is

$$R(u) = \left\{ j : H \left(q_j^{(1)}, q_j^{(2)} \right) < u \right\} \tag{12}$$

where H is a function of combining two quality measures into a single measure. FNMR is false nonmatch performance as the proportion of nonexcluded scores below the threshold:



Biometric Sample Quality, Fig. 3 Quality-ranked detection error tradeoff characteristics. Each plot shows five traces corresponding to five transformed NFIQ levels (Note that the DET used here plots FNMR vs. FMR on log scales. It is unconventional in that it does not transform

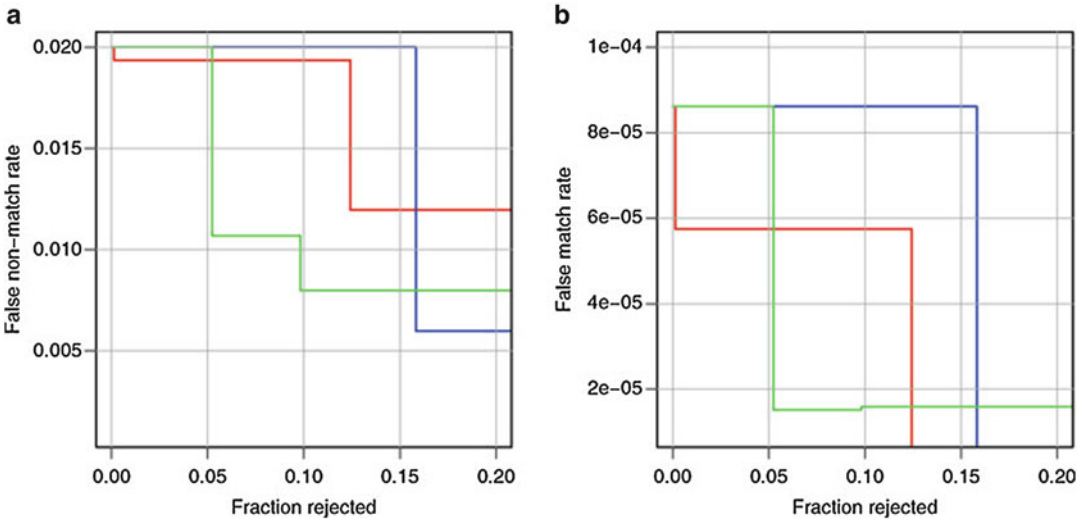
the data by the CDF of the standard normal distribution. The receiver operating characteristic plots 1 – FNMR on a linear scale instead. These characteristics are used ubiquitously to summarize verification performance)

$$FNMR(t, u, v) = \frac{|\{s_{jj} : s_{jj} \leq t, j \notin R(u, v)\}|}{|\{s_{jj} : s_{jj} < \infty\}|} \tag{13}$$

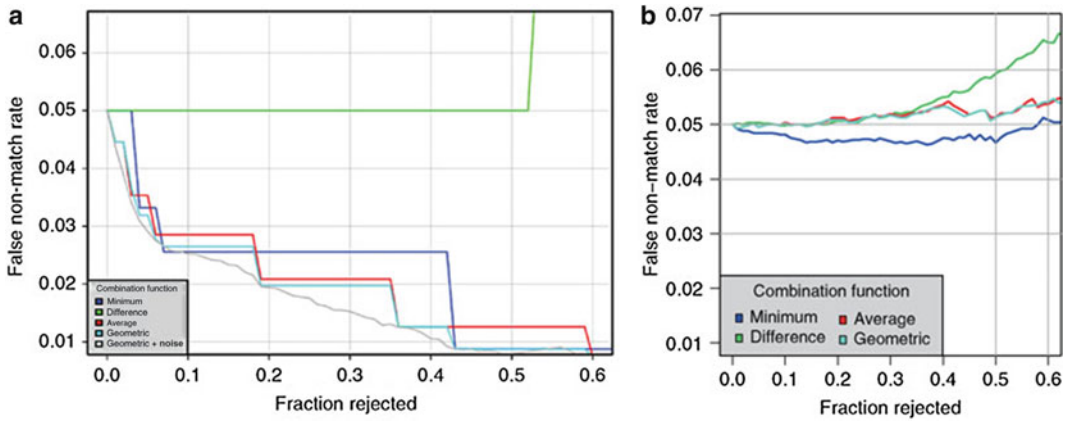
If the quality values are perfectly correlated with the genuine scores, then when t is set to give an overall FNMR of x and then reject proportion

x with the lowest qualities, a recomputation of FNMR should be zero. Thus, a good quality metric correctly labels those samples that cause low genuine scores as poor quality. For a good quality algorithm, FNMR should decrease quickly with the fraction rejected. The results of applying

B



Biometric Sample Quality, Fig. 4 Error versus reject performance for three fingerprint quality methods. (a) and (b) show reduction in FNMR and FMR at a fixed threshold as up to 20 % of the low-quality samples are rejected. The similarity scores come from a commercial matcher

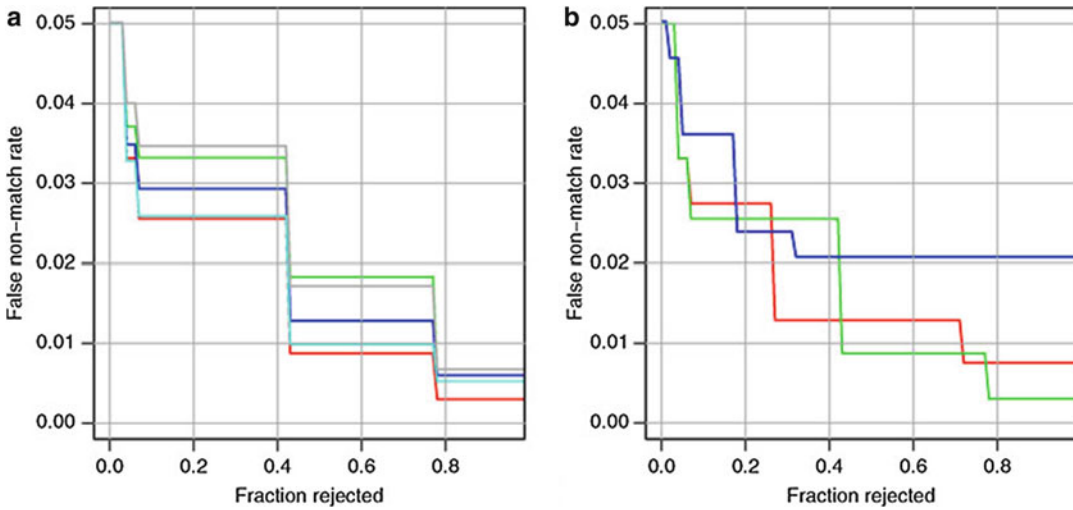


Biometric Sample Quality, Fig. 5 Dependence of the error versus reject characteristic on the quality combination function $H(\cdot)$. The plots show, for a fixed threshold, the decrease in FNMR as up to 60 % of the low-quality values are rejected. The similarity scores come from commercial matchers. The steps in (a) are result of discrete quality metric. Continuous quality metrics such as in (b) do not usually exhibit such steps

this analysis are shown in Fig. 4. Note that the curves for each of the three fingerprint quality algorithms trend in the correct direction but that even after rejection of 20 % the FNMR value has fallen only by about a half from its starting point. Rejection of 20 % is probably not an operational possibility unless an immediate reacquisition can yield better quality values for those persons. Yoshida, using the same approach, reported similar figures [18]. Note, however, that

for NFIQ, the improvement is achieved after rejection of just 5 %. In verification applications such as access control, the prior probability of an impostor transaction is low, and thus, the overall error rate is governed by false nonmatchers. In such circumstances, correct detection of samples likely to be falsely rejected should drive the design of QMAS.

Figure 5 shows error versus reject behavior for the NFIQ quality method when the various



Biometric Sample Quality, Fig. 6 Error versus reject characteristics showing how NFIQ generalizes across (a) five verification algorithms and (b) three operational data

sets. The steps in (a) occur at the same rejection values because the matchers were run on a common database

$H(q_1, q_2)$ combination functions are used. Between the minimum, mean, and geometric mean functions, there is little difference. The geometric mean is best (absent a significance test) with steps occurring at values corresponding to the square roots of the product of NFIQ values. The gray line in the figure shows $H = \sqrt{q_1 q_2} + N(0, 0.01)$, where the Gaussian noise serves to randomly reject samples within a quality level and produces an approximation of the lower convex hull of the geometric mean curve. The green line result, for $H = |q_1 - q_2|$, shows that transformed genuine comparison score is unrelated to the difference in the qualities of the samples. Instead, the conclusion is that FNMR is related to monotonic functions of the two values. The applicability of this result to other quality methods is not known.

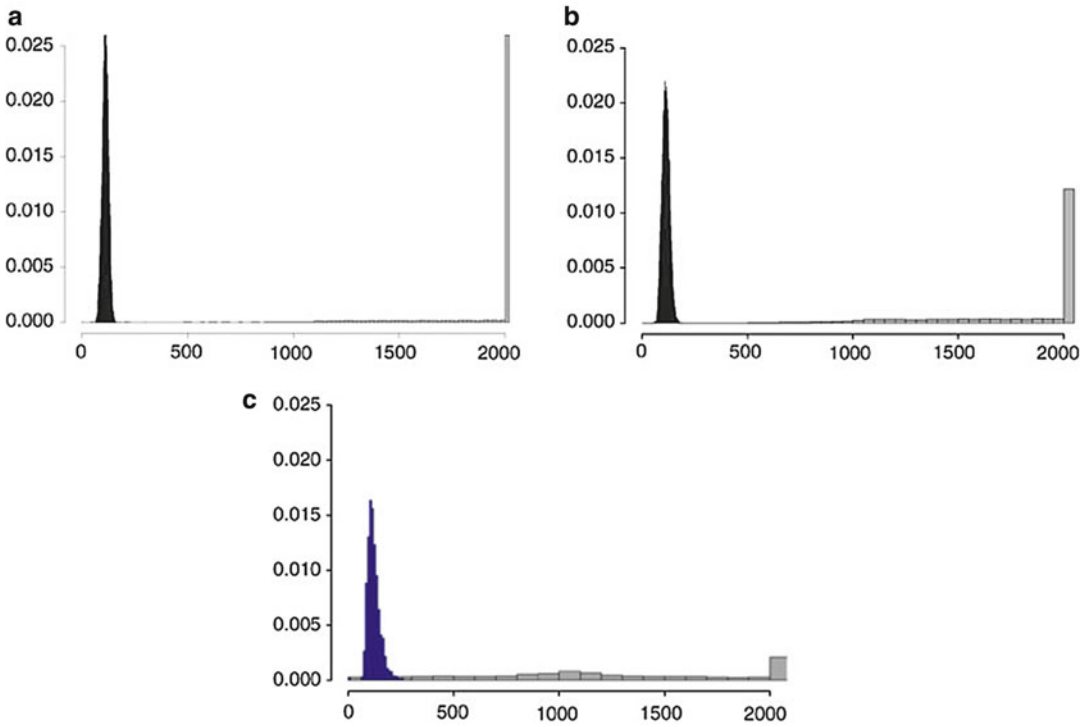
Generalization to Multiple Matchers

It is a common contention that the efficacy of a quality algorithm is necessarily tied to a particular matcher. It is observed that this one-matcher case is commonplace and useful in a limited fashion and should, therefore, be subject to evaluation. However, it is also observed that it is possible for a quality algorithm to be capable of generalizing across *all* (or

a class of) matchers, and this too should be evaluated.

Generality to multiple matchers can be thought of as an interoperability issue: can supplier A's quality measure be used with supplier B's matcher? Such a capability will exist to the extent that pathological samples do present problems to both A and B's matching algorithms. However, the desirable property of generality exposes another problem: it cannot be expected to predict performance absolutely because there are good and bad matching systems. A system here includes all of the needed image analysis and comparison tasks. Rather, it is asserted that a quality algorithm intended to predict performance generally need only be capable of giving a relative or rank ordering, i.e., low-quality samples should give lower performance than high-quality samples.

The plots of Fig. 6 quantify this generalization for the NFIQ algorithm using the error versus reject curves of section "Error Versus Reject Curves." Figure 6a includes five traces, one for each of five verification algorithms. The vertical spread of the traces indicates some disparity in how well NFIQ predicts the performance of the five matchers. A perfectly general QMA would produce no spread.



Biometric Sample Quality, Fig. 7 There is a higher degree of separation between the genuine and impostor distribution for better quality samples as measured by NFIQ

Biometric Sample Quality, Table 1 KS statistics for quality levels of three quality algorithms

Quality algorithm	$Q = 1$	$Q = 2$	$Q = 3$	$Q = 4$
Quality algorithm 1	0.649	0.970	0.988	0.993
Quality algorithm 2	0.959	0.995	0.996	0.997
Quality algorithm 3	0.918	0.981	0.994	0.997

Measuring Separation of Genuine and Impostor Distributions

Quality algorithms can be evaluated on their ability to predict how far a genuine score will lie from its impostor distribution. This means instead of evaluating a quality algorithm solely based on its FNMR (i.e., genuine score distribution), the evaluation can be augmented by including a measure of FMR because correct identification of an enrolled user depends both on correctly finding the match and on rejecting the nonmatches. Note also that a quality algorithm could invoke a matcher to compare the input sample with some internal background samples to compute sample mean and standard deviation.

The plots of Fig. 7 show, respectively, the genuine and impostor distributions for adjusted

NFIQ values, 1, 3, and 5. The overlapping of genuine and impostor distributions for the poorest NFIQ means higher recognition errors for that NFIQ level and vice versa; the almost complete separation of the two distribution for the best quality samples indicates lower recognition error. NFIQ was trained to specifically exhibit this behavior.

The Kolmogorov-Smirnov is considered statistic. For better quality samples, a larger KS test statistic (i.e., higher separation between genuine and impostor distribution) is expected. Each row of Table 1 shows KS statistics for one of the three quality algorithms tested. KS statistics for each quality levels $u = 1, \dots, 5$ are computed by first computing the genuine (i.e., $\{s_{ii} : (i, i) \in R(u)\}$) and impostor

(i.e., $\{s_{ij} : (i, j) \in R(u), i \neq j\}$) empirical cumulative distributions, where $R(u) = \{(i, j) : H(q_i^{(1)}, q_j^{(2)}) = u\}$. Thereafter, the largest absolute difference between the genuine and impostor distributions of quality u is measured and plotted. (Note that to keep quality algorithm providers anonymous, KS statistics of the lowest four quality levels were reported.)

Summary

Biometric quality measurement is an operationally important and difficult problem that is nevertheless massively under-researched, in comparison to the primary feature extraction and pattern recognition tasks. It was asserted that quality algorithms should be developed to explicitly target matching error rates, and not human perceptions of sample quality.

Several means were given for assessing the efficacy of quality algorithms. The existing practice was reviewed, cautioned against the use of detection error tradeoff characteristics as the primary metrics, and instead advanced boxplots and error versus reject curves as preferable. This entry suggests that algorithm designers should target false nonmatch rate as the primary performance indicator.

Related Entries

- ▶ [Biometric Sample Quality, Standardization](#)
- ▶ [Biometric Systems, Agent-Based](#)
- ▶ [Biometric Vulnerabilities, Overview](#)
- ▶ [Biometric Verification/Identification/ Authentication/Recognition: The Terminology](#)
- ▶ [Fingerprint Image Quality](#)
- ▶ [Quality Measures in Biometric Systems](#)
- ▶ [Remote Authentication](#)

References

1. A.J. Mansfield, ISO/IEC 19795-1 biometric performance testing and reporting: principles and framework, FDIS ed., JTC1/SC37/Working Group 5, Aug 2005, <http://isotc.iso.org/isotcportal>
2. T. Ko, R. Krishnan, Monitoring and reporting of fingerprint image quality and match accuracy for a large user application. In: *Proceedings of the 33rd Applied Image Pattern Recognition Workshop*, Washington, D.C. (IEEE Computer Society, 2004), pp. 159–164
3. *Proceedings of the NIST Biometric Quality Workshop (NIST)*, Gaithersburg, Mar 2006, <http://www.itl.nist.gov/iad/894.03/quality/workshop/presentations.html>
4. D. Benini et al., ISO/IEC 29794-1 biometric quality framework standard, 1st ed. JTC1/SC37/Working Group 3 (Jan 2006), <http://isotc.iso.org/isotcportal>
5. Y. Chen, S. Dass, A. Jain, Fingerprint quality indices for predicting authentication performance. In: *Proceedings of the Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Rye Brook, July 2005, pp. 160–170
6. E. Tabassi, Fingerprint Image Quality, NFIQ, NISTIR 7151 ed. National Institute of Standards and Technology, Gaithersburg (2004)
7. Bioscrypt Inc., Systems and methods with identify verification by comparison and interpretation of skin patterns such as fingerprints, <http://www.bioscrypt.com>. June 1999
8. F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia, A review of schemes for fingerprint image quality computation, in *COST 275 – Biometrics-Based Recognition of People over the Internet*, Hatfield, Oct 2005
9. E. Lim, X. Jiang, W. Yau, Fingerprint quality and validity analysis, in *Proceedings of the IEEE Conference on Image Processing*, Rochester, Sept 2002, vol. 1, pp. 469–472
10. C. Tilton et al., *The BioAPI Specification* (American National Standards Institute, Washington, D.C., 2002)
11. ISO/IEC JTC1/SC37/Working Group 3, ISO/IEC 19794 biometric data interchange formats (2005), <http://isotc.iso.org/isotcportal>
12. E. Tabassi, A novel approach to fingerprint image quality, in *IEEE International Conference on Image Processing ICIP-05*, Genoa, Sept 2005
13. J.M.Chambers, W.S.Cleveland, B. Kleiner, P.A. Tukey, *Graphical Methods for Data Analysis* (Wadsworth and Brooks/Cole, Belmont, 1983), p. 62
14. J. Fierrez-Aguilar, L. Muñoz-Serrano, F. Alonso-Fernandez, J. Ortega-Garcia, On the effects of image quality degradation on minutiae and ridge-based automatic fingerprint recognition, in *IEEE International Carnahan Conference on Security Technology*, Las Palmas, Oct 2005
15. A. Martin, G.R. Doddington, T. Kamm, M. Ordowski, M.A. Przybocki, The DET curve in assessment of detection task performance, in *Proceedings of Eurospeech*, Rhodes, 1997, pp. 1895–1898
16. A.J. Mansfield, J.L. Wayman, Best practices in testing and reporting performance of biometric devices. National Physics Laboratory Report CMSC 14/02, Aug 2002, <http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf>

17. D. Simon-Zorita, J. Ortega-Garcia, J. Fierrez-Aguilar, J. Gonzalez-Rodriguez, Image quality and position variability assessment in minutiae-based fingerprint verification. *IEE Proc. Vis. Image Signal Process.* **150**(6), 395–401 (2003). Special issue on biometrics on the Internet (2003)
18. A. Yoshida, M. Hara, Fingerprint image quality metrics that guarantees matching accuracy, in *Proceedings of NIST Biometric Quality Workshop*, Gaithersburg, (NEC Corp., 2006), <http://www.itl.nist.gov/iad/894.03/quality/workshop/presentations.html>

Biometric Sample Quality, Standardization

Elham Tabassi

National Institute of Standards and Technology,
Gaithersburg, MD, USA

Synonyms

Biometric quality; Sample quality

Definition

Open documented data structures for universally interpretable interchange of biometric sample quality data.

Biometric data interchange standards are needed to allow the recipient of a data record to successfully process data from an arbitrary producer. This defines biometric interoperability and the connotation of the phrase “successfully process” the data, in this case, ► [Biometric Sample Quality](#) score, can be accurately exchanged and interpreted by different applications. This can only be achieved if the data record is both syntactically and semantically conformant to the documentary standard.

Introduction

Performance of biometric systems depends on the quality of the acquired input samples. If quality can be improved, either by sensor

design, user interface design, or by standards compliance, better performance can be realized. For those aspects of quality that cannot be designed in, an ability to analyze the quality of a live sample is needed. This is useful primarily in initiating the reacquisition from a user but also for the real-time selection of the best sample and the selective invocation of different processing methods. That is why quality measurement algorithms are increasingly deployed in operational biometric systems. With the increase in deployment of quality algorithms rises the need to standardize an interoperable way to store and exchange of biometric quality scores.

Roles

With advancement in biometric technologies as a reliable identity authentication scheme, more large-scale deployments (e.g., e-passport) involving multiple organizations and suppliers are being ruled out. Therefore, in response to a need for interoperability, biometric standards have been developed.

Without interoperable biometric data standards, exchange of biometric data among different applications is not possible. Seamless data sharing is essential to identity management applications when enrollment, capture, searching, and screening are done by different agencies, at different times, using different equipment in different environments and/or locations. Interoperability allows modular integration of products without compromising architectural scope and facilitates the upgrade process and thereby mitigates against obsolescence.

This entry focuses on biometric quality standardization. Broadly biometric quality standards serve the same purpose as many other standards, which is to establish an interoperable definition, interpretation, and exchange of biometric quality data. Like other standards, this creates grounds for a marketplace of off-the-shelf products and is a necessary condition to achieve supplier independence and to avoid vendor lock-in.

Biometric quality measurement has vital roles to play in improving biometric system accuracy and efficiency during the capture process (as a control-loop variable to initiate reacquisition), in database maintenance (sample update), in enterprise-wide quality-assurance surveying, and in invocation of quality-directed processing of samples. Neglecting quality measurement will adversely impact accuracy and efficiency of biometric recognition systems (e.g., verification and identification of individuals). Accordingly, biometric quality measurement algorithms are increasingly deployed in operational systems [3, 6]. These motivated for biometric quality standardization efforts.

Standards do not themselves assure interoperability. Specifically, when a standard is not fully prescriptive, or allows for optional content, then two implementations that are exactly conformant to the standard may still not interoperate. This situation may be averted by applying further constraints on the application of the standard. This is done by means of “application profile” standards which formally call out the needed base standards and refine their optional content and interpretation.

Standards Development Organizations

Standards are developed by a multitude of standards development organizations (SDOs) operating in a great variety of technical disciplines. SDOs exist within companies and governments and underneath trade associations and international body umbrellas. International standards promise to support larger marketplaces and the development process involves more diverse and thorough review and so consensus is more difficult to achieve. Standard development processes are conducted according to definitive sets of rules. These are intended to achieve consensus standards that are technically sound, implementable, and effective.

The following list gives an overview of the relevant SDOs. Note that the published standards

are usually copyrighted documents and available only by purchase:

- ISO/IEC JTC 1/SC 37: SubCommittee 37 (SC 37) *Biometrics* was established in mid-2002 as the most new of 17 active subcommittees beneath Joint Technical Committee 1 (JTC 1) and its parent the International Standard Organization (ISO) and the International Electrotechnical Commission (IEC) (ISO maintains a catalog of its standards development efforts at <http://www.iso.org/iso/en/CatalogueListPage.CatalogueList>). The scope of JTC 1/SC 37 is standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. The establishment of JTC 1/SC 37 provided an international venue to accelerate and harmonize formal international biometric standardization and to coalesce a wide range of interests among information technology and biometric industry and users of biometric-based solutions for multiple identification and verification applications. SC 37 portfolio is divided into six working groups of SC 37. The body responsible for biometric quality standardization is Working Group 3. The group is the largest Working Group in SC 37 and develops biometric data interchange format standards, which have the highest profile adoption in the marketplace.
- M1: M1 is Technical Committee of the International Committee for Information Technology Standards (INCITS). It serves as the United States Technical Advisory Group (TAG) to SC 37. It was established in June 2002 and is responsible for formulating US positions in SC 37 where it holds the US vote. It is also a standards development organization in its own right. Its standards are published in the US, but may be purchased worldwide.
- ANSI/NIST The US National Institute of Standards and Technology (NIST) is also a SDO. It developed the ANSI/NIST standards for law enforcement under the canvass process defined by American National Standard Institution (ANSI).

The ISO/IEC 29794 Biometric Sample Quality Standard

In January 2006, the SC37 Biometrics Subcommittee of JTC1 initiated work on ISO/IEC 29794, a multipart standard that establishes quality requirements for generic aspects (Part 1), fingerprint image (Part 4), facial image (Part 5), and, possibly, other biometrics later. Specifically, Part 1 of this multipart standard specifies derivation, expression, and interpretation of biometric quality regardless of modality. It also addresses the interchange of biometric quality data via the multipart ISO/IEC 19794 Biometric Data Interchange Format Standard [1]. Parts 4 and 5 are technical reports (not standard drafts) which address the aspects of biometric sample quality that are specific to finger images and facial images as defined in ISO/IEC 19794-4 and ISO/IEC 19794-5, respectively.

The generic ISO quality draft (ISO/IEC 29794-1) requires that quality values must be indicative of recognition performance in terms of false match rate, false non-match rate, failure to enroll, and failure to acquire. Furthermore, it considers three components of biometric sample quality, namely, character, fidelity, and utility. The character of a sample indicates the richness of features and traits from which the biometric sample is derived. The fidelity of a sample is defined as the degree of similarity between a biometric sample and its source, for example, a heavily compressed fingerprint has low fidelity. The utility of a sample reflects the observed or predicted positive or negative contribution of an individual sample to the overall performance of a biometric system. Utility is a function of both the character and fidelity of a sample and is most closely indicative of performance in terms of recognition error rates (i.e., false match rate, false non-match rate, failure to enroll, and failure to acquire).

Part 1 of multipart ISO/IEC 29794 draft standard defines a binary record structure for the storage of a sample's quality data. It establishes requirements on the syntax and semantic content of the structure. Specifically it

states that the purpose of assigning a quality score to a biometric sample shall be to indicate the expected utility of that sample in an automated comparison environment. That is, a quality algorithm should produce quality scores that target application-specific performance variables. For verification, the metric would usually be false match and false non-match rates that are likely to be realized when the sample is matched.

In addition, revision of all parts of ISO/IEC 19794 Biometric Data Interchange Format began in January 2007. This opened the opportunity to revise or add quality-related clauses (e.g., compression limits) to data format standards so that conformance to those standards ensures acquisition of sufficient quality samples. This constitutes quality by design. To enable an interoperable way of reporting and exchanging biometric data quality scores, the inclusion of a five-byte quality field to the view header in each view of the data in a Biometric Data Block (BDB) for all parts of ISO/IEC 19794 is being considered. By placing quality field in the view header (as opposed to general header) of a BDB, one can precisely report quality score for each view of a biometric sample (Fig. 1). Table 1 shows the structure of the quality field that SC 37 Working Group 3 is currently considering.

The 1-byte quality score shall be a quantitative expression of the predicted matching performance of the biometric sample. Valid values for quality score are integers between 0 and 100, where higher values indicate better quality. Value 255 is to handle special cases. An entry of "255" shall indicate a failed attempt to calculate a quality score. This value of quality score is harmonized with ISO/IEC 19784-1 BioAPI Specification (section 0.5) [2], where "255" is equivalent to BioAPI "-1" (note that BioAPI, unlike ISO/IEC 19794, uses signed integers).

To enable the recipient of the quality score to differentiate between quality scores generated by different algorithms, the provider of quality scores shall be uniquely identified by the two most significant bytes of 4-byte quality algo-



Biometric Sample Quality, Standardization, Fig. 1 Structure of header in a biometric data block as defined in ISO/IEC 19794-x

Biometric Sample Quality, Standardization, Table 1 Structure of 5-byte quality field that SC 37 Working Group 3 is considering

Description	Size (byte)	Valid values	Note
Quality score	1	[0–100] 255	0: lowest; 100: highest; 255: failed attempt
Quality algorithm vendor ID	2	[1,65,535]	These two bytes uniquely identify the supplier (vendor) of quality score
Quality algorithm ID	2	[1,65,535]	These two bytes uniquely identify the algorithm that computes the quality score. It is provided by the supplier (vendor) of quality score

gorithm vendor ID (QAID). The least significant 2 bytes shall specify an integer product code assigned by the vendor of the quality algorithm. It indicates which of the vendor’s algorithms (and version) were used in the calculation of the quality score and should be within the range 1–65,535.

Different quality assessment methods could be used to assess quality of a biometric sample, for example, quality algorithm A could be used at the time of enrollment, but the verification phase might deploy quality algorithm B. To accommodate interchange of quality scores computed by different quality algorithms, multiple blocks of quality as shown in Table 1 could be encoded in a view header. Block(s) of quality data as shown in Table 1 is preceded by a single byte which value indicates how many blocks of quality data are to follow. A value of 0 means no attempt was made to calculate a quality score (i.e., no quality score has been specified). This is equivalent to BioAPI “–2.” The structure of the quality field is modality independent and therefore generalizable to all parts of ISO/IEC 19794.

The ISO/IEC 29794 standard is currently under development, and ISO/IEC 19794 is currently under revision. The reader is cautioned that standards under development or revision are subject to change; the documents are owned by the respective working groups and their content can shift due to various reasons including but

not limited to technical difficulties, the level of support, or the need to gain consensus.

The ANSI/NIST ITL 1-2007 Quality Field

Initiated in 1986, this standard is the earliest and most widely deployed biometric standard. It establishes formats for the markup and transmission of textual, minutia, and image data between law enforcement agencies, both within United States and internationally.

The ANSI/NIST standard includes defined *types* for the major biometric modalities. The standard is multimodal in that it allows a user to define a transaction that would require, for example, fingerprint data as Type 14, a facial mug shot as Type 10, and the mandatory header and metadata records Types 1 and 2. These are linked with a common numeric identifier.

In its latest revision [7], the standard adopted the ISO five-byte quality field (Table 1) structure, but unlike ISO/IEC 29794, it allows for multiple quality fields, where each quality score could be computed by a different quality algorithm supplier. In addition, it mandates NIST Fingerprint Image Quality (NFIQ) [9] for all Type 14 records.

The BioAPI Quality Specification

ISO/IEC 19784 Biometric Application Programming Interface (BioAPI) [4] (and its national counterpart the BioAPI specification [2]) allows for quality measurements as an integral value in

Biometric Sample Quality, Standardization, Table 2 BioAPI quality categories

Value	Interpretation
0–25	<i>Unacceptable</i> : the sample cannot be used for the purpose specified by the application. The sample needs to be replaced using one or more new biometric samples
26–50	<i>Marginal</i> : the sample will provide poor performance for the purpose specified by the application and in most application environments will compromise the intent of the application. The sample needs to be replaced using one or more new biometric samples
51–75	<i>Adequate</i> : the biometric data will provide good performance in most application environments based on the purpose specified by the application. The application should attempt to obtain higher-quality data if the application developer anticipates demanding usage
76–100	<i>Excellent</i> : the biometric data will provide good performance for the purpose specified by the application

the range of 0–100 with exceptions that value of “–1” means that the quality field was not set by the Biometric Service Provider (BSP) and value of “–2” means that quality information is not supported by the BSP. The primary objective of quality measurement and reporting is to have the BSP inform the application how suitable the biometric sample is for the purpose specified by the application (as intended by the BSP implementer based on the use scenario envisioned by that BSP implementer), and the secondary objective is to provide the application with relative results (e.g., current sample is better/worse than previous sample). BioAPI also provides guidance on general interpretation of quality scores as shown in Table 2.

Summary

The benefit of measuring and reporting of biometric sample quality is to improve performance of biometric systems by improving the integrity of biometric databases and enabling quality-directed processing in particular when utilizing multiple biometrics. Such processing enhancements result in increasing probability of detection and track accuracy while decreasing probability of false alarms. Given these important roles of biometric sample quality in improving accuracy and efficiency of biometric systems, quality measurement algorithms are increasingly deployed in operational systems. Biometric sample quality standards have been developed to facilitate universal seamless exchange of sample quality information.

Related Entries

- ▶ [Face Sample Quality](#)
- ▶ [Fingerprint Image Quality](#)
- ▶ [Fusion, Quality-Based](#)
- ▶ [Iris Image Quality](#)

References

1. ISO/IEC JTC1/SC37/Working Group 3: ISO/IEC 19794 Biometric Data Interchange Formats, 2005
2. ISO/IEC JTC1/SC37/Working Group 3: ISO/IEC 19784-1 Biometric application programming interface with Amd. 1 (2008)
3. T. Ko, R. Krishnan, Monitoring and reporting of fingerprint image quality and match accuracy for a large user application, in *Proceedings of the 33rd Applied Image Pattern Recognition Workshop*, Washington, DC (IEEE Computer Society, 2004), pp. 159–164
4. R.M. McCabe et al., *Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information* (ANSI/NIST, Gaithersburg, 2007)
5. *Proceedings of the NIST Biometric Quality Workshop* (NIST, 2006), <http://www.itl.nist.gov/iad/894.03/quality/workshop/presentations.html>
6. B. Scott Swann, Integrating standard biometric quality metric within the FBI IAFIS, in *Proceedings of the NIST Biometric Quality Workshop* (NIST, 2006), <http://www.itl.nist.gov/iad/894.03/quality/workshop/presentations.html>. B. Wing, Why is biometric quality important to DNS and other government agencies, in *Proceedings of the NIST Biometric Quality Workshop* (NIST, 2006), <http://www.itl.nist.gov/iad/894.03/quality/workshop/presentations.html>
7. E. Tabassi, C. Wilson, C. Watson, *Fingerprint Image Quality*. NFIQ, NIST Interagency Report, NISTIR7151 (National Institute of Standards and Technology, Gaithersburg, 2004)
8. C. Tilton et al., *The BioAPI Specification* (American National Standards Institute, Gaithersburg, 2002)

Biometric Sample Synthesis

Douglas J. Buettner
The Aerospace Corporation, El Segundo,
CA, USA

Synonyms

Artificial biometrics; Artificial digital biometrics; Artificial image biometrics; Intermediate biometrics; Synthetic biometrics

Definition

Biometric sample synthesis is the computer generation of simulated digital biometric data using parametric models. Parametric models are in general the computer creation steps derived from the empirical analysis of digitized biometric patterns or mathematical equations from the physics of the biometric sample's creation.

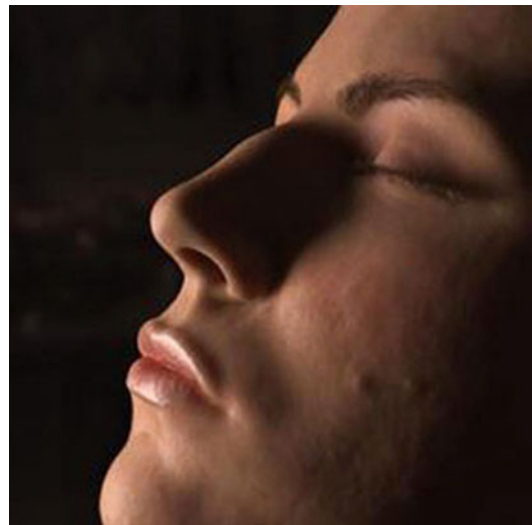
Introduction

Biometric sample synthesis is the art and science of creating artificial digital biometrics that mimic real digital biometric samples. Researchers involved in the creation of synthetic biometric samples may have any number of possible noble goals; included in these may be striving for a fundamental understanding of the factors that affect the digitization process of real human biometric samples for a specific type of biometric sensor, attempting to improve or test computer algorithms used in biometric security devices, striving for statistically realistic equations of human populations, or simply attempting to efficiently computer-generate an image that is similar in visual appearance to a digitized biometric image.

No matter what the underlying reason for creating synthetic biometrics by researchers, the movie industry's quest for realistic computer-generated artificial personas has led to physics-

based models to control physical form, motion, and illumination properties of materials [1]. Computer-generated human characteristics now address a broad range of human details including facial features, skin, hair, and gait, as well as more 0 bodily movements, such as emotive gestures and even eye movement. The Association for Computing Machinery (ACM) Special Interest Group on Computer Graphics (SIGGRAPH) has a large body of work spanning over three decades with the long-standing goal of achieving photo-realism in the computer generation of synthetic images [2]. This achievement of modeling, animation, and rendering of visual human subjects is widely viewed in feature films, commercial art, and video games. An example of the state of the art in the synthesis of an image-based facial biometrics is illustrated in Fig. 1.

The ultimate goal of biometric sample synthesis can be summarized as the use of a standard computer model containing parameter settings that provide the ability to create a synthetic cor-



Biometric Sample Synthesis, Fig. 1 Rendering of a synthetic face using 13 million triangles and a bidirectional surface scattering reflectance distribution function (BSSRDF) model for subsurface light scattering and an oily reflection layer (http://graphics.ucsd.edu/~henrik/papers/face_cloning/) (Reproduced with permission from the author)

pus of biometrics, which would be indistinguishable from that of a corpus of biometric samples obtained from real people.

Factors Affecting Biometric Samples

There are a number of factors that directly affect real biometric samples, which the process of biometric sample synthesis must take into account. For example, biological human responses to environmental conditions are known to directly influence a biometric sample such as heat to sweat, cold to shivering, or light level on pupil dilation. Likewise, the environment can also directly affect the biometric digitizing device; for example, fog, rain, smoke, or light level decrease a video camera's ability to get a clear image, or water on a fingerprint device's platen can adversely affect the quality of the image. The environment can also cause behavioral changes that affect biometric sample acquisition; for example, influencing the clothes we wear during hot or cold weather or during a cloudy or sunny day, or whether or not we are likely to be wearing sunglasses, gloves, or certain types of headgear. Additionally, one's occupation can affect the exposure of a biometric to specific environments that may degrade the quality of the biometric sample. The impact of handling rough surfaces on the skin ridges and troughs on the fingers and hands of people in certain occupations can directly affect the quality of biometric samples from some biometric fingerprint digitizing devices.

Regional location also affects the likelihood of finding various ethnicities who may wear different kinds of hats, different styles of facial hair growth, or various types of garments, which may directly influence biometric sample acquisition. Additional factors may effect biometric sample acquisition through the presentation of a biometric to the digitizing device. An example is the habituation of users to fingerprint sensor technologies that require pressing the sensor's platen; users unfamiliar with the technology are more likely to press extremely hard or very lightly, while habituated users are more likely to provide a closer to nominal amount of pressure when

placing a digit on the device. The amount of pressure may (or may not) adversely affect the biometric feature extraction algorithm used by the vendor. For example, light pressure could decrease the number of minutia available to the biometric matching algorithm.

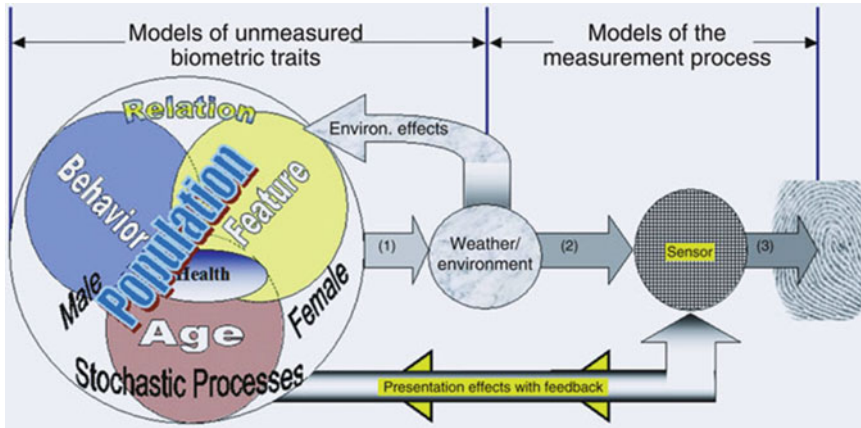
Genetic factors also play an important role in biometrics. Examples here include the generally smaller size of Asian fingerprints, gender, skin color, and others. Another environmental factor that can affect a biometric is our health, in the sense that our unique genetic makeup and our environmental exposure to triggering factors can make us more susceptible to (for example) diseases that can affect a biometric. Here an example is psoriasis that can affect the skin, which (if located on the hand or fingers) can affect the quality of a finger or palm acquisition device's digitized image that in turn can affect the ability of the biometric feature extraction algorithm to extract a consistent biometric feature. Finally, the natural process of aging and relationships with exposure to the sun affects the quality or number of features available for biometric matching algorithms.

The method of sample measurement also directly affects the quality and depth of information obtained about the real biometric trait that the device is attempting to measure. Examples are optical, electrical resistance, or ultrasound for fingerprint devices, and number of pixels used by a digital camera to acquire images of the face. The final representation of the synthetic biometric sample must adequately mimic the digitization process on the biometric sample. Figure 2 illustrates the taxonomy framework that distinguishes between the feedback effects of environment on unmeasured biometric samples and the measurement/digitization process [3].

How all these factors directly or indirectly affect biometric samples is an ongoing research activity in the field of biometrics.

Synthesis Methods

Synthesis of image-based biometrics has been achieved for the most widely recognized digital-



Biometric Sample Synthesis, Fig. 2 A conceptual biometric-environment-sensor interaction model for understanding the taxonomy of modeled parameters in synthetic biometrics

Biometric Sample Synthesis, Table 1 Synthetic biometric data generation

	Fingerprint	Face	Iris	Voice
Synthetic generation	Yes	Yes	Yes	Yes
Model types	Physical – finger/skin growth model; Statistical – level 2 minutiae	Physical – craniofacial growth & human skin light scattering models; Statistical – morphable feature	Statistical – feature	Statistical and Physical – articulatory
Validated statistical models	No	No	Partial	No

image-type biometrics of fingerprint, face, and iris. Table 1 identifies the available model types for a number of widely used biometric modalities.

The methods used for biometric sample synthesis can be categorized depending on the approach for feature synthesis. These are loosely placed into statistical or physical modeling categories based on characteristics of the biometric formation process.

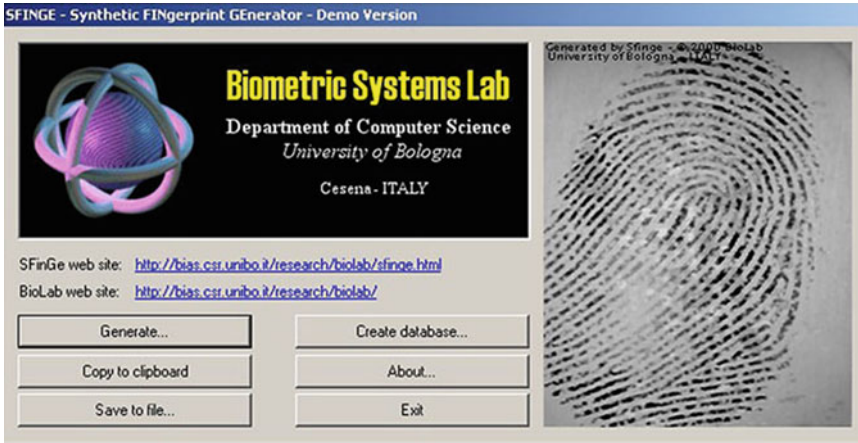
Physical models are those that are based on the physics of how the biometric is created. Examples of biometric features that have physical models for the body part containing the biometric sample include stress/strain finger growth models that have been used to describe fingerprint patterns, craniofacial 3D growth models, and speech synthesis models for the human vocal tract.

Statistical models are those that use empirical analysis of real 2D or 3D biometric images to

create empirically derived statistical information that can be parameterized into some sort of equation or algorithmic synthesis steps to create a synthetic biometric sample. The SFinGe fingerprint generation tool in Fig. 3 is one example of the use of this intermediate-pattern type of biometric feature generator. This tool also exemplifies the parametric or mathematical model of synthesis. Face creation and morphing tools, such as the one from FaceGen Modeler from Singular Inversions, Inc. (Fig. 4) is another example of a statistical modeling tool that also provides age progression functionality as well as the ability to rotate, translate, add texture, or make a number of possible modifications to face/head models.

Validated statistical models would (at a minimum) be those models that have been rigorously validated to match across a wide range of human ethnic populations under specific image-gathering conditions that could affect the image. Matching could be achieved by using quantile-

B



Biometric Sample Synthesis, Fig. 3 The SFingE tool as an example of the synthesized intermediate biometric patterns based on an empirical statistical model

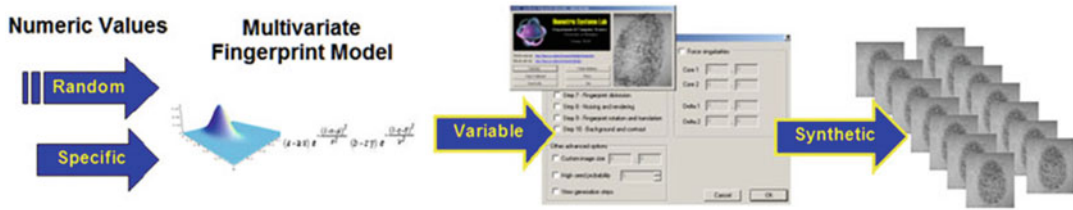


Biometric Sample Synthesis, Fig. 4 A photographic image of a live person added to a 3D face model (Reproduced with permission from the original author)

quantile (q-q) plots to show that the distributions from the two different populations are identical as was done by Daugman for iris codes [4]. The broader view would be the validation of these models across the human populations and

the widest variety of possible environments and devices.

After the statistical taxonomy, parameters are understood for the acquisition of a particular biometric sample, the tool can be configured to



Biometric Sample Synthesis, Fig. 5 Methodology for creating synthetic sample databases using parametric models

generate a large number of synthetic biometric samples (as shown in Fig. 5).

Uses of Synthetic Biometrics

Synthetic biometric samples should not be considered a replacement for real biometric samples, which are still needed to understand the specifics of how the biometric acquisition device and system as a whole handles real world conditions. Mansfield and Wayman provide a warning about the “external validity” from the use of artificial images due to the bias that can result from their generation [5]. This bias is introduced during the analysis of the training set of images used in creating the parametric equations. However, synthetic biometric samples offer a number of potential uses, some positive and some negative.

Among the positive useful benefits of synthetic biometric sample is a cost-effective means for studying a biometric system’s algorithmic sensitivity to specific biometric images from a variety of sensor types, or the performance impacts from biometric images that have been affected by any of a number of various environmental or presentation factors.

Injecting synthetic biometric images into real world or synthetic world scenes provides an ability to perform operational scenario testing in a laboratory environment. The modeled “subjects” can be generated randomly according to statistical models of a target population or in this randomly generated target population, very specific real or synthetic biometrics can be injected to determine gross failure to detect rates in a system context. Operational scenarios can include videos of synthetic

subjects walking through a security checkpoint, and in the system context could include a specifically injected individual with specific behavioral characteristics, or individual wearing troublesome garments, such as sunglasses. Validated biometric models could also be used in the area of fingerprinting where they could readily provide the effects of age, ethnicity, and gender on performance. Biometric systems engineers could run a vast array of potential scenarios to categorize the performance of a layered security system that contains security devices that have a known reliability or can use it to optimize camera locations and lighting conditions.

National security support can be provided in the areas of border control in airports, border crossings, and in ports – by providing the capability to understand potential vulnerabilities through controlled areas. Countries that lack sufficient biometric diversity to test border control systems for underrepresented ethnic groups would certainly benefit from the ability to inject synthetic biometrics from these groups to insure the system is not biased in its ability to properly handle those individuals. Systems that underperform on specific ethnic groups mostly lacked sufficient training data for the engineers building the system.

Synthetic biometric samples are not associated with specific individuals; hence one could then argue that they enhance privacy. Biometric databases generally must be encrypted and secured for protection of an individual’s identity, especially when additional metadata about that individual providing the biometric sample is accumulated in the same data-gathering exercise. Synthetic biometric samples do not have this restriction.

A sensitive subject for some is the use of biometrics by governments. The U.S. Department of Defense's antiterrorism total information awareness system attracted significant congressional and public scrutiny concerning the privacy, policy, and potential abuses of a system whose intended purpose was to protect US citizens from individuals known to want to cause the USA harm. A concern about the potential ultimately led to the cancellation of the program and is summarized in a December 2003 audit report from the Inspector General of the U.S. Department of Defense [6].

There should be few if any restrictions on sharing the parameters used to create synthetic biometric samples or entire synthetic biometric databases. Further, assuming the modeling science can progress to an advanced state, the engineers and researchers could eventually create standard models, from which they would only need to exchange parameter settings to allow anyone to recreate specific or statistically similar synthetic biometric samples.

Another benefit of using synthetic biometrics is the cost and time savings from the need to acquire real biometric samples for testing systems. Provided the device acquisition and the impacts from factors like environmental changes are modelable, and the effects of presentation variations are well understood, realistic synthetic samples can be quickly generated. The synthetic samples can subsequently be used to augment or perhaps someday reduce the need for system scenario tests, saving money.

As with a number of technologies, synthetic biometrics generators have the potential for misuse. Among these uses are as rapid "hill-climbing" biometric generation devices that can be used to identify people in a biometric system that has not taken appropriate security safeguards to thwart hill-climbing attacks. Another potential misuse would be to characterize an individual's biometric with specific parameters, which could then be used to generate specific synthetic biometrics that could fool biometric systems across a wide variety of possible sensors and environmental conditions through the creation of phony biometrics. Fortunately, biometric

system engineers are cognizant of these potential security vulnerabilities and routinely take appropriate precautions to counter potential attacks from phony biometrics [7, 8].

Summary

Biometric technology becoming a ubiquitous addition to many modern security technologies. The synthesis of biometric samples has important benefits that may one day play an important role in the future of biometrics. The likelihood that image biometric sample synthesis of facial or body characteristics may become nothing more than a scientific curiosity is remote. This is due to the movie industry's quest to create lifelike animated avatars.

The biometrics industry lacks validated models. This shortfall remains one of the primary issues facing the use of synthetic biometrics. In addition, the accurate transformation of a specific synthetic biometric between sensors and environments remains as an important next step that has been achieved to a certain degree by at least some of the vendors of these products.

The ultimate potential for synthetic biometrics is providing a cost-effective method to avoid widely publicized biometric deployment failures. The poster child deployment failure was the Boston Logan Airport's attempt to utilize a face recognition system that according to reports failed to match the identities of 38% of a test group of employees. Had the deployment specifics (lighting conditions, algorithms, camera type, angles, etc.) been checked in the lab with a synthesized environment with injected real and synthetic biometric avatars, it is entirely possible that this snafu could have been avoided [9].

Despite some potentially negative uses, there are significant potential benefits from biometric sample synthesis. Increases in sophistication, reliability, and accuracy of synthetic biometrics will improve the potential for decreasing false match and false non-match rates in systems through the use of finely tuned biometric

samples to allow algorithm improvements to account for numerous noise inducing factors. This improvement would be cost effective and privacy enhancing – provided the synthetics accurately reflect what a real subject’s biometric would (or could) appear like to the system’s biometric template extraction and matching algorithms.

Biometric sample synthesis is a technology with promising applications – the potential of which has not been fully realized.

Related Entries

- ▶ [Biometric Vulnerabilities, Overview](#)
- ▶ [Face Sample Synthesis](#)
- ▶ [Fingerprint Sample Synthesis](#)
- ▶ [Iris Sample Synthesis](#)
- ▶ [Markerless 3D Human Motion Capture from Images](#)
- ▶ [SFinGe](#)
- ▶ [Signature Sample Synthesis](#)
- ▶ [Voice Sample Synthesis](#)

References

1. N.M. Orlans, D.J. Buettner, J. Marques, A survey of synthetic biometrics: capabilities and benefits, in *Proceedings of the International Conference on Artificial Intelligence (IC-AI'04)*, Las Vegas, Los Angeles, vol. 1, 2004, pp. 499–505
2. D.P. Greenberg et al., A framework for realistic image synthesis, in *Computer Graphics Proceedings of SIGGRAPH*, Los Angeles, vol. 1 (Los Angeles, 1997), pp. 477–494
3. D.J. Buettner, N.M. Orlans, A taxonomy for physics based synthetic biometric models, in *Proceedings of the Fourth IEEE Workshop on Automatic Identification Technologies (AUTOID'05)*, Buffalo, vol. 1, 2005, pp. 499–505
4. J. Daugman, The importance of being random: statistical principles of iris recognition. *Pattern Recognit.* **36**, 279–291 (2003)
5. A.J. Mansfield, J.L. Wayman, Best practices in testing and reporting performance of biometric devices version 2.01. Centre for Mathematics and Scientific Computing, National Physical Laboratory (NPL Report CMSC 14/02):10 (2002), http://www.npl.co.uk/upload/pdf/biometrics_bestprac_v2_1.pdf
6. Department of Defense Office of the Inspector General (Information Technology Management), Terrorism Information Awareness Program (D-2004-033), Dec 2003
7. C. Soutar, Biometric system security, p. 4, http://www.bioscrypt.com/assets/documents/whitepapers/biometric_security.pdf
8. C. Roberts, Biometric attack vectors and defences. *Comput. Secur.* **26**(1), 14–256 (2007)
9. S. Murphy, H. Bray, Face recognition devices failed in test at Logan. *The Boston Globe*, http://www.boston.com/news/local/articles/2003/09/03/face_recognition_devices_failed_in_test_at_logan. Accessed 3 Sept 2003

Biometric Security Standards

Greg Cannon¹, Asahiko Yamada², and Philip Statham³

¹Cross Match Technologies, Palm Beach Gardens, FL, USA

²IT Research and Development Center, Toshiba Solutions Corporation, Tokyo, Japan

³Biometrics Consultant, Specialising in Standards and Security Cheltenham, Gloucestershire, UK

Synonyms

ACBio instance

Definition

Biometrics holds out the promise of increased confidence in personal authentication processes compared with traditional passwords and tokens (e.g., keys and cards). This is because of the direct link between the biometric characteristic and the individual (strong binding) compared with the indirect link represented by passwords and tokens (weak binding).

Biometric systems are IT systems that include biometric recognition functionality. The security of biometric systems shares much with the traditional IT system security, but there are some factors that are biometric specific. These include threats such as spoofing and the personal nature of biometric data that require special handling.

The earliest work on biometric security standards has been related to biometric security management for the financial services sector. However the recent growth in the deployment of biometric systems, particularly in public domain applications such as passports, visas, and citizen cards, has given a strong impetus to the development of standards that address the comprehensive requirements of biometric systems and application security. Consequently, there is now a concerted effort by the two major standards groups involved ISO (International Organization for Standards)/IEC JTC 1 (Joint Technical Committee 1 (the IT Standards Committee of ISO)) SC37 (Biometric Standards Subcommittee of JTC 1) and SC 27 (IT Security Standards Subcommittee of JTC 1) to cooperate to develop the new guidelines and standards needed to deploy biometric systems securely in the modern world.

Current areas of study include:

1. Biometric security evaluation
2. Biometric transaction security
3. Protection of biometric data
4. Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics

Introduction

The rapid growth of biometric technology for authentication in public domain applications, such as passports, visas, border control, and citizen card schemes, is fuelling an intensive program of work to develop international standards for future biometric systems. The availability of standards provides suppliers with a set of specifications and “good practices” as targets for their products and gives system designers more confidence that their systems will work as intended and be interoperable with other products designed to conform to the same standards. Alongside the technical standards, corresponding security standards are needed to ensure that biometric applications can be designed, built, and deployed with adequate protection for the system and for its users.

Since biometric systems are also IT systems, the threats to security will share some aspects

with those of IT systems generally. However, there are specific considerations for biometric systems that lie outside the normal. These include areas such as vulnerabilities, which include the threat of spoofing with an artifact (e.g., gummy fingerprint), mimicry, the capture and replay of biometric data, and privacy concerns because of the personal nature of biometric data. Function creep and identity theft are examples of possible misuse that are particularly relevant to biometric applications. The consequence of these special factors is that, for biometric systems, security considerations need to extend beyond the system to include protection for the biometric data of individuals whose biometric data are processed by or stored on the system.

Although there is already a rich vein of IT security standards available that are applicable to biometric systems, the use of biometrics brings new biometric-specific security requirements that existing standards do not deal with. Biometric and IT security standards bodies are currently focused on the development of new biometric security standards that address the deficiencies.

The biometric and IT security standards communities need to collaborate closely because of the vital need for shared expertise and also because of the inevitable dependencies between standards specifying the technology and others aimed at security. For example, providing end-to-end security assurance of biometric transactions across a network will require security information to be generated and processed by the biometric hardware and software at each end of the connection as well as on the linking network. These endpoints are governed by the technical biometrics standards BioAPI (Biometric Application Programming Interface) [1] and CBEFF (Common Biometric Exchange Format Framework) [2] developed by SC 37, and these have strong interdependencies with ACBio (Authentication Context for Biometrics) [3], the biometric transaction security standard under development in SC 27. This and other examples are discussed in more detail in later sections of this entry.

Close liaison between SC 37 and SC 27 has existed since the formation of SC 37 in December

2002. Each subcommittee has appointed liaison officers who attend meetings of both the subcommittees and take responsibility for identifying projects requiring cooperation between SC 27 and SC 37 and ensuring that relevant experts can be provided to support them. Recent action taken by SC 37 will further strengthen the cooperation with SC 27 through a coordinated support group operating within SC 37. The motivation is not only for the reasons given earlier but also because much of the biometric expertise essential for the biometric security standards work is concentrated in SC 37.

The following sections of this entry provide a brief discussion of the biometric security issues currently being addressed by the standards community and the associated standards development projects. Readers should however note that, although the information here was correct at the time of writing, many of these standards are still in development and are evolving rapidly; in consequence, some of the information will inevitably become out of date. Readers are therefore urged to visit the Web sites of the relevant international standards subcommittees for the current status of biometric security standards. The URLs are listed in the reference section at the end of the entry [4,5].

Biometric Data Management Standards

Biometric Data Management is concerned with the broader issues of management and procedural measures for protecting biometric data. These include awareness training and accounting and auditing procedures as well as a reference to technical measures such as those described in this entry.

Historically, this work originated from the ANSI X9 subcommittee in the US X9.84 Standard – Biometric Information Management – Security (2003) [6]. X9.84 progressed into the international standards domain to become the starting point for the development of ISO 19092-2008, Financial services – Biometrics

– Security Framework [7]. ISO 19092 is a biometric-specific extension of ISO 17799, the Code of Practice for Information Security Management, which is now subsumed into the ISO 27000 family of ISMS standards [8].

Biometric Data Security Standards

Biometric data stored and processed in biometric systems are security sensitive. Their loss or disclosure could potentially lead to the undermining of the authentication integrity of the system and misuses such as function creep, identity theft, and breaches of personal privacy. The disclosure of biometric reference data (e.g., fingerprint templates) might provide identifying information for an attacker to transfer to an artifact for use in a spoofing attack, or to generate an electrical signal that could be directly injected in an electronic attack. If exported for use elsewhere without the authority of the individual, this would constitute function creep and possibly a breach of privacy. In many countries, such practices are regulated by data protection legislation or codes of conduct.

To guard against these threats, various procedural and technical measures can be employed. Current technical standards work focuses on the protection of stored biometric data, including biometric samples and biometric references, using cryptographic techniques such as digital signatures and encryption.

The core standard for biometric data storage and exchange is ISO/IEC 19785 CBEFF (Common Biometric Exchange Format Framework). CBEFF is a multipart standard where Part 4 – Security block format specifications – provides for the protection of biometric data integrity and confidentiality.

The CBEFF standard defines a basic block of biometric data called a BIR (Biometric Information Record). The BIR is further subdivided into a standard block header (SBH), a biometric data block (BDB) containing the biometric data themselves (which may be encrypted), and a security block (SB). The SBH header includes indicators of the security mechanisms that are

used to protect the data. The SB security block contains relevant security information such as cryptographic checksums, digital certificates, and data encryption algorithm specifications that are used to guarantee the integrity and confidentiality of the data. The details of these options and the structure of SB are being standardized in 19785-4 CBEFF Part 4, using the Internet Society's RFC 3852 CMS (Cryptographic Message Syntax) [9]. The specifications within the CBEFF security block are planned to encompass the security requirements associated with the ACBio (Authentication Context for Biometrics) standard [3], which is being developed in SC 27 to provide end-to-end assurance for biometric transactions. Essentially, the CBEFF security block will contain a set of ACBio instances which contain data that can be used to validate the end-to-end integrity of the biometric transaction. Further information on ACBio appears in the next section of this entry.

SC 37 biometric standards are being modified in order to support ACBio. The effect on CBEFF has been described, but the BioAPI (ISO/IEC 19784-1 Information technology – Biometric Application Programming Interface – Part 1: BioAPI specification) is also in the process of being updated to accept BIRs, including security blocks. An Amendment 3 to the BioAPI standard is under development to deal with the extended requirement for the provision of security of data.

One approach to protecting biometric data is to replace the central database of biometric references by storage of each enrollee's reference on a personally held smart card. This is often advocated by groups concerned about the privacy implications of centralized biometric databases. Secure smart cards could also provide the necessary biometric processing, the main system capturing the biometric sample, passing the sample to the smart card for matching against the reference stored on the card, and authenticating the result delivered by the smart card. This is what is known as "on-card matching." A claimant could carry the smart card with him/her, present the card to the system together with a biometric sample, and assure the system that he/she is genuine by allowing the secure processor of the smart

card to perform the comparison between the live sample and the stored reference. In this way, the biometric data and the comparison algorithm are immune from attacks on the central system.

The SC 37 19794-2 Fingerprint Minutia Standard includes a section specifying a compact format fingerprint minutiae standard suitable for the limited storage capability of smart cards. We envision that more standards may be necessary, especially standards that allow for more interoperability between the smart card and the IT system.

Biometric Transaction Security Standard: ACBio

Transaction security standards are well established in the IT world, principally driven by the banking and financial sectors where transactions need to be secure not only over private networks but also between banks and customers using the Internet. These standards typically involve secure protocols using digital certificates and data encryption to guarantee the integrity and confidentiality of remote transactions. If transactions are to include biometric authentication, the security envelope needs to extend to provide assurance for the biometric elements of the transaction. Such assurance might include the authentication of the biometric hardware (e.g., fingerprint reader), certification of biometric performance capability, the quality of the current biometric authentication instance, and the integrity of the biometric data transfer process.

This is the scope of the SC 27 standard 24761 Authentication Context for Biometrics (ACBio) [3]. ACBio specifies the structure of data that can provide the necessary assurance for a remote biometric verification transaction.

ACBio models a biometric transaction as a set of processes executed by Biometric Processing Units (BPUs). A BPU places relevant security data into a block called an ACBio instance. BPUs generate and transmit ACBio instances together with the associated biometric transaction data. ACBio instances secure the integrity of the data, using security techniques such as digital signa-

tures and cryptographic checksums. ACBio instances can also contain data that provide the means of assuring other aspects of the transaction such as validation of the biometric hardware used and the certification of the performance capability of the biometric verification process.

Transactions passing between BPUs will typically accumulate a collection of ACBio instances associated with the various processing stages. Each ACBio instance will contain security markers (cryptographic checksums, digital signatures, etc.) that can provide assurance for the corresponding process stages. Further details are beyond the scope of this entry, but the security techniques used can provide protection against the substitution of “bogus” components and data replay attacks as well as general threats to the integrity of the transaction data.

ACBio instances depend on other biometric and security standards for their operation and effect. Interdependencies with the CBEFF and BioAPI standards have already been described in the *Biometric Data Security Standards* section. Other standards are also referenced by ACBio. An ACBio instance uses data types defined in the RFC 3852 CMS (Cryptographic Message Syntax) standard [2]. ACBio instances also use X.509 digital certificates [10]. For the certification of biometric performance capability, ACBio calls on the SC 37 19795 series of biometric performance test standards [11]. To provide test results in a suitable format for use by ACBio, work has begun in SC 37 on the 29120 standard: machine-readable test data for biometric testing and reporting [12]. Work is also expected in SC 27 to produce a standard for the electronic format of cryptographic modules that will be used by ACBio. Finally, ACBio refers to the SC 27 19792 Biometric Evaluation Methodology standard [13] to provide security assurance for the biometric hardware and software used in an application.

ACBio will therefore use existing cryptographic and digital certificate techniques to assure transaction data integrity end-to-end. The integrity of the biometric hardware and the performance and security of the biometric technology will be provided by external evaluation schemes, and the results will be

embedded in machine-readable data formats that can be authenticated by the validation of the biometric verification process as required.

The multiple dependencies between SC 27 and SC 37 standards for the successful operation of ACBio call for close ongoing cooperation between the two subcommittees to ensure consistency and interoperability of the standards. Other collaborations are also required. In the area of smart cards, there is collaboration between SC 17 and SC 27 to include in ACBio an informative annex of command sequences for the realization of ACBio on STOC (STore On Card) cards and OCM (on-card matching) cards. An STOC is a smart card that stores the biometric reference data on the card, but does not perform the biometric verification, and an OCM card is a smart card that both stores biometric reference data and performs the biometric comparison between the reference and the input biometric sample data.

Biometric System Security Evaluation Standards

Historical Background

Biometrics is about identification and verification. However, in many systems, failures of identification or verification will have security implications. Often the reason that biometric technology is used is because of the perceived increase in assurance of correct identification or verification that biometrics will provide. However, to reliably assess this level of assurance, a properly constituted security evaluation procedure is needed.

Security evaluation of IT systems is now well established. Various evaluation schemes exist for specific market sectors such as antivirus products and smart cards. The internationally recognized standard for IT security evaluation is ISO 15408 – Common Criteria [14]. This is a government-developed scheme aimed primarily at evaluation for government use, but it is also recognized and used commercially as a “gold standard” for security evaluation. Evaluations are performed by government-licensed evaluation laboratories in member countries, and the results are recog-

nized across the participant countries (and wider) through a mutual recognition agreement.

Although the Common Criteria evaluation methodology is generic and therefore suitable for biometric system evaluations, there are a number of special factors that need to be considered when undertaking biometric system security evaluations. These include statistical performance testing and biometric-specific vulnerabilities. This was first recognized during a pioneering Common Criteria evaluation of a biometric fingerprint verification system in Canada in 2000 [15], which led the evaluation team to investigate and develop the methodology to deal with the special factors. Subsequently, this work was further developed by an informally constituted group of biometric and Common Criteria experts to produce a biometric evaluation addendum for the Common Criteria Methodology known as the Biometric Evaluation Methodology or BEM [16]. The BEM describes the special requirements of a biometric system security evaluation and gives guidance to evaluators on how to address these requirements in a Common Criteria evaluation. At the time of writing, the BEM had not attained official status as a formal part of CC methodology. Nonetheless, it is frequently referenced as a source of information on CC and other security evaluations of biometric products and systems.

ISO/IEC 19792: Information Technology, Security Techniques, Security Evaluation of Biometrics

This international standard is currently under development in SC 27 [13]. Project 19792 is not targeted at a specific evaluation scheme such as Common Criteria; rather, its aim is to provide guidance to developers and evaluators on security concerns for biometric systems and to specify a generic methodology for their evaluation. It is similar to the BEM, but is not limited to Common Criteria evaluations and contains more detailed information on potential threats, countermeasures, and evaluation requirements. Like the BEM, it assumes that evaluators are

familiar with the broader IT security evaluation issues and does not address these.

19792 covers biometric-specific security issues of the system as a whole as well as threats and potential vulnerabilities of the component parts. It describes technical and nontechnical threats and how these may be reduced or eliminated by appropriate countermeasures. It provides guidance to evaluators on testing and the assessment of potential vulnerabilities and countermeasures, and it defines the responsibilities of vendors and evaluators in the evaluation process.

Biometric-specific aspects of system security and evaluation methodology covered by 19792 include the following.

Statistical Performance Testing

Biometric comparison decisions (match and non-match) are not certainties, but are prone to false match and false non-match errors. Comparison results are therefore often expressed in terms of the probabilities of correct and incorrect decisions, the actual numbers being expressed in terms of statistical performance figures. An example of what this means in practical terms is that for an access control application with a false match rate of 1%, if 100 randomly chosen impostors were to present their own biometric characteristic to the system while claiming to be legitimate enrollees, one of them might succeed in gaining admittance through chance error. The quantification of errors through robust performance testing therefore forms one part of a biometric system security evaluation. The international standard for biometric testing and reporting is provided by the multipart ISO/IEC standard 19795 [11].

The significance of biometric error rates to security depends on the purpose of the identification or verification in the application domain. For access control, the false match rate may be the most important security relevant factor, but for applications such as passport or ID card registration, an important requirement will be the successful detection of attempts to register multiple times under different claimed

identities. Here, the system needs to search its biometric database to determine if there is an apparent match with any existing enrollee. If a false non-match occurs during the search, a multiple enrolment attempt may succeed, and therefore for this function, the false non-match rate statistics will be the most important security consideration.

Biometric System Threats and Countermeasures

The use of biometrics brings potential security threats and vulnerabilities that are distinct from those of other IT technologies, including spoofing, mimicry, and disguise. Further details of these threats and examples of countermeasures can be found in the definitional entries for Biometric System Threats and Countermeasures.

Human Security and Privacy Concerns

Since biometric systems collect and store the personal data of its enrollees, security measures are necessary to protect the data and the privacy of the enrollees. This is another important difference between systems using biometrics for authentication and those that depend on inanimate entities such as passwords and tokens.

People have a right to privacy regarding the use and sharing of their personal data, that is, data about their lifestyle, preferences, habits, etc., that can be linked to them as individuals. Such data should be collected, processed, and stored only with the informed consent of the individual and only for the declared and authorized purpose. Unauthorized disclosure and misuse can lead to undesirable consequences such as identity theft and function creep. Biometric data are regarded as particularly sensitive, because their strong binding to specific persons may make it difficult for individuals to repudiate transactions authorized by biometric authentication.

Technical security measures such as data encryption and the use of cryptographic signatures to bind data to an application can help to secure biometric data, but usually, complete protection also requires administrative controls and sanctions implemented within an overall system security policy.

Future Directions for Biometrics Security Standards

The first generation of biometric standards may be characterized as a collection of largely self-contained or stand-alone parts that provide the essential building blocks for future biometric systems. These building blocks are now largely in place, but the course of their development has uncovered new areas of work that need to be addressed by a second generation of biometric standards.

Building on the experience of developing the earlier standards, the second generation will target the broader requirements for system and application level standards. The new standards will tackle areas that were omitted from the first-generation standards and serve to bind together the earlier work to furnish a comprehensive standards package that will meet the wider systems and application-level standards requirements. Biometric system designers and implementers need these standards to support the rapid growth in large public domain biometric systems that we are now seeing, including passports, visas, border control applications, and financial transaction systems. Many of these systems are international in reach and raise important privacy and other human concerns as well as major technical challenges.

In the security area, work is needed on standards that deal with such issues as:

1. The use of multimodal biometrics to increase the security that biometric authentication offers
2. Comparing and quantifying the security capabilities of biometrics and password- and token-based authentication technologies individually and in combination
3. Assessing the requirement for biometric performance in the context of a system where biometrics provides only one element of security as part of an overall system security policy
4. The potential role of biometric authentication in identity management systems
5. Locking biometric data to specific applications to prevent misuse and potential identity theft

6. Referencing, interpreting, and using other relevant security standards, for example, US Government Federal Information Processing Standards FIPS 140 for data encryption, X.509 digital certificates, in the domain of biometric security standards

Some groundwork has already begun. In the United States, the International Committee for Information Technology Standards (INCITS) M1 Standards Committee has picked up on earlier work by the US National Institute of Standards and Technology (NIST) on Electronic Authentication and E-Authentication for US Federal Agencies [17, 18] and produced a study report on the use of biometrics in e-authentication [19].

A special group has been formed by SC 37 to study and develop a proposal for future work on providing guidance for specifying performance requirements to meet security and usability needs in applications using biometrics. Both this initial study and any subsequent work will require close cooperation and involvement of experts from other standards subcommittees, in particular SC 27.

Related Entries

- ▶ [Biometric Technical Interface, Standardization](#)
- ▶ [Finger Data Interchange Format, Standardization](#)
- ▶ [Performance Testing Methodology Standardization](#)

References

1. ISO/IEC JTC 1 SC 37 19784 Biometric Application Programming Interface (BioAPI). Multi-part standard, some parts under development at the time of writing
2. ISO/IEC JTC 1 SC 37 19785 Common Biometric Exchange Format Framework (CBEFF). Multi-part standard, some parts under development at the time of writing
3. ISO/IEC JTC 1 SC 27 24761 Authentication Context for Biometrics (ACBio). Standard under development at the time of writing
4. SC 27 http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45-306. Accessed 30 Oct 2007
5. SC 37 http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=31-3770. Accessed 30 Oct 2007
6. ANSI X9.84 Biometric information management and security for the financial services industry, see: http://www.techstreet.com/cgi-bin/detail?product_id=1327237 for further details. Accessed 30 Oct 2007
7. ISO 19092-2008 – Financial services – biometrics – security framework. ISO 19092-1, see: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?cnumber=50145 for further details. Accessed 30 Oct 2007
8. ISO 27000 family of Information Security Management Systems (ISMS) standards, see: <http://www.itgovernance.co.uk/infosec.aspx> for further details. Accessed 30 Oct 2007
9. RFC Cryptographic Message Syntax 3852. The Internet Society, see <ftp://ftp.rfc-editor.org/in-notes/rfc3852.txt>. Accessed 30 Oct 2007
10. ITU-T X.509 Information technology – open systems interconnection – the directory: public-key and attribute certificate frameworks
11. ISO/IEC JTC 1 SC 37 19795 Biometric testing and reporting. Multi-part standard, some parts under development at the time of writing
12. ISO/IEC JTC 1 SC 37 29120 Information technology: machine readable test data for biometric testing and reporting. Multi-part standard under development at the time of writing
13. ISO/IEC JTC 1 SC 27 19792: Information technology – security techniques – security evaluation of biometrics. Standard under development at the time of writing
14. ISO/IEC 15408, Common criteria for information technology security evaluation, <http://www.commoncriteriaportal.org/>
15. Bioscrypt™ enterprise for NT logon, version 2.1.3: common criteria evaluation <http://www.cse-cst.gc.ca/services/cc/bioscrypt-eng.html>. Accessed 30 Oct 2007
16. Common Criteria, Common evaluation methodology for information technology security evaluation – Biometric Evaluation Methodology supplement (BEM), http://www.cesg.gov.uk/policy_technologies/biometrics/media/bem_10.pdf
17. NIST SP800-63, Electronic authentication guideline, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. Accessed 30 Oct 2007
18. OMB M-04-04, E-authentication guidance for federal agencies, <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>. Accessed 30 Oct 2007
19. INCITS M1/06-0642 study report on biometrics in E-authentication, <http://m1.incits.org>

Biometric Sensor and Device, Overview

Geppy Parziale
 INVASIVECODE INC., San Francisco,
 CA, USA

Synonyms

Biometric sensors; Biometric devices

Definition

A biometric sensor is a transducer that converts a biometric trait (fingerprint, voice, face, etc.) of a person into an electrical signal. Generally, the sensor *reads* or *measures* pressure, temperature, light, speed, electrical capacity, or other kinds of energies. Different technologies can be applied to achieve this conversion using common digital cameras or more sophisticated combinations or networks of sensors.

It is important to highlight that the output signal of a sensor or device is only a representation of the real-world biometrics. Hence, if B is a biometrics of a real world and s is the transfer function of a sensor or a device, the output signal is $B' = s(B)$ and $B' \neq B$.

A biometric device is a system which a biometric sensor is embedded in. Communication, processing, and memory modules are usually added to provide additional functionalities that the biometric sensor cannot if standalone.

Interchanging the terms *sensor* and *device* is very a common practice, even if they are two different concepts. A sensor is responsible only for the conversion of biometrics into an electrical signal. Instead, when a processor and a memory module are also involved, the term device is more appropriate.

Introduction

Biometric identification and verification are slowly penetrating the security market. The convenience of avoiding to recall passwords

and/or loose tokens (id cards, smart cards, etc.) is one of the strongest advantage of biometrics compared to the legacy security tools. Moreover, biometrics concretely links a person to her/his identity, compared to the traditional approaches that associate the person identity to a token or a password that can be forged, lost, forgotten or used by other people.

The most sensitive step in the biometric authentication chain is the biometric capture. The accuracy and the repeatability of this process influence the remaining steps of the chain. Since the output signal of a device is only a representation of the real-world biometrics, the choice of the representation type is a very important issue, because it should try to meet the four biometric axioms: uniqueness, repeatability, permanence, and collectibility [1]. However, this is a very complex task influencing the choice of a technology used and the design of the sensor/device for a defined application.

Biometric sensors must be designed taking into account many factors. User convenience, portability, electrical and optical characteristics, and price are only some of them. They are very important factors when choosing among different sensors for a defined application. However, they cannot be always met and the right balance of these factors has to be found according to the final application in which a biometric sensor will be involved.

Below, the main features of a biometric sensor and device are reported. This is not intended to be an exhaustive list of features and only the most important characteristics are highlighted.

User Acceptance

User acceptance is an important factor that has to be taken into account during the choice of a technology and the design of a biometric device. Easy-to-use devices are preferable to user-unfriendly ones. For example, devices pointing lasers to the eyes or providing small electrical current to the body of a person are for sure difficult to be accepted by the final user. Sensors touching a person body are less preferred than

remote sensors or device reused to touch many individuals are not well accepted for hygienic reasons. Some biometric devices could be difficult to be accepted because of cultural or religious motivations.

In general, biometric sensors and devices can be classified into two main families: *intrusive* and *nonintrusive*. The closer the device to the person, the more intrusive the device. For example, a surveillance camera able to identify people face remotely is less intrusive than imaging sensors touching the user eye to scan the retina.

Some biometric devices need the user to cooperate during the capture and offer her or his own biometrics. Other devices do not need any user cooperation. Moreover, when an operator is needed during the normal use, the device can be classified as a *supervised device*, while when the user can operate the sensor with no extra support, it can be classified as an *unsupervised device*. Usually, unsupervised devices are preferred to supervised ones, because they do not need extra human resources to operate.

Portability

Form factor and weight are sometimes very important characteristics that must be taken into account during the design of a biometric sensor, because they can influence its portability. Embedding a face or fingerprint or iris sensor (or all together) in a mobile handheld computer or laptop or cell phone is becoming a very attractive solution for different kinds of applications. When the portability is important, the sensor is usually embedded in a more complex device containing all the functionalities (signal processing, communication, matching, etc.) that the biometric sensor cannot provide alone. The possibility to process locally the captured biometrics requires the existence of processor and memory modules. Instead, when the processing is performed remotely a communication interface must be considered as part of this more complex device. In both cases, the power consumption becomes an issue, because the need of supplying the energy through portable batteries can limit the choice of the technology.

Ruggedness and Lifetime

When a biometric device has to be installed or carried in difficult environments (very low or high temperature, high humidity, vibrations, dust, noisy locations) or when mechanical moving parts are involved (line-scan cameras, auto-focusing cameras, auto-position sensors, etc.) important features are the ruggedness and the lifetime. These influence the maintenance costs of the device. Thus, during the design, these features have to be taken into account and special housing or materials must be used for the sensor manufacturing.

Calibration

The standard functionality of a sensor is usually influenced by the external or internal factors and thus, it can change during time, due to temperature, pressure or humidity variations or due to some mechanical movements. To reduce this problem, sensors need to pass a periodical procedure to restore the initial operational conditions. This process is called sensor or device calibration.

Calibration refers to different processes used according to the type of sensor and the technologies involved for the capture. Electrical calibration is the process used to restore the initial electrical conditions that could change over time due, for example, to temperature variations. Mechanical calibration is performed instead when a device has moving parts. In this case, mechanical friction starts to appear during the normal sensor life, altering the measure the sensor was designed for. Optical calibration is instead the process used to refocus lenses or reestablish the initial illumination conditions.

The calibration is sometimes a process that is also needed when the sensor is used for the first time (out of the box). Due to inaccuracies of the manufacturing, the sensor functionality can be slightly different than the defined one. Positioning, orientation, or placement of sensor parts can be sometimes very difficult and the production

process are usually not free of imperfections. Thus, the first time the device is used and then periodically, a calibration procedure is needed. This can be a manual, semiautomatic, or fully automatic procedure. Fully automatic calibration is usually possible when the biometric device does not contain mechanical and optical parts. In this case, the sensor calibration is usually obtained using special electrical circuits controlling the status of the device and reestablishing the correct initial electrical conditions. Optical calibration often requires the use of special optical targets. These are mechanical models used to measure predefined known values against which the output of the sensor is compared. Mechanical calibration is usually done manually by an experienced operator, reviewing all the mechanical functionalities.

Operating Conditions

The set of conditions (e.g., voltage, temperature, humidity, pressure, etc.) over which specified parameters maintain their stated performance rating are called *operating conditions*. When these are not respected, the biometric sensor could not work as defined by the manufacturer. The operating conditions must be chosen according to the final sensor applications. Sensors used for military applications have usually very large operating conditions and the devices are supposed to work under huge stress (high or low temperatures, vibrations, dust, high humidity, etc.). As other electrical or mechanical components, biometric sensors must meet some standard requirements and pass a certification process. For example, ISO certifications define the electrical and mechanical characteristics that an electronic device should meet to be sold.

Sensor Interface

The possibility to interface a sensor or device with other sensors or devices and with a processing unit is an important feature that must be considered when choosing a sensor for a defined

biometric application. USB and Firewire can be the best choice, when the biometric sensor needs to be connected to a standard PC. When the data throughput is an issue, optical fibers or gigabit ethernet are possible solutions. Moreover, if the quantity of data the sensor has to transfer to a processing unit is large, the interface must be able to transfer this data as fast as possible to avoid long latency. Wired or wireless communication interfaces can be chosen according to the final application.

Power Supply

Low-current absorption is usually a very required feature for a biometric device, because this facilitate to embed it in other devices. Usually the basic sensors (e.g., cameras and microphones) do not need to drain too much current, but when illuminators (Light Emission Diode or optical fibers) or mechanical movements (line scanning cameras) or heating generators (palmprint devices reducing the halo effect) are involved, then extra power is needed. Modern communication interfaces as USB 2.0, Firewire, and Ethernet can supply power to the sensor with no need of extra wires. This is a very interesting alternative especially when the biometric application requires a portable device connected to a laptop.

Failure Rate

Failure Rate is the frequency with which an engineered system or component fails. It can be expressed in failures per hour. Mean Time Between Failures (MTBF) is the mean (average) time between failures of a system, and is often attributed to the useful life of the device i.e., not including infant mortality or *end of life*, if the device is not repairable. Calculations of MTBF assume that a system is renewed, i.e., fixed, after each failure and then returned to service immediately after failure. The average time between failing and being returned to service is termed mean down time (MDT) or mean time to repair (MTTR).

Cost

The cost of a biometric device or sensor is a very important factor influencing the final target application in which the device or the sensor will be involved. The final costs depend on many factors. The availability of the basic technology used for the biometric capture is one of them. If special and sophisticated technologies are used instead of the common ones, the costs of the device increase. Moreover, the production materials, the manufactured number of samples, and the maintenance are also factors influencing the final costs.

Sensor Resolution

Sensor resolution refers to the ability of a device to acquire, scan, or distinguish details of the acquired biometric trait. Depending on the sensor type, it can be distinguished among spatial, frequency, time, and radial resolution. For example, a face device can be an area sensor and its spatial resolution measures the quantity of details of the face skin it can acquire.

Spatial resolution represents the number of pixels in a unitary length and is usually expressed in *pixel per inch* or shortly, *ppi*. *Frequency resolution* represents the ability of a device to distinguish frequency variations. *Time resolution* measures the ability of a sensor to distinguish time variations. For example, microphones used as speech devices should have a certain capacity to recognize fast speakers. *Radial resolution* represents the ability of a sensor to distinguish variation in the distance.

The increase in the resolution increases the accuracy of the sensor and usually its final cost. In many applications, a trade-off between resolution and final cost must be found.

Optical and Imaging Characteristics

When a biometric sensor generates as output signal an image and an optical system is involved

in the capture process, the choice of a sensor is based on optical characteristics.

Image Depth or *Dynamic Range* determines how finely a sensor can represent or distinguish differences of intensity. It is usually expressed as a number of gray levels or bits. For example, 8 bits or 256 gray levels is a typical dynamic range of fingerprint image or 24 bits or 256 Red, Green, and Blue (RGB) levels which is typical of face image.

The Modulation Transfer Function (MTF) or *Spatial Frequency Response* represent the relationship between the input and the output signal of a sensor. Spatial frequency is typically measured in cycles or line pairs per millimeter (*lp/mm*). The more extended the response, the finer the details and the sharper the image. MTF is the contrast at a given spatial frequency f relative to contrast at low frequencies, and it can be computed with the following (1):

$$\text{MTF} = 100\% \frac{C(f)}{C(0)}, \quad (1)$$

where $C(f) = (V_{max} - V_{min}) / (V_{max} + V_{min})$ is the contrast at frequency f and $C(0) = (V_W - V_B) / (V_W + V_B)$ is the low frequency contrast. V_B , V_W , V_{min} and V_{max} represent the luminance for black areas, the luminance for white areas, the minimum luminance for a pattern near spatial frequency f and the maximum luminance for a pattern near spatial frequency f , respectively.

Geometric Image Accuracy represents the absolute value of the difference $D = X - Y$, between the distance X measured between any two points on the input image and the distance Y measured between those same two points on the output image. This is a very important parameter especially for devices having a very large capture area. This feature is measured using special optical targets.

The capacity of a sensor to capture the whole biometrics in a single image is expressed by the *Field of View* (FoV). For a digital camera, this represents the angular extent of the observable object that is seen at any given moment. For some biometric devices, it is fundamental to capture the biometrics in a single capture. For example,

hand geometry devices need to capture the full hand in a single shot. Sweep fingerprint sensors allow only the capture of a fingerprint in different instant of times, since their FoV is very limited.

Precise focus is possible at only one distance; at that distance, a point object will produce a point image. *Depth of Field* (DoF) represents the range of distance in which the object remains focused. This is a very important feature for remote cameras, since it represents the location in which the biometrics must be placed to be always focused.

The *Intensity Linearity* represents the capacity of a device to reproduce the intensity level values correctly. To prove this feature, a target with gradually varying grayscale levels is usually used for this scope. The grayscale levels on the output image are compared with the grayscale levels on the input target to measure the accuracy of the representation. Large variations in the representation lead that the sensor is calibrated.

The Signal-to-Noise Ratio is a measure of the level of noise introduced by the sensor during the biometric capture. This is usually measured using a special optical target representing an intensity level as a reference.

The *Frame Rate* is the number of frames per unit time that a sensor can generate. It is usually measured in *frames/s*. These parameter is very important when the object movements are involved (sweep devices, touchless devices, gait device, face device) during the biometric capture.

In optics, the *F-number* (sometimes called focal ratio, f-ratio, or relative aperture) of an optical system expresses the diameter of the entrance pupil in terms of the effective focal length of the lens; in simpler terms, the f-number is the focal length divided by the aperture diameter. It is a dimensionless number that is a quantitative measure of lens speed, an important concept in photography.

The *Shutter Speed* is the time that a detector needs to capture a single image. In photography, shutter speed is the length of time while the shutter is open; the total exposure is proportional to this exposure time or duration of light reaching the film or image sensor.

Summary

Biometric sensors and devices are slowly penetrating the security market, because of the advantages of biometrics with respect to traditional security means as passwords and tokens. The choice of a sensor for a defined application is usually dependent on some electrical, ergonomic, optical, mechanical, and other characteristics. An overview of these important features has been reported here.

Related Entries

- ▶ [Biometric Sample Acquisition](#)
- ▶ [Biometric Verification/Identification/Authentication/Recognition: The Terminology](#)

Reference

1. J. Clark, A. Yulle, *Data Fusion for Sensory Information Processing Systems* (Kluwer Academic, Boston, 2009)

Biometric System Design, Overview

Anil K. Jain¹ and Karthik Nandakumar²

¹Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA

²Institute for Infocomm Research, A*STAR, Fusionopolis, Singapore

Definition

Biometric system design is the process of defining the architecture, selecting the appropriate hardware and software components, and designing an effective administration policy such that the biometric system satisfies the specified requirements. The requirements for a biometric system are typically specified in terms of six major design parameters, namely, accuracy, throughput, cost, security, privacy, and usability.

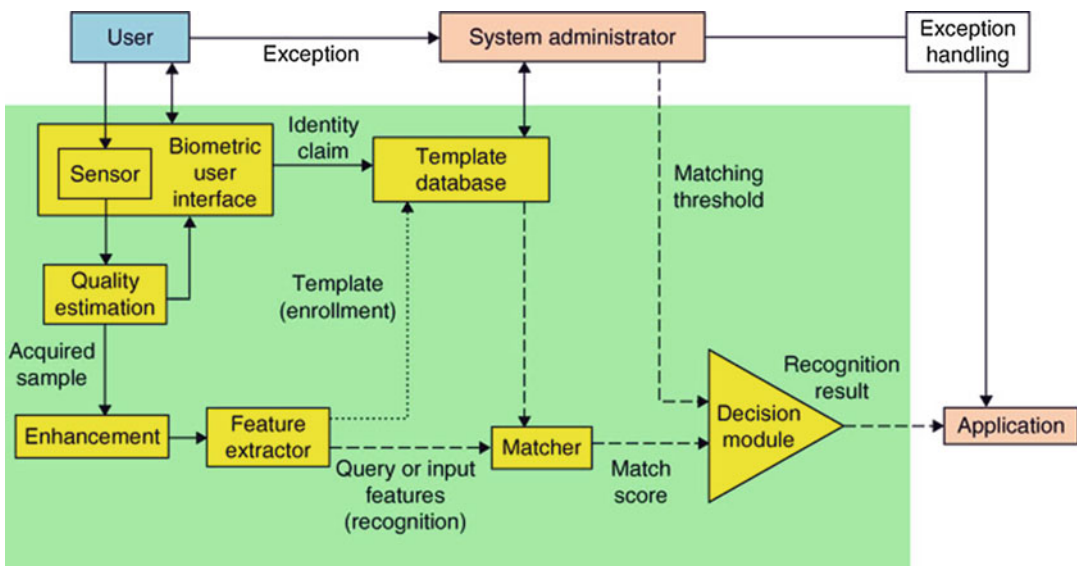
Introduction

In general, biometric systems consist of seven basic modules that operate sequentially [1], as shown in Fig. 1. These building blocks or modules include (i) a user interface incorporating the biometric reader or sensor, (ii) a quality check module to determine whether the acquired biometric sample is of sufficient quality for further processing, (iii) an enhancement module to improve the biometric signal quality, (iv) a feature extractor to glean only the useful information from a biometric sample that is pertinent for the person recognition task, (v) a database to store the extracted features along with the biographical information of the user, (vi) a matcher to compare two feature sets during recognition and to determine their degree of similarity and (vii) a decision module that determines the user identity based on the similarity, (match scores) output by the matcher.

Though all biometric systems are composed of the same basic modules, there are three main steps involved in the design of a biometric system. Firstly, the designer needs to choose the appropriate architecture for a biometric system. Secondly, the hardware and software components

required for the implementation of the architecture must be selected. Finally, appropriate policies must be defined for the effective administration of the biometric system. Before the essay dwells deeper into these three issues, it is important to remember that the goal of any design process is to develop a system that satisfies the *requirements* of the *application*. Hence, most of the design decisions in a biometric system are fundamentally driven by the nature or functionality of the application and the specified requirements.

The functionalities provided by a biometric system can be broadly categorized as *verification* and *identification* [2]. In verification, the user claims an identity, and the system verifies whether the claim is genuine by comparing the input biometric sample to the template corresponding to the claimed identity. In identification, the user's biometric input is compared with the templates of all the persons enrolled in the database, and the system returns either the identity (in some scenarios, multiple identities whose templates have high similarity to the user's input may be returned by the system.) of the person whose template has the highest degree of similarity with the user's input or a decision indicating that the user presenting the input is not an enrolled user.



Biometric System Design, Overview, Fig. 1 Basic building blocks of a biometric system

Design Specifications

The six basic design specifications [3] of a biometric system are presented below. While some of the parameters like accuracy and throughput can be measured quantitatively, factors such as security, privacy, and usability are generally addressed in a qualitative manner.

Accuracy

A biometric system can make two types of errors, namely, false nonmatch and false match. When the intra-user variation is large, two samples of the same biometric trait of an individual (mate samples) may not be recognized as a match, and this leads to a false nonmatch error. A false match occurs when two samples from different individuals (nonmate samples) are incorrectly recognized as a match due to large interuser similarity. Therefore, the basic measures of the accuracy of a biometric system are False Nonmatch Rate (FNMR) and False Match Rate (FMR). In the context of biometric verification, FNMR and FMR are also known as False Reject Rate (FRR) and False Accept Rate (FAR), respectively. In biometric identification, the false match and false non-match errors are measured in terms of the False Positive Identification Rate (FPIR) and False Negative Identification Rate (FNIR), respectively [4].

Accuracy requirements for a biometric system depend on the application. For example, a verification application usually involves co-operative users and may require a low FMR (0.1 % or less), while a relatively high FNMR (1–5 %) may be acceptable. On the other hand, a negative identification application like airport screening may require both a low FNIR to prevent undesirable individuals from circumventing the system and a low FPIR to avoid causing inconvenience (in the form of secondary screening) to the other passengers.

Throughput

Throughput refers to the number of transactions that can be handled by the biometric system per unit time. Since the input is matched only to a

single template in verification, throughput is not a major issue in verification systems. However, for the sake of user convenience, it is essential that the entire process of sample acquisition, feature extraction, and matching be completed within a few seconds even in verification applications. Throughput is a major concern in the identification mode because it requires matching the biometric query to all the templates in the database. Therefore, large-scale identification systems employ special schemes (both hardware and software) such as indexing, binning, or filtering to facilitate efficient searching of the database and thereby improve the system throughput.

Cost

The cost of a biometric system includes the cost of all the components of the biometric system and the recurring costs required for the operation, maintenance, and upgrade of the system. Often, there is a trade-off between the cost of the biometric components and the performance (accuracy, throughput, and usability) of the biometric system. Furthermore, the intangible costs such as those incurred due to the errors made by the biometric system must also be considered while designing a biometric system. A thorough cost-benefit analysis is essential prior to any biometric system deployment.

Security

Since biometric systems provide a more secure and reliable authentication functionality compared to password and token-based systems, it is now being widely deployed in many real-world applications. However, the biometric system itself is vulnerable to a number of attacks [5] such as usage of spoofed traits and tampering of biometric data, communication channels, or modules. These attacks may either lead to circumvention of the biometric system or denial of service to legitimate users. Hence, a systematic analysis of these security threats is essential when designing a biometric system.

Privacy

While biometrics facilitates secure authentication by providing an irrefutable link to the identity of a

person, it also raises privacy concerns. One major objection raised by privacy experts is the problem of function creep, where the acquired biometric data is abused for an unintended purpose. For example, allowing linkage of identity records across biometric systems may facilitate tracking of users without their knowledge. Hence, due diligence must be exercised during the design process, and appropriate checks and balances must be incorporated in the biometric system to protect the privacy of users [6].

Usability

Usability of a biometric system can be measured in terms of different factors, like effectiveness (Can users successfully provide high-quality biometric samples?), efficiency (Can users quickly authenticate themselves without errors?), satisfaction (Are users comfortable using the system?), and learnability (Do users get habituated to the system?) [7]. Two common metrics used to measure the effectiveness of use of a biometric system are the failure to enroll rate (FTER) and failure to capture rate (FTCR). If an individual cannot interact correctly with the biometric user interface or if the biometric samples of the individual are of very poor quality, the sensor or feature extractor may not be able to process these individuals. Hence, they cannot be enrolled in the biometric system, and the proportion of individuals who cannot be enrolled is referred to as FTER. In some cases, a particular sample provided by the user during authentication cannot be acquired or processed reliably. This error is called failure to capture, and the fraction of authentication attempts in which the biometric sample cannot be captured is denoted as FTCR. Usability depends on the choice of the biometric trait, the design of the user interface, and sensor quality.

Design Issues

Given the design specifications of the biometric system and the nature of the biometric system, a system designer needs to address the following three issues systematically.

Biometric System Architecture

Architecture of a biometric system is primarily defined by the storage location of the templates and the location of the matcher. The templates (or the template database) may be stored in (1) a centralized/distributed server, (2) a local workstation at the client side, and (3) a portable device such as smart card or token that is in the possession of the user. Similarly, matching may also take place at any one of the above three sites. This allows for a wide range of possible architectures ranging from a fully centralized model, where the templates reside on the server and matching also takes place at the server, to a completely decentralized model (e.g., match-on-card or system-on-device), where all the biometric processing takes place on the device and the template never leaves the device. Other intermediate architectures are also possible. For example, the template may be stored on a smart card, and during authentication, the client workstation may read the template off the card and match it with the input biometric to provide access. Note that feature extraction usually takes place only at the client side (on the local workstation or the portable device) to avoid costs involved in transmitting the raw biometric sample over a communication network.

The most important factor that decides the biometric system architecture is the mode of operation of the biometric system. While it is possible to decentralize the database (e.g., storing the biometric templates on personalized smart cards) in the verification mode, the identification mode necessarily requires centralized databases. Other characteristics of the application such as cooperative versus noncooperative users, overt versus covert recognition, attended versus unattended application, onsite versus remote authentication, etc. also influence the architecture of a biometric system.

In the special case of multibiometric systems [8] that involve integration of evidence from different biometric sources, the term *architecture* may also include the design of the fusion methodology. The fusion architecture in a multibiometric system is determined by the following three factors: (1) sources of information that need to be combined (i.e., different modalities like

face, fingerprint, and iris; different instances of the same trait like left and right index fingers, etc.), (2) the acquisition and processing sequence (i.e., cascade, parallel or hybrid), and (3) the type of information to be fused (i.e., features, match scores, decision, etc.).

Hardware/Software Implementation

Once the architecture of the biometric system has been defined, the system designer/integrator needs to select the appropriate hardware and software components to implement the chosen system. If the system designer also manufactures all the required components like the biometric sensor, feature extraction, and matching modules, it is relatively easy to put all these pieces together to build the complete biometric system. However, in the biometrics field, the vendors who design the biometric system or develop the application around it typically partner with another set of vendors who build the biometric hardware and software modules and create OEM (original equipment manufacturer) solutions. Therefore, the following issues need to be considered by the system designers [9]:

- *Sample Acquisition:* The biometric sensor or the sample acquisition hardware plays a very important role in determining the performance and usability of a biometric system. Apart from its ability to acquire or record the biometric sample of the user precisely, other factors such as the size, cost, robustness to different environmental conditions, etc. must also be considered when selecting the biometric sensor. Another problem that needs to be addressed during sample acquisition is how to deal with poor-quality biometric samples.
- *User Interface:* The design of a good user interface is also critical for the successful implementation of a biometric system. An intuitive, ergonomic, and easy-to-use interface may facilitate rapid user habituation and enable the acquisition of good-quality biometric samples from the user. Demographic characteristics of the target population like age and gender and other cultural issues (e.g., some users may be averse to touching a sensor surface) must

also be considered when designing the user interface.

- *Biometric Processing Components:* This includes the hardware and/or software required for performing the core biometric processing tasks of feature extraction and matching. Usually, the vendors supply software development kits (SDKs) to perform these tasks. The system designer must examine whether these components are proven and tested by reliable third-party evaluations. Other factors to be considered include the cost/performance trade-off and the availability of documentation and product support.
- *Communication Channels:* The establishment of secure communication links between the different modules of the biometric system is one of the key steps in ensuring the security of the entire system. Tamper resistance, cryptographic algorithms, and challenge-response mechanisms must be incorporated to secure the communication channels so as to avoid vulnerabilities such as denial-of-service, attacks, replay attacks, man-in-the-middle attacks, etc.
- *Database Design:* The system designer is typically entrusted with the task of storing and retrieving the biometric templates and other user information in/from a database. Therefore, the organization of the records in the database must be addressed carefully to avoid unnecessary delays that may decrease the throughput. The database design is especially important in the case of large-scale identification systems.
- *Interoperability:* When a biometric system is designed using components obtained from multiple vendors, it is very important to ensure their interoperability. If possible, it is always better to use products that are compliant with the existing or emerging standards so that they can be replaced seamlessly in future. In the case of software components, the system designer must also check compliance with different operating systems and platforms.

Administration Policy

Setting the administration policy of a biometric system is one of the critical steps in ensuring

the successful deployment of a biometric system. The administration policy may cover a variety of issues including.

- *Integrity of Enrollment*: The success of any biometric recognition system is mainly decided by the integrity of the enrollment process. If an adversary can enroll into the system surreptitiously (under a false identity) by producing his or her biometric traits along with false credentials (e.g., fake passports, birth certificates, etc.), the effectiveness of the biometric system gets completely nullified. Hence, the administrator needs to set appropriate policies that will guarantee the integrity of enrollment.
- *Quality of Enrollment Samples*: Enrollment is generally performed under human supervision to ensure that good-quality biometric samples are obtained from the users. Furthermore, the administrator needs to define policies such as the number of enrollment samples required, the minimum sample quality required for enrollment, ways to select the best-quality samples, user training, and exception procedures for persons who are unable to provide good-quality samples.
- *System Configuration*: This includes setting system parameters such as the matching threshold (which determines the FMR and FNMR of the system), the number of unsuccessful trials allowed before an account is locked, the alarms to be generated, template update policies, etc.
- *Exception Handling*: Biometric systems are usually riddled with exception handling procedures (or fall-back systems) to avoid inconvenience to genuine users. For example, when a user has an injury in his finger, he may still be granted access based on alternative authentication mechanisms without undergoing fingerprint recognition. Such exception processing procedures can be easily abused to circumvent a biometric system. It is very important to define appropriate policies for handling such exceptions so that an adversary cannot exploit this potential loophole easily.
- *Privacy Measures*: Given the sensitivity of the biometric information, it is essential to set

policies that will prevent insiders and external adversaries from modifying or tampering the template database or using the biometric data for unintended tasks. Measures such as strict audit of access logs must be implemented to protect the user's privacy.

Summary

Designers of biometric systems need to define the system architecture, address the implementation issues, and set the administration policies in such a way that the design specifications like accuracy, throughput, cost, security, privacy, and usability are met. However, this is generally a complicated task because some of the design requirements may be contradictory. Depending on the nature of the application, a number of trade-offs such as cost versus accuracy, accuracy versus throughput, usability versus cost, or accuracy versus security may be involved in the design of a biometric system. Optimizing these requirements so as to obtain the maximum return on investment is a challenging problem that requires a systematic design approach.

Related Entries

- ▶ [Privacy Issues](#)
- ▶ [Security and Liveness, Overview](#)

References

1. A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition. *IEEE Trans. Circ. Syst. Video Technol. Spec. Issue Image Video-Based Biom.* **14**(1), 4–20 (2004)
2. A.J. Mansfield, J.L. Wayman, Best practices in testing and reporting performance of biometric devices, version 2.01. Technical report NPL Report CMSC 14/02, National Physical Laboratory (2002)
3. R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior, *Guide to Biometrics* (Springer, New York, 2003)
4. ISO/IEC 19795-1:2006: Biometric Performance Testing and Reporting – Part 1: Principles and Framework (2006). Available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41447

5. S. Prabhakar, S. Pankanti, A.K. Jain, Biometric recognition: security and privacy concerns. *IEEE Secur. Priv. Mag.* 1(2), 33–42 (2003)
6. NISTC Subcommittee on Biometrics: Privacy and Biometrics: Building a Conceptual Foundation (2006). Available at <http://www.biometrics.gov/Documents/privacy.pdf>
7. M. Theofanos, B. Stanton, C.A. Wolfson, Usability & Biometrics: Ensuring Successful Biometric Systems (2008). Available at http://zing.ncsl.nist.gov/biousa/docs/Usability_and_Biometrics_final2.pdf
8. A. Ross, K. Nandakumar, A.K. Jain, *Handbook of Multibiometrics* (Springer, New York, 2006)
9. D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd edn. (Springer, London, 2009)

Biometric System-on-Card

Chen Tai Pang¹, Wei-Yun Yau²,
Robert Mueller³, and Lin Yih⁴

¹Institute for Infocomm Research, A*STAR,
Singapore, Singapore

²Institute for Infocomm Research, Singapore

³Next Biometrics AS, Next Biometrics, Nesoya,
Norway

⁴Digital Applied Research and Technology Pte
Ltd, Singapore, Singapore

Synonyms

BSoC; Full biometric authentication-on-card

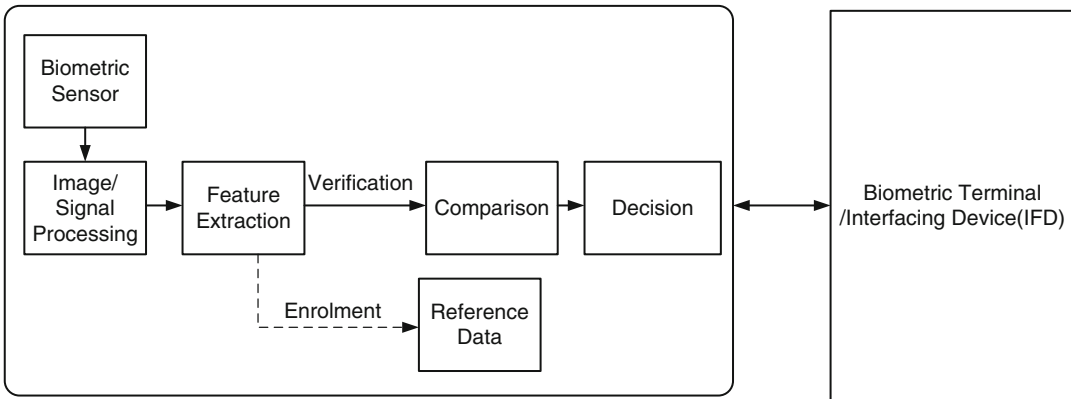
Definition

Biometric system-on-card (BSoC) is a type of on-card biometric comparison in which the entire biometric authentication, including acquisition of a biometric sample, is performed in the smart card or known as integrated circuit card (ICC). To perform BSoC comparison, a biometric sensor, which is built into the smart card, captures the biometric sample and extracts biometric data. The captured and processed biometric data is then used for enrolment or verification. The biometric verification process is executed in the smart card. Once the card completes the verification,

based on the result of biometric comparison, the BSoC module updates the security status inside the smart card for other on-card applications to enable subsequent transactions. The BSoC shall never transfer any biometric sample and biometric reference data to any external terminal.

Introduction

Traditional biometric authentication systems require using a terminal (PC or embedded system) with a biometric sensor to capture a biometric sample to perform biometric identification or verification for security access or approval for transaction. The overall system can be quite bulky. Moreover, during biometric verification, the system needs to acquire the biometric reference data (also known as enrolled biometric template) of the respective user from local database or from central database via network infrastructure that requires protection to avoid security breach. The overall infrastructure and maintenance cost will be expensive, if a large number of biometric terminals are required to be implemented for a specific application such as immigration and checkpoints. To avoid maintaining such database locally or remotely, alternative biometric authentication methods such as template-on-card and on-card biometric comparison, also referred to as on-card matching/match-on-card, have been proposed. On-card biometric comparison which is a token-based biometric authentication is capable to solve quite a number of security issues. Both template-on-card and match-on-card are able to eliminate the need for maintaining the database at the local terminal side and allow users to use biometrics with smart card to perform authentication instead of using PIN. Due to the strong security capabilities of a smart card, especially using on-card matching, it is not easy to hack into a smart card to steal the user's information including biometric reference data. However, the terminal still needs to have the biometric acquisition device to be installed to capture the biometric sample. With the advancement of semiconductor technology, biometric sensor and smart card become more energy efficient,



Biometric System-on-Card, Fig. 1 Biometric system-on-card

more capable to execute complicated biometric authentication algorithms and lower cost. Hence, on-card matching technology is evolving to have a built-in biometric sensor and a more powerful processor. This type of on-card biometric comparison is termed as biometric system-on-card (BSoC).

Figure 1 shows the general architecture of a BSoC module. The BSoC module shall consist of on-card biometric sensor, processor, memory, and interface device for communication. The on-card biometric sensor captures biometric image/signal (e.g., a fingerprint image). The captured image/signal will be processed for extraction of biometric data. During enrolment, the biometric data shall be stored in the secured memory (shown as dotted line arrow in the Fig. 1) inside the smart card as biometric reference data. The biometric reference data shall never be released to any external device to avoid security breach. During verification, the biometric data will be used as query template which will then be compared with the biometric reference data to generate a comparison score. This comparison score will be compared with the internal predefined security threshold to decide whether the query is from the genuine user or an imposter. The BSoC module will base on the decision to update its security status for processing the subsequent transaction requested by the user.

As shown in Fig. 1, all the components, including the capturing device, are implemented

inside the smart card. If the card is well designed with strong protection, the card shall not be easily hacked. The biometric terminal is also known as interfacing device (IFD) for some applications using smart card.

Advantages of BSoC

Applications using BSoC allow service providers to keep personal biometric information in the hand of the respective owner, instead of using a centralized database with expensive infrastructure that requires regular maintenance and strong protection. The BSoC module contains all the necessary components of a biometric terminal to allow user performing on-card biometric authentication. The BSoC module as a smart card is a plastic card with an embedded microprocessor, memory, and security features. The user can conveniently carry the card, therefore bringing mobility to biometric reference data. The combination of biometrics and smart card is able to provide the advantages of mobility, security, and strong identity authentication capability and allowing user to have a high degree of control over who has access to that biometric data. It eliminates the need of storing biometric data/samples in a central database that might raise privacy concerns. Even during verification, the query template is only generated and used on-card, without leaking of any sensitive data to an external ter-

minal. The following are distinct advantages of BSoC:

1. **Stronger Security:** The decision of biometric comparison is computed inside the BSoC and can be accessed by authorized on-card applications protected by firewall. The installation of on-card applications is usually done during card personalization in a secure production environment. After installation of all on-card applications, the card can be locked permanently to prevent additional applications to be installed. Each application has restriction to access resources from other applications limited by access policies defined in the smart card OS. Among the trusted applications, information such as the card security status can be shared via the firewall controlled by the OS. Therefore, it is not easy for a hacker to perform a software attack to a tamper-proof smart card that would be easy with many other systems.
2. **Better Privacy:** No matter during enrolment or verification, the biometric sample is captured within the card and the generated biometric data will only be used inside the card without leaking to any external terminal. Hence, privacy can be guaranteed.
3. **Hygiene:** Some biometric capture devices require the user to touch the sensor to acquire biometric sample data, e.g., a capacitive silicon fingerprint sensor. The BSoC is a hygienic way to perform biometric authentication as each person has his or her own device such as fingerprint system-on-card, rather than touching on the same sensor such as the biometrics-enabled auto-gate currently used at the immigration and checkpoint.
4. **Strong Two-Factor Authentication Token:** The BSoC technology will set up a true two-factor authentication process for the identity management needs. Prior to exchanging information between the terminal and the smart card, a secure channel shall be established with mutual authentication before any transaction takes place. This stage is to allow the terminal and the smart card to verify the cryptogram from each side to ensure both are valid and genuine. This stage relies on the strength

of the cryptogram being used for protection. Hackers may use Trojans or similar methods to steal challenge code and attempt to eavesdrop the channel and steal useful information from the smart card. With a BSoC, biometrics can be used to unlock the card before any communication including mutual authentication takes place.

Implementation of BSoC and Performance

BSoC is a relatively new technology. Only few commercial products can be found in the market using BSoC form factor. Fingerprint sensor is currently the only biometric sensor which can be manufactured thin enough to fit inside a smart card body.

Academic community is mainly focusing on on-card fingerprint biometric comparison and studying the algorithm to perform biometric authentication. For BSoC, as all the components are required to be integrated on the smart card, the cost and complexity for prototyping are high. Most researches related to on-card biometric comparison are using off-the-shelf smart card for prototyping together with a sensor attached to the PC to capture biometric sample. Past attempts can be found for implementing on-card fingerprint comparison that may be applied to BSoC implementation. Mohamed [1] proposed a memory-efficient method which requires using a 32-bit DSP to use line extraction of fingerprint that could speed up the matching process. Krivec et al. [2] suggested a new hybrid fingerprint matcher, which combines minutiae matcher and homogeneity structure matcher, to perform on-card matching. Surya Rikin et al. [3] proposed using minutia with a ridge shape for fingerprint matching. Bistarelli et al. [4] introduced a matching method using local relative information between nearest minutiae. Sanchez-Avila et al. published two reference implementations [5, 6] of fingerprint match-on-card for specific application. These two reference implementations addressed the

basic components and requirements for the on-card matching. Chen et al. [7] presented a novel method to perform on-card biometric comparison using work-sharing architecture. Although these past attempts are mainly for on-card fingerprint matching, these methods can be considered for designing better algorithms for BSoC implementation.

For commercial implementation, only few companies such as e-Smart, Gemalto, and SmartMetric can be found which are able to provide fingerprint system-on-card or similar products. As of 2013, few fingerprint sensor manufacturers claimed that they are able to fabricate fingerprint sensor using small form factor and this is available in flexible membrane type, but not in mass production stage. With the advancement of technologies including microprocessor (in terms of power consumption and processing power), near-field communication (NFC), flexible battery, and smart card processor, the feasibility of productizing BSoC using fingerprint becomes higher.

Some commercial companies disclosed the accuracy and matching speed in their websites without disclosing the database and test methods for generating such result. Hence, it is difficult to justify the actual accuracy in real life. National Institute for Standards and Technology (NIST) completed the MINEX [8] for fingerprint template-on-card, MINEX II Phase II [9] and MINEX II Phase IV [10] for fingerprint on-card matching to test for interoperability. No similar test was organized for BSoC.

Standardization

For better global interoperability using BSoC, several efforts to standardize the BSoC are ongoing. In 2011, after publishing the ISO/IEC 24787:2010 "On-card biometric comparison standard" [11], the international standards body ISO/IEC Joint Technical Committee 1 (JTC1) Subcommittee (SC)17 Working Group (WG) 11 started a new project to develop a new

standard for BSoC. SC17 WG11 identified that those existing standards for smart card are not sufficient for BSoC especially for the form factor because BSoC requires additional components such as biometric sensor. Hence, WG11 is developing a new three-part standard for BSoC:

1. **ISO/IEC 17839-1 Information Technology Biometric System-on-Card Part 1: Functional Architecture:** This part of standard defines the functional architecture of BSoC, two types of BSoC (in terms of form factor), minimum requirements of BSoC implementation with respect to discriminative power, interfaces and power supply. For the form factor of BSoC, type S1 and type S2 are defined in this part. Type S1 is for the BSoC which is fully ISO/IEC 7810 compliant and Type S2 contains relaxing requirements based on the existing specifications from respective standards for smart card required by BSoC implementation. As of December 2013, this part of standard is at Final Draft for International Standard (FDIS) stage and is expected to be published as international standard in 2014.
2. **ISO/IEC 17839-2 Information Technology Biometric System-on-Card Part 2: Physical characteristics:** This part of standard defines physical characteristics includes: dimension of type S1 and type S2 of BSoC as specified in part 1, position and size of biometric capturing device, as well as minimum requirements for BSoC including mechanical durability and man-machine-interface and ergonomics. Specifications for implementing electronic display and keypad are out of the scope of this international standard. However, WG11 is aware of ongoing standardization efforts in other working groups in SC17 for electronic display and keypad that may affect the physical position of biometric capturing device to be implemented on the smart card. Therefore, WG11 is working with respective working groups in SC17 to harmonize the specification. As of December 2013, this part of standard is at the third Committee Draft (CD3) stage and expected to be published as international standard in 2015.

3. ISO/IEC 17839-3 Information Technology Biometric System-on-Card Part 3: Logical information interchange mechanism:

This part of standard defines logical data structures, enrolment procedures, usage of commands and data structures defined in corresponding ISO standards for BSoC to execute on-card biometric comparison, and security policies on managing threshold parameters and other security related interoperability issues. The current status of this part of standard is at the sixth Working Draft (WD6) stage. This part of standard is expected to be published in 2016.

Specifications mentioned in ISO/IEC 24787 and ISO/IEC 7816-11 [12] are still required to be used in BSoC. For example, for fingerprint BSoC implementation, the ISO/IEC 19794-1 [13] and ISO/IEC 19794-2 [14] are required as per ISO/IEC 24787 to store the fingerprint minutiae data inside the BSoC for fingerprint verification.

Summary

BSoC technology provides strong security with good privacy protection. This technology is still relatively new compared to on-card biometric comparison (match-on-card) but becoming feasible and aiming at reasonable cost with the advancement of sensor technology especially for fingerprint authentication. This technology can provide a good platform with strong identity authentication which allows many other new applications with advantages of more convenience, protection, and security for users to create more business opportunities.

Related Entries

- ▶ [Biometric System-on-Card](#)
- ▶ [On-Card Matching](#)

References

1. M.M.A. Allah, A fast and memory efficient approach for fingerprint authentication system, in *IEEE*

- Conference on Advanced Video and Signal Based Surveillance*, Como, Italy 2005, pp. 259–263
2. V. Krivec, J. Birchhauer, W. Marius, H. Bischof, A hybrid fingerprint matcher in memory constrained environments, in *Proceedings of the 3rd International Symposium on Image and Signal Processing and Analysis*, Rome, Italy 2003, pp. 617–620
3. A.S. Rikin, D. Li, T. Isshiki, H. Kunieda, A fingerprint matching using minutia ridge shape for low cost match-on-card systems. *IEICE Trans.* **E88-A**(5), 1305–1312 (2005)
4. S. Bistarelli, F. Santini, A. Vaccarelli, An asymmetric fingerprint matching algorithm for Java cardTM. *Pattern Anal. Appl. J.* **9**(4), 359–376 (2006)
5. R. Sanchez-Reillo, L. Mengibar-Pozo, C. Sanchez-Avila, Microprocessor smart cards with fingerprint user authentication. *IEEE Aerosp. Electron. Syst. Mag.* **18**(3), 22–24 (2003)
6. R. Sanchez-Reillo, C. Sanchez-Avila, Fingerprint verification using smart cards for access control systems. *IEEE Aerosp. Electron. Syst. Mag.* **17**(9), 12–17 (2002)
7. T.P. Chen, W.-Y. Yau, X. Jiang, ISO/IEC standards for on-card biometric comparison. *Int. J. Biometrics* **5**(1), 30–52 (2013)
8. P.J. Gother, R.M. McCabe, C.I. Watson, M. Indovina, W.J. Salamon, P. Flanagan, E. Tabassi, E.M. Newton, C.L. Wilson (ed.), Performance and interoperability of the INCITS 378 fingerprint template. National Institute of Standards and Technology, 2006
9. P. Grother, W. Salamon, C. Watson, M. Indovina, P. Flanagan (ed.), Performance of fingerprint match-on-card algorithms phase II report. National Institute of Standards and Technology, 2008
10. P. Grother, W. Salamon, C. Watson, M. Indovina, P. Flanagan (ed.), Performance of fingerprint match-on-card algorithms phase IV report. National Institute of Standards and Technology, 2011
11. Standards: Information technology – identification cards – on-card biometric comparison, ISO/IEC 24787:2010. International Organization for Standardization/International Electrotechnical Commission, 2010
12. Standards: Identification cards – integrated circuit cards with contacts – part 11: personal verification through biometric methods, ISO/IEC 7816-11:2004. International Organization for Standardization/International Electrotechnical Commission, 2004
13. Standards: Information technology – Biometric data interchange formats – part 1: framework, ISO/IEC 19794-1:2006. International Organization for Standardization/International Electrotechnical Commission, 2006
14. Standards: Information technology – biometric data interchange formats – part 2: finger minutiae data, ISO/IEC 19794-2:2006. International Organization for Standardization/International Electrotechnical Commission, 2006

Biometric System-on-Card, Standardization

Raul Sanchez-Reillo¹ and Robert Mueller²

¹GUTI (University Group for Identification Technologies), University Carlos III of Madrid, Leganes, Madrid, Spain

²Next Biometrics AS, NEXT Biometrics, Nesoya, Norway

Synonyms

BSoC; Sensor-on-card

Definition

Smartcard that contains capabilities for performing the on-card comparison of a biometric record and also embeds the biometric capture device in the card body. In a biometric system-on-card (BSoC), the sample to be compared with the stored biometric reference is obtained directly from the embedded sensor, and all biometric processing steps are performed in the smartcard.

Introduction

The International Standard ISO/IEC 24787:2010 [1] developed by WG 11, *Application of biometrics to cards and personal identification* of ISO/IEC SC 17, *Cards and personal identification* [2], defines several architectures to integrate biometrics with smartcards, including the storage-on-card alternative (i.e., the biometric reference is stored securely in the smartcard memory and read by the external world when the verification is needed) and the on-card biometric comparison (i.e., the biometric feature vector is sent to the smartcard for performing an internal comparison with the stored biometric reference). The biometric system-on-card (BSoC) is a functional extension to the on-card biometric comparison where the whole biometric process is executed inside the card, including the capture of

the biometric sample. This architecture is being standardized by ISO/IEC JTC1/SC17 WG11 in the ISO/IEC 17839 multipart international standard [3–5].

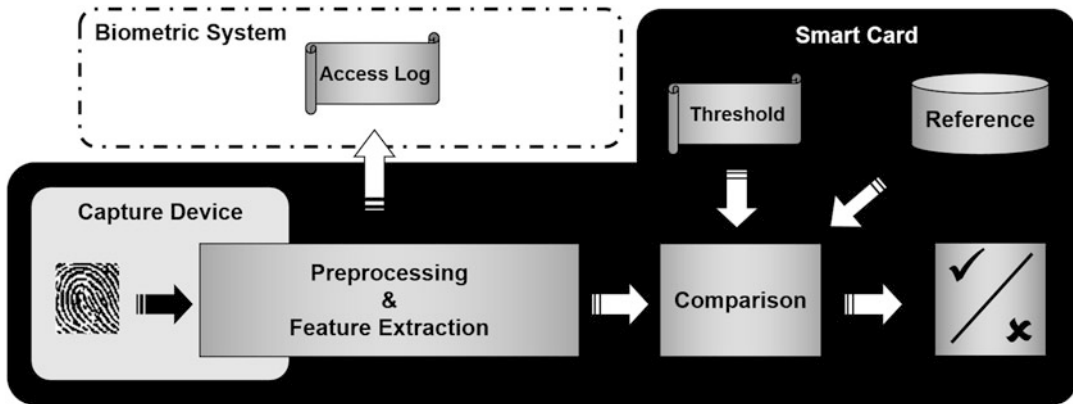
As it can be seen in Fig. 1, a BSoC includes the sensor (biometric capture device) in the smart-card, together with the signal processing and feature extraction algorithms, plus the same services as offered by an on-card biometric comparison smartcard. While the decision takes place in the BSoC, it can provide information to the outer world to allow recording the process in the application. This information shall be minimal, as to not allow hill-climbing attacks. It is important to note that the main difference of a BSoC with other kind of biometric dongles is that a BSoC is actually a smartcard. Therefore, it provides all the security mechanisms traditionally available in a smartcard, including a tamperproof security controller and operating system.

BSoC Architecture

The development of BSoCs is on the very edge of current technology. The integration of a biometric sensor in an ISO/IEC 7810 [6] compliant smart-card is challenging. The card thickness and the bending and stiffness requirements are currently not addressable in a mass production context. The rest of the specifications can be satisfied, and therefore ISO/IEC 17839-1 [3] defines two possible system architectures for a BSoC. These two architectures are defined as:

- Type S1: this architecture is a fully flexible card compliant with ISO/IEC 7810.
- Type S2: architecture that intentionally deviates from the requirements of Type S1, by defining a thicker card body and easing the requirements to torsion, bending, and stiffness.

Type S1 may communicate with the external world by any of the smartcard communication interfaces, either with contacts (e.g., ISO/IEC 7816-3 [7] or the USB connection defined in ISO/IEC 7816-12 [8]) or contactless (e.g., ISO/IEC 14443 [9] or ISO/IEC 15693 [10]). In the case of Type S2, in order to avoid the creation of new readers that accept thicker cards, the



Biometric System-on-Card, Standardization, Fig. 1 Block diagram of a BSoC

communication interface is limited to contactless, either by using proximity cards (i.e., ISO/IEC 14443 [9]) or vicinity cards (i.e., ISO/IEC 15693 [10]). Type S2 is also motivated by the fact that the BSoC anyhow has to be contactless with most card readers to allow physically touching the embedded sensor. The thickness of Type S2 is defined to ease integration of components and to avoid damaging currently deployed card readers.

Although the first products will likely rely on fingerprint recognition, the BSoC standard is not limited by the biometric modality, allowing other capture devices to be embedded in the card as soon as technology allows it. Due to ergonomics, it seems logical that for some modalities (e.g., face recognition), only contactless interfaces would be available, as capturing the face of the cardholder with the smartcard already inserted in the reader may not be physically possible.

For the correct operation of the BSoC, the cardholder may require some feedback to signal when the data capture is in progress and when the acquisition is already complete. For some kind of sensors, such as fingerprint sweep sensors, further feedback for helping the cardholder during the process of data capture may be needed. Such feedback shall be provided without compromising the security and integrity of the BSoC and its data, i.e., avoiding hill-climbing attacks.

In order to improve performance, a BSoC may be designed in a way that the enrolment is performed using sensors and algorithms outside

of the smartcard, in order to obtain biometric reference data of superior quality.

Last but not least, power to the BSoC can be supplied either from the contact interface, from the contactless field, or using internal power supply devices such as a battery or a capacitor.

Physical Specifications for BSoC

Part 2 of ISO/IEC 17839 [4] defines the physical characteristics of the card including the dimensions of the card body, the location of the sensor, ergonomic requirements depending on the biometric modality, and the coexistence with other ID technologies included in the smartcard, plus other storage and operating conditions, such as temperature.

As previously mentioned, the Type S1 card shall be in accordance to the ID-1 specification in ISO/IEC 7810. In the case of Type S2, the physical characteristics are defined in the ID-T card format also defined in a forthcoming revision of ISO/IEC 7810. No other physical dimensions are in the scope of ISO/IEC 17839.

In any of these cases, but particularly in Type S1 when using a contact interface, the location of the sensor shall be carefully decided as not to limit the use of the card. Therefore, if the contact interface is used, the sensor shall be located in the right edge of the card, as to allow, for example, the placement of the finger with half of the card inserted in the reader.

In addition, the sensor shall be separated from the edges of the card, as to limit potential damage. A minimum margin from each of the edges is defined.

Biometric capture devices can coexist with other identification technologies already defined for smartcards, such as magnetic stripes, photographs, bar codes, or even embossing. The only limitation is that the introduction of such identification data shall not limit the functionality of the sensor, either mechanically (e.g., with traditional embossing technologies) or by ergonomics.

Commands and Security Mechanisms

In order to reach interoperability between BSoC and external applications, not only physical characteristics shall be defined but also the way information is exchanged and managed. This includes instruction codes for the card, logical data structures, and security mechanisms. Part 3 of ISO/IEC 17839 [5] provides solutions to all these needs, in accordance with the rest of the smartcard standards such as ISO/IEC 24787 [1], ISO/IEC 7816-11 [11], ISO/IEC 7816-4 [12], and the recent development works on the future International Standard ISO/IEC 18328.

This third part of ISO/IEC 17839 provides the mechanisms for the external world to recognize that a connected card (either inserted or in the field) is a BSoC card, plus additional information such as the biometric modality and the functionality and security mechanisms offered to the external world. One of the important aspects when using a BSoC is the security link between the application and the integrity and validity of the biometric data capture and comparison process. Therefore, integrity and authentication mechanisms are defined.

As has been previously mentioned, the BSoC can be designed forcing the enrolment to be done with the embedded sensor, or it can allow the biometric reference to be sent from the external world. In the latter case, coding of the imported biometric reference data is also defined in this standard.

Configuration data is also defined in the standard and may contain sensitive operational information, such as comparison thresholds. The configuration data and access regulations are typically provided to the card during personalization. Only part of the data is publically available after issuance of the card. A card may have several biometric references, corresponding to different biometric traits of the cardholder. For example, enrolling two different fingerprints allows usage of the BSoC even in the case of temporary disability, i.e., damage of the finger.

Finally, the commands for performing the biometric system-on-card verification are defined, together with the feedback mechanisms for the human-machine interaction. Feedback data is limited to simple mechanical movement or placement and not providing information about, for example, the quality of the sample being acquired, as to avoid hill-climbing attacks.

Summary

A biometric system-on-card (BSoC) is a smartcard containing a complete set of biometric modules, from the data acquisition to the decision making. This technology is being standardized in the ISO/IEC 17839 series of standards in a modality independent way to allow in the future multiple biometric modalities available in the market.

Related Entries

- ▶ [Biometric System-on-Card](#)
- ▶ [Tamper-Proof Operating System](#)

References

1. ISO/IEC JTC1/SC17: ISO/IEC 24787:2010, Information technology – Identification cards – On-card biometric comparison (2010), available at <http://www.iso.org/iso/home/store>
2. ISO website, ISO/IEC JTC 1/SC 17 Cards and personal identification. http://www.iso.org/iso/home/standards_development/list_of_iso_technical_

[committees/iso_technical_committee.htm?commid=45144](http://www.iso.org/iso/technical_committee.htm?commid=45144)

3. ISO/IEC JTC1/SC17: ISO/IEC DIS 17839-1, Information technology – Identification cards – Biometric system on card – Part 1: functional architecture. (Under development, more information in http://www.iso.org/iso/home/search.htm?qt=17839&published=on&active_tab=standards&sort_by=rel)
4. ISO/IEC JTC1/SC17: ISO/IEC CD 17839-2, Information technology – Identification cards – Biometric system on card – Part 2: physical characteristics. (Under development, more information in http://www.iso.org/iso/home/search.htm?qt=17839&published=on&active_tab=standards&sort_by=rel)
5. ISO/IEC JTC1/SC17: ISO/IEC WD 17839-3, Information technology – Identification cards – Biometric system on card – Part 3: logical information interchange mechanism. (Under development, more information in http://www.iso.org/iso/home/search.htm?qt=17839&published=on&active_tab=standards&sort_by=rel)
6. ISO/IEC JTC1/SC17: ISO/IEC 7810:2003, Identification cards – Physical characteristics (2003), available at <http://www.iso.org/iso/home/store>. There is a revision in process (more information in http://www.iso.org/iso/home/search.htm?qt=7810&published=on&active_tab=standards&sort_by=rel)
7. ISO/IEC JTC1/SC17: ISO/IEC 7816-3:2006, Identification cards – Integrated circuit cards – Part 3: cards with contacts – Electrical interface and transmission protocols (2006), available at <http://www.iso.org/iso/home/store>
8. ISO/IEC JTC1/SC17: ISO/IEC 7816-12:2005, Identification cards – Integrated circuit cards – Part 12: cards with contacts – USB electrical interface and operating procedures (2005), available at <http://www.iso.org/iso/home/store>
9. ISO/IEC JTC1/SC17: ISO/IEC 14443, Identification cards – Contactless integrated circuit cards – Proximity cards (2008–2013), available at <http://www.iso.org/iso/home/store>
10. ISO/IEC JTC1/SC17: ISO/IEC 15693, Identification cards – Contactless integrated circuit cards – Vicinity cards (2006–2013), available at <http://www.iso.org/iso/home/store>
11. ISO/IEC JTC1/SC17: ISO/IEC 7816-11:2004, Identification cards – Integrated circuit cards – Part 11: personal verification through biometric methods (2004 – currently under revision, more information in http://www.iso.org/iso/home/search.htm?qt=7816-11&published=on&active_tab=standards&sort_by=rel)
12. ISO/IEC JTC1/SC17: ISO/IEC 7816-4:2013, Identification cards – Integrated circuit cards – Part 4: organization, security and commands for interchange (2013), available at <http://www.iso.org/iso/home/store>

Biometric Systems, Agent-Based

Farzin Deravi

University of Kent, Canterbury, Kent, UK

Definition

Agent-based biometric systems use the computational notion of intelligent autonomous agents that assist the users and act on their behalf to develop systems that intelligently facilitate biometrics-enabled transactions, giving them the ability to learn from the users and adapt to application needs, thus enhancing recognition performance and usability.

Introduction

The ultimate effectiveness and success of biometric systems to a large part is dependent on the user experience when interacting with such systems. It is therefore essential that issues of user interaction and experience are considered when designing biometric systems. As user behavior and expectations as well as application requirements and operating conditions can vary widely, it becomes important to consider how systems can be developed that can adapt and learn to provide the best possible performance in a dynamic setting.

Here the paradigm of intelligent software agents may be effectively utilized to design and implement biometric systems that can dynamically respond to user and application needs. Intelligent autonomous agents and multiagent systems form a rapidly expanding research field [1]. Agents can be defined as software subsystems that interact with some environment and are capable of autonomous action while representing the interests of some user or users. Such agents may know about their users' wishes and goals using a presupplied knowledge base as well as through a learning system. They can then use this knowledge to seek the accomplishment

of their users' goals. While seeking such goals in a flexible response to their environment, agents may be designed to be proactive in exploiting any opportunities that may be available. They may also cooperate and compete with other agents and may have other valuable properties such as mobility and adaptability.

A group of interacting agents may be implemented to form a multiagent system (MAS) [2]. These are systems composed of multiple interacting agents that can be used to tackle applications, which are not possible to handle effectively with just a single agent and are well suited to situations where multiple perspectives of a problem-solving situation may be exploited. Interactions in a MAS may include cooperation, coordination, and negotiation between agents.

Negotiating agents are of particular importance in electronic commerce, and the proliferation of Internet-based applications is a driving force for research and development of such multiagent systems [3]. Such multiagent systems when applied to user authentication applications can facilitate a bargain between the needs of the information provider for establishing sufficient trust in the user on the one hand and the confidentiality of the user's personal information and the ease of use of the system on the other hand. Such a balance may need to be achieved for each different service, transaction, or session and may even be dynamically modified during use. Multiagent systems can provide an effective framework for the design and implementation of such systems.

Other areas of active research and development in the field of intelligent agents include software development environments and specialist programming and agent communication languages as well as the design of the overall architecture where layered or hybrid architectures, involving reactive, deliberative, and practical reasoning architectures, continue to be of considerable interest [4].

Challenge of Complexity

The application of biometric systems in most realistic scenarios is bound to face the challenge of complexity resulting from a range of interrelated

sources of variability that are likely to affect the performance and overall effectiveness of such systems.

These sources include, for example, users' physiological/behavioral characteristics, users' preferences, environmental conditions, variability of the communication channels in remote applications, and so on. If one considers the users' biometric characteristics alone, it is clear that with a widening user base it is important to consider the impact of "outliers" – those users who find it difficult or impossible to use the system. Failure to enroll on biometric systems or to consistently provide useable images for biometric matching may be due to a range of factors including physical or mental disability, age, and lack of familiarity or training in the use of the particular biometric systems deployed. In many applications, it is essential to ensure that no part of the user population is excluded from access, and therefore, measures must be introduced to handle such outliers in a way that does not reduce the security or usability of the system.

One approach to address this issue as well as to tackle the other grand challenges of biometrics such as performance, security, and privacy [5] is to adopt a multibiometric approach [6]. In multibiometric systems, information from several sources of identity are combined to produce a more reliable decision regarding identity. This may include fusing information from a number of modalities such as face, voice, and fingerprint, using a different sensor and biometric matching module for each modality. Here information may be fused at various stages of processing, including fusion of biometric features extracted from each modality (feature fusion) or fusion of matching scores after matching of each the biometric samples against the respective templates for each modality (score fusion). There is a wide, extensive, and varied literature on such multimodal identification systems [6]. While in most of the reported works, attention is generally focused on a multimodal recognition procedure based on a fixed set of biometrics, it is clearly possible to adopt a more flexible approach in choosing which modalities to integrate depending on individual user needs and constraints – thus

removing, or at least reducing, the barrier to use by “outlier” individuals and facilitating universal access through biometrics.

Research has shown the potential advantages of a more flexible structure for multibiometric systems allowing an element of reevaluation and adaptation in the information fusion process [7]. Mismatched recognition and training conditions can lead to a reduced recognition accuracy when compared to matched conditions, suggesting that robust recognition may require a degree of adaptation. Inclusion of biometric sample quality information can further enhance the fusion process [8]. Here, an estimate is made of the quality of the live biometric sample, and this is used to adapt the operation of the fusion module, which may have been trained earlier incorporating knowledge from both biometric samples and their associated quality.

The move towards multibiometrics further accentuates system complexity and the burden on the biometric system users to efficiently utilize such systems. Instead of having to provide a sample for only one sensor, there is a set of sensors to interact with. There is more effort required from the user and more choices available in the design of the interaction with the system. Intelligent agents can thus provide a valuable way forward for designing and managing intelligent and adaptable user interfaces, while multi-agent architectures can facilitate the negotiation of trust, security, and privacy requirements of system users.

With an agent-based biometric system, selection of a variable set of biometric modalities can be accommodated to match the demands of a particular task domain or the availability of particular sensors. For example, a multimodal system should be able to deal with situations where a user may be unwilling or simply unable to provide a certain biometric sample or where a preferred biometric modality cannot support a required degree of accuracy. The deployment of a multimodal approach, where it is possible to choose from a menu of available modalities and modes of interaction, can therefore help to overcome barriers to access. In the case of users with disabilities, where the use of a particular modality (e.g., speech) may be difficult or impossible,

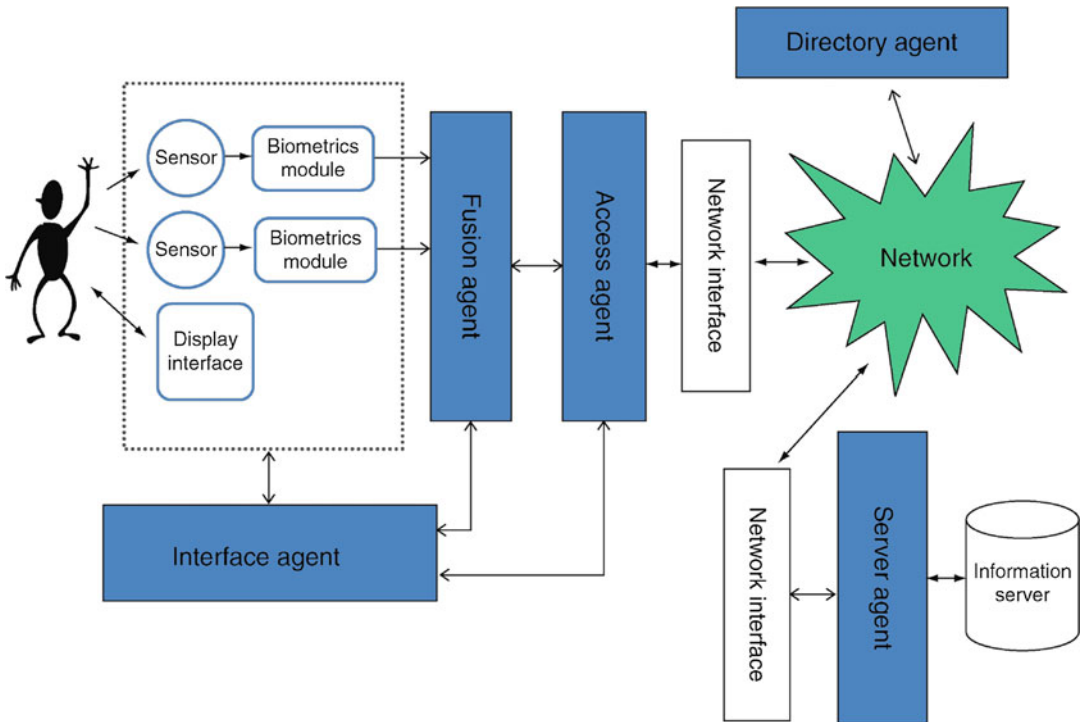
identity information is captured through alternative sensors to suit the user constraints.

When considering remote and unsupervised biometrics-enabled access, it is essential to build in protection against attacks on the system. In particular, it is essential to establish “liveness” of the biometric input to protect against spoofing and replay attacks. This is an important consideration as for many modalities biometric samples can easily be recorded, even without the subjects’ active cooperation, and it may be equally easy to present such recorded samples at the sensor or at other stages of processing to gain unauthorized access. While some progress has been made in integrating liveness detection in individual modalities, it is likely that an agent-managed multimodal framework provides a platform with additional flexibility to support more advanced robustness measures. For example, the agent interface can be deployed to provide a sophisticated challenge/response mechanism making it much more difficult to use replay attacks and much easier to establish the appropriate level of confidence in the liveness of samples.

Another important consideration when deploying biometrics in remote and networked applications is to ensure the legitimate requirements of the users at the client side to reveal only as much personal biometric information as may be necessary for establishing their access rights and no more, thus ensuring that the release of their private information is limited and controlled. At the same time, on the server side, there is the need to establish the identity of user with as high a confidence as may be required for a particular type of information access. Clearly, these goals at the client and server sides are in contention, and a negotiating multiagent architecture may be effectively utilized to engage in such negotiation on behalf of the users at the server and client sides.

Agent Architectures

The agent paradigm may be employed in a number of ways to enhance the performance of biometric systems. Its value is perhaps best illustrated in a multimodal biometric system for



Biometric Systems, Agent-Based, Fig. 1 A multiagent architecture for multimodal biometric authentication

remote authentication and information access through a communication network. Here the management of the user interface, handling the information fusion process, and the negotiation between the information user and information server across a network may all be delegated to a set of autonomous agents. An example of such a system for a healthcare application, using a multimodal biometric interface, has been the IAMBIC project [9], which is outlined below to illustrate possible applications of intelligent agent technologies in a biometric authentication setting (Fig. 1).

On the client side of such a client-server architecture, a set of agents will be cooperating to manage the user interface and to address the user's specific requirements and constraints. A user interface agent manages the direct interaction with the user, establishing, according to past user choices and behavior as well as the requirements of the current transaction, the set of biometric measurements that must be obtained

from the user as well as assessing the quality and reliability of the measurements from each of the available biometric recognition modules. This agent defines the mode of interaction with the user according to the user constraints and characteristics such as computer literacy, familiarity with the system being used, and so on.

The interface agent may also be responsible for the capture of other important non-biometric information. Additional environmental data may be captured by the available sensors (e.g., for the face modality a sample of background illumination may be captured). Analysis can be performed on these samples to determine the quality of any acquired data; this can be used to help the agent to analyze any possible systematic enrollment and/or verification failures. The results from this type of analysis can be used to provide feedback to the user or to system operators to improve future performance. The agent may offer immediate suggestions to a user who is finding it difficult to provide useable samples on how better

to interact with the system or may request from a user whose performance has been declining over a period of time to re-enroll on to the system, thus ensuring that the biometric template aging effects are minimized.

Additionally, the acquired samples may be associated with appropriate quality scores, and this information can be passed on the fusion stage. The interface agent will also manage the individual biometric modules that will produce features and/or matching scores or decisions. Depending on the level at which the fusion takes places (sample, feature, score, or decision) [10], the appropriate information is transmitted to the fusion agent to manage the fusion process.

A fusion agent can be used for the integration of the biometric measures taken from the user. Its main role is to choose the best technique for combining several different biometric measures. The design of the fusion agent requires knowledge of the types of biometrics measured as well as of their corresponding characteristics and of the levels of confidence in claimed identity that they can typically generate. This agent may have a set of different fusion algorithms to choose from. Biometric samples, features, matching scores, or decisions obtained from the interface agent as well as sample quality and environmental information obtained from the user are passed on to the fusion agent, which in turn can produce an overall confidence score, which will be passed to the access agent for transmission to the server agent.

The access agent is then responsible for negotiating the access to the required data (e.g., medical records or other sensitive data) on behalf of the user. Essentially, this agent receives access information from the interface agent, locates the data, chooses the best location (in the event that the data can be found in different places), contacts the sources of the desired information, and negotiates its release with the appropriate server agent(s). The access agent is responsible for the negotiation with the server agent and has its goal to achieve the release of the requested information. The goal of the server agent is to ensure that the information is only released to authorized

users. It must ensure that sufficient confidence is reached in the identity of the claimed user. What may be considered as sufficient confidence may depend on the sensitivity of the data requested and the class of user who is accessing the information. If the result of the activities of the interface and fusion agents does not provide enough evidence to satisfy the server agent, it may enter into negotiation with them through the access agent. As part of this negotiation, a re-measurement of the biometric samples, as well as the recalculation of the combined output, may be required under specific conditions.

Optionally a directory agent may be deployed for discovering and cataloging all relevant information about location of services within the network. In a healthcare system, for instance, this agent may store information on which databases contain particular information about the patients, medical tests, and treatments. Additionally, information may be stored with regard to databases of biometric information for matching and authentication as well as information regarding where suitable and trusted algorithms for matching, fusion, and sample quality assessment may be obtained to facilitate the agents' tasks. In the search for information, this agent may also suggest the best way of accessing required information (e.g., in the situation where several databases contain the information specified), based on network traffic, distance, and so on.

Such a community of interacting agents can be implemented using a number of different methodologies for agent-based systems. These include methodologies for modeling the agents and their interactions, schemes for representing agent knowledge, and languages for facilitating the communication between agents in unambiguous ways [4, 11, 12]. An important aspect of agent communication, especially in the contexts where biometrics may be involved, is to ensure the security and privacy of the information exchanged between agents. The incorporation of encryption and secure communication techniques is therefore an important consideration in the application of agent technologies to security applications.

Summary

To overcome some of the existing challenges that limit the performance and acceptability of biometric systems, as well as to develop future applications incorporating the vision of ambient intelligence, increasingly systems of greater complexity are being devised. Such systems are required to cope with large user communities, increased requirements for accuracy, security, and usability. The additional complexity of such systems provides a suitable ground for the exploitation of the intelligent agent paradigm. Multibiometric systems in particular provide a viable approach for overcoming the performance and acceptability barriers to the widespread adoption of biometric systems. An agent-based architecture can provide the support needed for the management of multimodal biometrics for person recognition and access authorization within an overall security framework for trusted and privacy-preserving information exchange.

Related Entries

- ▶ [Fusion, Quality-Based](#)
- ▶ [Multibiometrics](#)
- ▶ [Security and Liveness, Overview](#)
- ▶ [User Acceptance](#)

References

1. M. Wooldridge, N.R. Jennings, Intelligent agents: theory and practice. *Knowl. Eng. Rev.* **10**(2), 115–152 (1995)
2. N.R. Jennings, K. Sycara, M. Wooldridge, *A Roadmap of Agent Research and Development*. Autonomous Agents and Multi-agent Systems, vol. 1 (Kluwer, Dordrecht, 1998), pp. 275–306
3. S.S. Fatima, M. Wooldridge, N.R. Jennings, Multi-issue negotiation with deadlines. *J. Artif. Intell. Res.* **27**, 381–417 (2006)
4. G. Weiß, Agent orientation in software engineering. *Knowl. Eng. Rev.* **16**(4), 349–373 (2001)
5. A.K. Jain, S. Pankanti, S. Prabhakar, J. Hong, A. Ross, Biometrics: a grand challenge, in *Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04)*, Cambridge, vol. 2, 2004, pp. 935–942
6. A.A. Ross, K. Nandakumar, A.A. Jain, *Handbook of Multibiometrics* (Springer, New York, 2006)
7. C.C. Chibelushi, F. Deravi, J.S.D. Mason, Adaptive classifier integration for robust pattern recognition. *IEEE Trans. Syst. Man Cybern. B Cybern.* **29**(6), 902–907 (1999)
8. K. Nandakumar, Y. Chen, A.K. Jain, S.C. Dass, Quality-based score level fusion in multibiometric systems, in *Proceedings of the 18th International Conference on Pattern Recognition (ICPR'06)*, Hong Kong, vol. 4, 2006, pp. 473–476
9. F. Deravi, M.C. Fairhurst, R.M. Guest, N. Mavity, A.D.M. Canuto, Intelligent agents for the management of complexity in multimodal biometrics. *Int. J. Univers. Access Inf. Soc.* **2**(4), 293–304 (2003)
10. ISO/IEC TR 24722:2007, Information technology – Biometrics – Multimodal and other multibiometric fusion (2007)
11. F. Zambonelli, N.R. Jennings, M. Wooldridge, Developing multiagent systems: the Gaia methodology. *ACM Trans. Softw. Eng. Methodol.* **12**(3), 317–370 (2003)
12. B. Chaib-draa, F. Dignum, Trends in agent communication language. *Comput. Intell.* **18**(2), 89–101 (2002)

Biometric Technical Interface, Standardization

Catherine J. Tilton
Standards & Technology, Daon, Reston,
VA, USA

Synonyms

Biometric interchange formats; CBEFF; BioAPI; BIP; Tenprint capture

Definition

There are three main sets of international biometric technical interface standards. The first set is the Common Biometric Exchange Formats Framework (CBEFF) standards that provide for the addition of metadata (such as date captured, expiry date, capture device information, and security information supporting integrity, and/or encryption) to a biometric data format (a fingerprint image or minutiae, an iris image, dynamic information related to a signature, etc., a

biometric data block or BDB). The second set is the Biometric Application Programming Interface (BioAPI) standards that provide for interchange of biometric information between modules (provided by different vendors) within a single biometric system. The third is the BioAPI Interworking Protocol (BIP) that provides for the exchange of biometric information and control of biometric devices between systems (provided by different vendors) over a network.

Introduction

This entry in the Encyclopedia describes the main standards specified by ISO/IEC JTC1/SC 37/WG2. WG2 is the working group responsible for biometric technical interface standards.

Biometric Data Records

There are many different forms of biometrics that can be used for human recognition (see ► [Biometric Data Interchange Format, Standardization](#)). These include the image of a face, a fingerprint, an iris, a signature, DNA, or a portion of speech. In general, comparison requires that features be extracted from the captured data to enable computers to identify the closeness of a match between enrolled data (data that is intended to be used for recognition purposes) and data captured for the purposes of authentication of the human being at a later time (see ► [Biometric System Design, Overview](#)).

There are approximately 15 standards [1] covering data interchange formats for recording such data, and all result in the specification of a biometric data record – a data structure (specified down to the bit level) that records the captured data, with different formats for the data captured before feature extraction and for that captured after feature extraction.

When used for interchange purposes with CBEFF (► [Common Biometric Exchange Formats Framework Standardization](#)), a biometric data record is called a biometric data block (BDB), sometimes referred to as “an opaque data block.”

CBEFF Wrappers

For interchange purposes, a biometric data record needs to be associated with metadata (described below) that relates to that BDB. The package of a BDB with the metadata (and possibly a security block) is then called a CBEFF biometric information record or CBEFF BIR. One of the most important pieces of metadata is to identify (using a worldwide unambiguous identification) the BDB that is included in the BIR, without the need to know the encoding of the BDB. Without this metadata, the nature of the BDB (fingerprint, face image, etc.) needs to be known by some side channel as the BDB formats are generally not self-identifying. A point to be mentioned here is that the encodings used in current BDB formats are sufficiently similar in their initial part that intelligent software could determine which format is present, but the metadata provides an identification without having to attempt to decode the BDB.

This is the first useful level for the interchange or storage of biometric data, unless the same modality or BDB format is used in the database or application always.

There are several forms for a BIR, designed for different applications. Some are binary encoded, and some are XML encoded. These are described below. The format of a BIR is generally referred to as a patron format, as it is defined by a recognized standards development organization that is the producer of open standards – standards that are subject to vetting procedures that ensure that they are technically accurate and have widespread approval (a CBEFF Patron). As of 2008, there is only one registered CBEFF Patron, ISO/IEC JTC1 SC37, though others are expected to follow, and there are many registered biometric organizations.

BioAPI Interfaces and Exchanges

If a BIR has to be passed between modules from different vendors in a single system, then the interfaces between such modules need to be

defined and standardized at the level of a program language interface.

This is the purpose of the BioAPI set of standards, currently defined in terms of C interfaces, but the use of other implementation languages is not precluded.

The BioAPI standard enables one or more applications to control and interact with one or more biometric devices or processes that transform a BDB (e.g., by feature extraction), typically by passing a BIR and control information in a standardized manner (allowing implementation of the relevant modules by different vendors).

BioAPI Interworking Protocol

BioAPI Interworking Protocol (BIP) is the final step in the interchange of biometric data. It builds on the BioAPI functions and parameters but provides a bit-level specification (language and platform independent) of the protocol exchanges needed, over identified network carriers, to allow an application in one system to interact with devices in a remote system, either to control their operation and graphical user interface or to collect a BIR (including one or more BDBs – biometric data records – and security information) from them.

It is not quite true to say that BIP is the final step. There is a requirement to include in BIP transfers the transfer of certificates related to the security policy and certified security of the devices that are being used in distributed biometric capture and processing. This work is in progress in 2008 and is beyond the scope of this entry.

CBEFF

► [Common Biometric Exchange Formats Framework Standardization](#)

History and Motivation

It was recognized at an early stage that definition of formats for recording biometric data (iris, fingerprint, face, signature, etc.) was not sufficient

for interchange purposes and that a minimum requirement was the addition of some metadata. CBEFF defines the elements of such metadata as forming a biometric information record (BIR).

One important (and mandatory) element in a CBEFF BIR is to identify the format of a BDB (fingerprint, face image, signature, etc.), so registration of identifiers for BDB formats (and other related formats) became an essential part of the CBEFF work.

CBEFF (► [Common Biometric Exchange Formats Framework Standardization](#)) started life as a USA Standard with a slightly different title (► [Common Biometric Exchange Formats Framework Standardization](#)) and was proposed for fast-tracking when ISO/IEC JTC1 SC37 was first established.

In the event, it went through the normal standardization process, and many changes were made during that process. CBEFF Part 1 [2] was published as an International Standard in 2006.

There are four parts to the CBEFF set of International Standards.

CBEFF Part 1 [2] defines (at the abstract level) a set of data elements that can be used to record metadata. Note that the definition at the abstract level means that a set of values and their semantics are specified, but the multiple ways of encoding those in a bit-pattern representation are not specified at this level. Additional specifications are needed for the encoding of those values (e.g., using various forms of binary or character representation, including XML representation, and using empty fields to denote common default values). These encoding issues are covered in CBEFF Part 3.

Some data elements are mandatory for inclusion in a CBEFF wrapper (a CBEFF Patron Format), but most are optional for use in the definition of a CBEFF Patron Format. The abstract value “NO VALUE AVAILABLE” is also frequently included for various data elements. This is important, as it enables mappings from a BIR that contains a very little metadata to one that provides for the recording of all (meta)data elements. The rules for this mapping are specified in CBEFF Part 1 [2]. Care should be taken when reading that a data element is “mandatory.” This

statement is made at the abstract level. When using an actual encoding of a header, it is always assumed that the associated patron format is known (otherwise it could not be decoded), and some patron formats can, and do, support only a single value for the “mandatory” data elements and encode those as an empty field (zero bits, zero octets).

CBEFF Part 2 [3] (published 2006) specifies the operation of a Registration Authority that assigns worldwide unambiguous identifications for all the “things” in the CBEFF architecture that need unambiguous identifications. CBEFF Part 2 Registration is described below.

CBEFF Part 3 [4] (published 2007) defines (at the bit level) a number of patron formats that are of general utility (BioAPI defines another and the profile for the seafarer’s identity card, where the encoding space is very limited). See section “CBEFF Part 3 Patron Formats” below.

CBEFF Part 4 [5] (work in progress in 2008) defines (at the bit level) a security block format, but others are expected to be added, including a minimal one for the seafarer’s identity card. CBEFF Part 4 security block (SB) formats are described below.

CBEFF Part 1 Data Elements

CBEFF defines (at the abstract level, devoid of encoding) a number of data elements, with their values, and the semantics of each value.

It also defines an architecture, where there is normally an SBH (Standard Biometric Header) that contains the metadata elements, a BDB, and (optionally) a security block (SB) that contains details of encryption and integrity parameters. This is depicted in Fig. 1.

The following summarizes the data elements (metadata) currently defined in CBEFF Part 1.

CBEFF version: The version of the CBEFF specification used for the elements of the SBH.

SBH	BDB	SB (optional)
-----	-----	---------------

Biometric Technical Interface, Standardization, Fig. 1
A simple BIR

BDB Format owner and format type: These metadata elements identify the (registered) biometric organization that has defined the BDB format and the identifier (typically an integer from zero upward) that has been registered as its identification (see [CBEFF Part 2 Registration](#)). They are mandatory in a BIR and identify the BDB that is contained in the BIR. A point to be mentioned here is that there are BIR formats that contain multiple BDBs, but discussion of these is outside the scope of this entry.

BDB encryption and BIR integrity options: These metadata elements are mandatory but are simple binary values saying whether the BDB is encrypted or not or whether there is an integrity value for the BIR provided in a security block. If either of these is “YES,” then the security block has to be present to provide the necessary security details; otherwise the security block is absent. We are operating here at the abstract level. A particular patron format may support only one of these values. If only one is supported by a particular patron format (e.g., NO encryption, NO integrity), then these values can be encoded as a null coding (depending on the nature of the encoding), so need not take up bit space (which matters for some applications).

BDB biometric type and subtype: This provides a broad identification of the nature of the BDB. Its value can be deduced from the “format owner and format type” but only through the registration authority, and it is not computer friendly. It identifies the broad nature of the format (finger, face, signature, ear, iris, vein, etc.), with the subtype identifying which finger, ear, iris, etc. The categorization is a bit ad hoc and has changed over time and will probably continue to change.

BDB product owner and product type: These two data elements identify the owner (a registered biometric organization – see [CBEFF Part 2 Registration](#)) and identification of the device/software used to produce the BDB.

BDB creation date and validity period: The date on which the BDB was created and the start and end of validity period. The use of the validity period depends on the application.

BDB purpose: This identifies the reason for the capture of the BDB – for enrolment or for

verification (and there are other options). The use of this field in actual applications is not clear yet.

BDB processed level: Again, this is implicit in the registered identifier, but it gives a broad indication of whether this is “raw” data, an enhanced image, or a format that has extracted features from an image. Values are “raw,” “intermediate,” or “processed,” which are very broad terms. The author is not aware of systems that use or require this information.

BDB quality: This is quite an important field, but there is still a lot of work ongoing to determine “quality” values for a BDB. It relates to whether a fingerprint is known to be smudged or not, how many pixels were used in the capturing of an image, whether a signature had enough turning points for minutiae extraction, etc. Work is ongoing in this area. (See ► [Biometric Sample Quality, Standardization](#)). It is likely that when the ongoing work is completed, this part of the Standard will be amended.

BDB index: A metadata element that can be used to point to a database entry for the BDB, rather than having the BDB encoded as part of the BIR. The use of this for storage is clear, but it is arguable that it is not needed, as the BIR is only defined at the abstract level, so encoding a BDB is not needed. The author is not aware of any current use.

Challenge/response: This provides data for security purposes when trying to retrieve the associated BDB from a database (like the registration procedure followed in a bank where a question is asked (e.g., “a favorite book”) and the response to that). It is not yet clear as to how this field can be practically used.

Security block (SB) format owner and type: These metadata elements identify the (registered) biometric organization that has defined the SB format and the identifier (typically an integer from zero upward) that has been registered as its identification (see [CBEFF Part 2 Registration](#)). They are mandatory if a security block is included.

BIR creator, creation date, and validity period: These data elements recognize that the BDB may have been created at a certain time but

that this BIR (following possible processing, perhaps on a remote machine) may have been produced by a different vendor at a different time. The “creator” is just a string of Unicode characters, is not registered, and, hence, may not be unambiguous. Examples of a “creator” might be “US Dept of State” or “Passport Australia.”

BIR patron format owner and type: The main (probably the only) use is in the complex BIR format, when a different BIR can be embedded in a simple BIR and BIR patron format owner and type identifies the nature and encoding of the embedded BIR.

BIR patron header version: A version number (major and minor) assigned in the patron format definition.

BIR index: A self-reference to a database entry for this BIR. The author is not aware of its any current use.

BIR payload: A transparent string of octets associated with the BDB. The author is not aware of its any current use.

Subheader count: This is a device to handle a BIR that contains multiple BDBs with different SBHs applied to each. The details are out of the scope of this entry.

CBEFF Part 2 Registration

The CBEFF Part 2 Registration provides for the worldwide unambiguous identification of:

- Biometric Organizations and Biometric Patrons
- Biometric data block formats (BDB formats)
- Patron formats (specific selections of metadata, with a bit-level encoding)
- Security block formats
- Biometric products (devices and/or software modules)

The identification is composed of three components:

- Arcs of the international object identifier tree that identify the register (implicit)
- A registered 16-bit identifier that identifies a biometric organization (of which the biometric patrons are a subset)
- An identification assigned by the biometric organization to a BDB format, a patron

format, a security block format, or a biometric product.

The CBEFF register is currently (2008) maintained by the International Biometric Industry Association (IBIA) and is available at URL <http://www.ibia.org/cbeffregistration.asp>.

There are a large number of biometric organizations registered, a few products, but in 2008 only ISO/IEC JTC 1 SC 37 has registered BDB formats, patron formats, or security block formats.

CBEFF Part 3 Patron Formats

The CBEFF Part 3 Patron Formats specify a range of patron formats designed for use in the areas of different application. The smallest is the minimal binary encoding, where most elements take only a fixed value (typically “NO VALUE AVAILABLE” if the element is optional) and produce zero bits in the encoding. There are other formats that produce XML encodings for the data elements and are capable of encoding the complete range of abstract values of every element.

Some patron formats are defined in English with a tabular format for the bit patterns, so no tool support is available for these.

Others are defined using the Abstract Syntax Notation One (ASN.1), the notation [6] which (provides a schema for both binary and XML encodings) is defined using both XSD (XML Schema Definition [7]) and an equivalent ASN.1 schema for an XML encoding, in addition to the English language specification.

Both the ASN.1 and XSD schemas are supported by a range of tools on many platforms.

In 2008 there are 17 patron formats defined, and they are the following:

- **Minimum bit oriented:** This takes only one octet for the SBH if the BDB format owner is SC 37 and the format type value is less than 64. It is default in all fields to fixed values apart from the BDB format owner and format type. The specification uses the ASN.1 notation and the ASN.1 Unaligned Packed Encoding Rules.

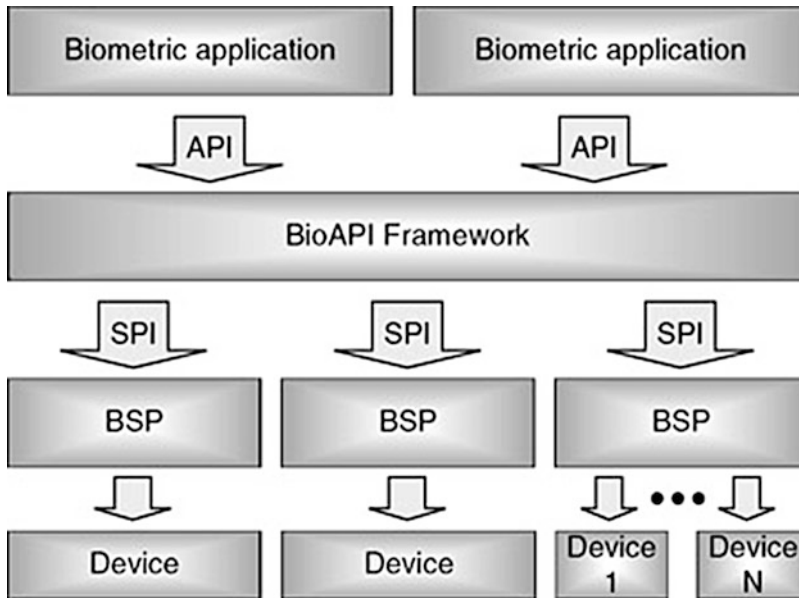
- **Minimum byte oriented:** This takes four octets and is specified with tables, diagrams, and English language.
- **Fixed-length fields, byte oriented:** This can handle all data elements (with some length restrictions), but optional ones that are absent (NO VALUE AVAILABLE) encode with a single “presence” bit of zero. The specification uses tables and English language.
- **Fixed-length fields, bit oriented:** This can handle all data elements, of arbitrary length (so length fields are frequently present), but optional ones that are absent (NO VALUE AVAILABLE) encode with a single “presence” bit of zero. The specification uses ASN.1 and the ASN.1 Unaligned Packed Encoding Rules.
- **Full support, TLV format:** This can handle all data elements. Length fields are always present, and every element is preceded by an identifying tag (or type) field. It is based on the earlier use in smart cards and uses an ASN.1 specification with the type length value (TLV) Basic ASN.1 Encoding Rules.
- **This supports nested BIRs within BIRs:** Specified with tables and English, with supporting ASN.1.
- **XML encoding:** Specified with tables and English language, with supporting ASN.1 (XML Encoding Rules) and XSD specifications.

There is also a patron format defined in BioAPI, largely for historical reasons.

CBEFF Part 4 Security Block (SB) Formats

CBEFF Part 4 Security Block (SB) formats is in progress in 2008, so a detailed discussion is not appropriate. At present, there is only one security block format being defined that handles all necessary security parameters for either encryption or integrity, or both, and allows the use of a wide range of security algorithms.

It is likely that a more minimum SB format will be defined for use with the seafarers’ identity card (a standard being progressed by ISO/IEC JTC1 SC37) and handles only integrity with fixed algorithms (See ► [Biometric Security Standards](#)).



Biometric Technical Interface, Standardization, Fig. 2 BioAPI architecture

BioAPI

Biometrics API/Interfaces

History and Motivation

Multiple application modules (perhaps from different vendors) should be allowed to interact (serially or simultaneously) with multiple modules supporting various biometric devices. Standard interfaces are needed to allow these modules to potentially be provided by different vendors.

The concept of a “framework” module, with which applications attach above and device-related software attaches below, providing a general routing function for commands and data transfer, is the main part of the BioAPI architecture.

There are four groups of standards in the BioAPI set.

The first is the base standard – BioAPI Part 1 [8] (published in 2006, but with several amendments to extend its functionality). This part defines the concept of the BioAPI framework module which interacts above with applications, using a C-defined API, and below with Biometric Service Providers (software and hardware related to biometric devices) using a C-defined Service

Provider Interface (SPI), broadly mirroring the functionality of the API. This is illustrated in Fig. 2 – BioAPI architecture. It also has a specification for graphical user interface to enable an application to control the “screens” for use during a capture operation.

The second group (currently only BioAPI Part 2 [9] and Part 4 [10]) is a set of standards providing a lower-level interface within a BSP to a so-called function provider module that is distinct from the vendor of the BSP module. This interface is designed to minimize the requirements on a device vendor and to enable the provider of software for a BSP to use modules from many different device vendors. Detailed interfaces are not covered in this entry.

Part 2 [9] was published in 2007 and provides an interface to archive devices (databases). Part 4 [10] is in progress in 2008 and provides an interface to sensor (capture) devices. Similar interfaces for matching algorithm modules and general processing modules are planned, but have not been started in 2008.

The third is a BioAPI Lite standard (BioAPI Part 3 [11]) that is intended to provide support for embedded devices. This is not mature in 2008 and will not be discussed further.

The fourth is a standard [12] specifying how to use the BioAPI interfaces to support the so-called ten-print slap – a roll of ten fingers, an image of four left fingers, an image of four right fingers, and an image of two thumbs – and the subsequent processing of the returned BDB, possibly to extract parts of the BDB to individual BDBs.

In fact, this standard is rather more general than just supporting a ten-print slap and recognizes the concept of gathering data into a single BIR from a number of different biometric devices, possibly of different modalities. This introduces a new BIR concept of a complete (complex) BIR with “holes” in it (place holders) that will be filled in whenever possible when passed to a BSP and can then be passed to other BSPs to complete it. The interesting thing is that this development does not require any change to the basic BioAPI architecture or function calls – these already allowed the transfer of a BIR to a BSP (e.g., for image enhancement purposes), with return of a new BIR. It is in progress in 2008 and is not discussed further but is likely to become important.

BioAPI Part 1

The two interfaces (API and SPI) are very similar, as the framework provides mainly routing and (when augmented with BIP functionality – see [Biometric Interworking Protocol \(BIP\)](#) below) communications functionality to remote systems.

Indeed, there is an amendment to Part 1 that is being developed which recognizes the use of a reduced API/SPI to provide a direct interface between an application and a BSP, with support for multiple BSPs, or multiple applications being done entirely through the (nonstandardized) operating system. This is called “frameworkless BioAPI.”

BioAPI generally assumes that the BSP is not state-free, so there can be a request for a BDB to be captured and a “handle” returned pointing to it. It is stored in memory controlled by the BSP and later “exported” to the application through a subsequent call. Thus, there are several memory management functions and parameters.

The normal sequence of interaction between any application module and (through the framework) a BSP module is described below. Note that there can be multiple such simultaneous interactions related to one application and multiple BSPs or BSP instances or related to one BSP and multiple application modules or instances. The normal sequence has some options within it (controlled by the application), and there can be a variety of error returns or signals that can disrupt the sequence. There are a variety of parameters that can be passed by the application to control the way the BSP operates, but these are beyond the scope of this entry. The normal sequence is:

- *Init*: This introduces the application instance module to the framework module and establishes that they both are using the same version of the interface specification.
- *Load BSP*: This tells the framework that (at least one) application instance wants to communicate with it.
- *BSP attach*: This initiates a dialogue with the BSP and establishes an error reporting mechanism.
 - Enroll for verification*: This initiates a capture and returns a BDB, suitable for enrolment of the subject.
 - Verify*: This initiates a capture and returns a BDB, suitable for verification against a previously stored biometric reference or template.
- *BSP close*: This says that the application is no longer interested in interactions with the BSP.

Of course, multiple calls between attach and close are possible. There are also calls to the framework to establish what BSPs are available, and their properties, but this is too detailed for this entry.

Tool Support

Implementations of the framework module are available from a number of vendors.

Implementations of BSPs that support the standardized (SPI) interface are still emerging (2008), as are application modules using the BioAPI API interface.

Biometric Interworking Protocol (BIP)

History and Motivation

The need for an application to interact with remote biometric devices (or with modules processing and transforming biometric data) over a network, in a fully standardized manner (providing vendor independence of the communicating systems) in the standardization process, was recognized early.

BioAPI was seen as the appropriate base for this. Essentially, the BIP specification extends the functionality of a BioAPI framework to allow it to route calls from an application to a remote framework (and hence a remote BSP) and to support the return of appropriate results.

It also supports the provision of a remote Graphical User Interface (screen), controlled by a remote application, to perform a capture.

Fundamentally, it provides a mapping from the BioAPI Part 1 C-functions and data structures into protocol elements and ASN.1 data structures that are then encoded with the ASN.1 unaligned packed encoding rules.

This means that a BIP-enabled framework can communicate with another BIP-enabled framework for communication between local applications and remote BSPs (or vice versa).

It is important to note that a computer system can support BIP if it provides the appropriate “bits-on-the-line” exchanges that would occur if it had a BioAPI framework module. The BIP specification is based on BioAPI but is a fully defined protocol that creates no constraints on the internal structure of the communicating systems. In terms of communication “bits-on-the-line,” internal module structure is invisible and irrelevant. The concept of a BioAPI framework is used in the specification of the messages, but that does not need to form a part of the internal structure of the communicating systems.

Supported Network Mappings

The BIP Standard is a fully defined protocol over TCP/IP (the Internet) using a recommended port

of 2376, registered with the Internet Assigned Numbers Authority (IANA).

It also specifies discovery and announcement protocols based on both IPv4 and IPv6. It also specifies its use over W3C SOAP/HTTP.

Tool Support

There are many tools supporting ASN.1 defined protocols that can be used, but there are some vendors already advertizing full BIP support within a BioAPI Framework.

Related Entries

- ▶ [BioAPI, Standardization](#)
- ▶ [Biometric Data Interchange Format, Standardization](#)
- ▶ [Biometric Interfaces](#)
- ▶ [Biometric Sample Quality, Standardization](#)
- ▶ [Biometric System Design, Overview](#)
- ▶ [Biometric Security Standards](#)
- ▶ [Biometric Vocabulary Standardization](#)
- ▶ [Common Biometric Exchange Formats Framework Standardization](#)
- ▶ [Multibiometrics and Data Fusion Standardization](#)

References

1. All parts of ISO/IEC 19794 *Biometric Data Interchange Formats*
2. CBEFF Part 1 (ISO/IEC 19785-1) *Data Element Specification*
3. CBEFF Part 2 (ISO/IEC 19785-2) *Procedures for the Operation of the Biometrics Registration Authority*
4. CBEFF Part 3 (ISO/IEC 19785-1) *Patron Formats*
5. CBEFF Part 4 (ISO/IEC 19785-1) *Security Blocks*
6. ASN.1 (ISO/IEC 8824-1) *Abstract Syntax Notation One*
7. XSD W3C XML Schema
8. BioAPI Part 1 (ISO/IEC 19784-1) *BioAPI Specification*
9. BioAPI Part 2 (ISO/IEC 19784-2) *Archive Function Provider Interface*
10. BioAPI Part 3 (ISO/IEC 19784-3) *BioAPILite*
11. BioAPI Part 4 (ISO/IEC 19784-4) *Function Provider Interface*
12. BioAPI Ten-print (ISO/IEC 29129) *Tenprint capture using BioAPI*

Biometric Template Binarization

Meng-Hui Lim¹ and Andrew B.J. Teoh²

¹Department of Computer Science, Hong Kong Baptist University, Kowloon Tong, Hong Kong

²School of Electrical and Electronic Engineering, Yonsei University, Seoul, South Korea

Synonyms

Biometric discretization

Definition

Biometric binarization is the process of converting real-valued biometric features into a binary string. For many modalities (e.g., face, fingerprint, and signature) where the extracted features are intrinsically real valued, biometric binarization is developed for transforming the features into an acceptable form of input to many template protection schemes such as fuzzy commitment, fuzzy extractor, secure sketch, and helper data systems. Due to noisy nature of biometrics, the binary biometric representation extracted during verification may contain errors (bit differences) with reference to the reference template. The number of bit differences must not exceed the system (Hamming distance) decision threshold for obtaining a positive match.

Biometric binarization can be assessed using three criteria – performance, security, and privacy. Performance is referred to as the classification performance of binary representations where a good performance of a binarization methodology implies extraction of highly distinctive binary representations from the users. This is imperative in thwarting “passive” impersonation attempts (minimizing false accept) and diminishing genuine verification failures (minimizing false reject) with respect to the system decision threshold. The security criterion requires binary representations to contain high information entropy (unpredictability) especially when the relevant

helper data (auxiliary information) stored in the system is compromised. This is important to protect the system from any adversarial brute force attack. Finally, the privacy criterion requires the helper data not to leak any sensitive information about the user itself in the case of helper data disclosure, since the compromise of one’s biometric data is permanent and irrecoverable.

Typical biometric binarization involves a quantization and an encoding process. Quantization segments a feature space into a number of intervals, and encoding tags each interval with a binary label so that features falling into an interval can be mapped to the corresponding binary label. When multiple feature spaces are involved, the individual binary outputs can be concatenated to form the final binary representation of a user.

Biometric binarization can broadly be classified in accordance with its quantization fashion: univariate vs. semi-multivariate vs. multivariate and static vs. dynamic. In accordance with the number of intervals defined in each feature space, different encoding can be considered. Univariate quantization performs quantization on each single-dimensional feature component by assuming independency among these components; semi-multivariate quantization performs quantization on each subset of multiple single-dimensional feature components by assuming independency among these subsets, while multivariate discretization performs quantization directly on a high-dimensional feature space that takes into account all the feature components. On another axis, static quantization creates equal partitions on each feature space, while dynamic quantization optimizes system false accept rate and/or false reject rate by creating varying number of partitions in each feature space. Dynamic quantization can be regarded as a weighting process where the more discriminative a feature component is detected to be, the more the segments will be formed or equivalently, the more the bits (the heavier the weight) will be assigned. This is due to that the maximum Hamming distance of the binary output of a dimension is dependent on the number of bits assigned to that dimension during the eventual matching process.

Introduction

Binary biometric representation is not only desired for biometric template protection and biocrypto key generation but also enables efficient template matching and storage, which is especially crucial when the processing time and storage space are of high concern. The fuzziness nature of biometric measurements often leads to nontrivial variation in the extracted query binary representation, thus affecting the stability of the representation. When exact matching is needed in the process of authentication, these fuzzy representations have to be corrected with respect to the reference binary template in the enrolment phase in order to obtain a positive match. As a consequence, extracted genuine binary strings often need to undergo an error correction process before it can be transformed into an exact input for use in the subsequent cryptographic applications. Hamming distance is a typical measure for evaluating the dissimilarity between two binary strings. A query binary string is accepted only if the Hamming distance between query and template bit string is not higher than a decision threshold distance.

A common way of generating a binary biometric representation is via biometric binarization based on the statistical distribution of training data. In general, biometric binarization can be decomposed into two essential components: biometric quantization and feature encoding. These components may be governed by a static or dynamic bit allocation algorithm, determining whether the quantity of binary bits allocated to every feature dimension is fixed or varied, respectively. Given a collection of extracted feature vectors of all users, a feature space is initially quantized into intervals. Each feature element is then mapped into a short binary string according to the label of the interval where the feature element is enclosed within.

The assessment of biometric binarization can be made based on the following three criteria:

- **Performance:** Adequate preservation of significance of real-valued features (from the feature extractor) by the discretizer is important to guarantee good recognition accuracy. This

requires the extracted binary representation to be at least as discriminative as the real-valued features. A better discretization includes a bit allocation process to ensure that only discriminative feature components are heavily weighted to obtain higher bit stability or accuracy in recognition performance.

- **Security:** High information in binary biometric representation is desired because it creates huge possibilities of binary representation that inhibits a brute force attack. Binarization output security can be measured using Shannon entropy. Output entropy can be heightened through (1) increasing the feature dimensions for extraction and/or (2) increasing the number of segmentations. Both such ways could in fact increase the number of possible binary representations. However, it is required that the revelation of auxiliary data must not expose any crucial information about the generated binary biometric representation to avoid facilitation of an adversarial attack.
- **Privacy:** A high level of protection is needed to prevent leakage of any user-specific information other than the verification decision of the system. Apart from the biometric data, it is also important to protect unnecessary yet sensitive information such as ethnic origin, gender, and medical condition. Since biometric data is inextricably linked to the user, it can never be reissued or replaced once compromised. Therefore, the auxiliary data must be uncorrelated to biometric data to avoid any possibility of privacy violation. Otherwise, it will have no difference from storing the biometric features in explicitly in the system database.

In general, there are a few dimensions by which binarization methods can be classified:

- (a) *Univariate vs. semi-multivariate vs. multivariate:* Univariate binarization quantizes every feature component individually by assuming independency among the components; semi-multivariate binarization considers multiple subsets of components and partitions them individually, while multivariate binarization considers the

feature components as a whole when quantization is performed.

- (b) *Static vs. dynamic*: Static binarization creates equal partitions in each feature space, while dynamic binarization optimizes system FAR and/or FRR by creating varying number of partitions in each feature space. Dynamic binarization can be regarded as a weighting process where the more discriminative a feature component is detected to be, the more the segments will be constructed or equivalently the more the bits (the heavier the weight) will be assigned. This can be justified from the fact that the maximum Hamming distance of the binary output of a dimension is dependent on the number of bits assigned to that dimension during the eventual matching process.

Univariate Static Approach

Perhaps the simplest binarization scheme is threshold-based binarization, where each feature space is partitioned into two quantization intervals based on a global threshold and a single-bit encoding scheme with two binary labels (“0” and “1”) is employed.

Equal-width quantization-based binarization is another univariate static approach that partitions every feature space (ranging from minimum v_{\min} to maximum sample value v_{\max}) into S nonoverlapping equal-width intervals of the following width: $\frac{v_{\max}-v_{\min}}{S}$. However, this binarization technique is very sensitive to the range of feature values, since the quantization can easily be affected by outliers. In practice, binary label in certain intervals may have higher probabilities to occur when the population probability distribution is not uniform. An adversary could succeed much easier in guessing the binary representation of a target user by outputting the binary label associated with higher probability of occurrence in each feature space. This also implies lower output entropy than the ideal case where the population distribution is uniform.

Furthermore, Linnartz-Tuyts developed a user-specific equal-width quantization-based

binarization scheme [12] that partitions each feature space into equal-width intervals that are labeled with binary “0” and “1” interchangeably. Given a designated binary output of a user, an offset is derived to shift the user feature distribution to the center of the closest interval (a.k.a. genuine interval) that has the same label as the selected binary output so as to minimize intra-user variation. Besides suffering the same drawback of limited output entropy as the thresholding scheme, another critical problem with this scheme is the potential exposure of the genuine measurements or the user’s probability density function (pdf), since the act of aligning the user pdf to the center of one of the intervals serves as a clue at which the user pdf or measurements could be located to the adversary. As a consequence, the number of possible locations of user genuine measurements can be drastically reduced to the number of central points of the intervals, thus facilitating adversarial guessing of the binarization input.

Entropy-quantization-based binarization [7] is a supervised technique that improves recognition of binary biometric representation by splitting each feature space recursively and inducing intervals that favors classification through minimizing class entropy (sample impurities) in every interval. The class information entropy of a segment induced by a specific cutpoint q on the d -th feature space is defined as $E(d, q; \gamma) = \frac{|\gamma_1|}{|\gamma|} E(\gamma_1) + \frac{|\gamma_2|}{|\gamma|} E(\gamma_2)$, where $E(\gamma_1)$ and $E(\gamma_2)$ represent the entropy of subset γ_1 and γ_2 , respectively. The interval cutpoint q for which $E(d, q; \gamma)$ is minimal among all the candidate cutpoints is taken to be the best cutpoint for a split. The final intervals are induced in such a way that majority samples enclosed within each interval belong to a specific identity.

Univariate Dynamic Approach

A univariate dynamic binarization scheme usually allocates different quantity of bits to each feature component of a user according to

the discrimination power of these components. Chang et al. [1] and Hao-Chan [6] presented a dynamic bit allocation-based binarization scheme, where the j -th user feature distribution with mean μ_j^d and standard deviation σ_j^d on the d -th feature space is used as a basis for constructing the genuine interval, such that $\text{int}_j^d = [\mu_j^d - k\sigma_j^d, \mu_j^d + k\sigma_j^d]$, where k is a free parameter. The remaining intervals are constructed based on constant width $2k\sigma_j^d$. These two schemes adopt direct binary representation (DBR) of the discrete interval indices (i.e., $1_{10} \rightarrow 000_2$, $2_{10} \rightarrow 010_2$, $3_{10} \rightarrow 011_2$) for encoding, and they have different boundary interval handling techniques. The latter scheme unfolds the feature space arbitrarily to include all remaining possible feature values in forming the leftmost and rightmost boundary intervals, whereas the former extends each feature space to account for the extra “virtual” equal-width intervals in forming 2^n intervals so as not to lose any entropy from not utilizing the complete elements of an n -bit binary code. Since μ_j^d and σ_j^d , as well as $\text{int}_{j(\min)}^d$ and $\text{int}_{j(\max)}^d$, are very likely to be distinct for different feature space, the resultant number of intervals would vary in direct proportion with the discrimination power of the feature component. Despite being able to improve the recognition performance, they suffer from the abovementioned privacy weakness [4, 12]. An additional security problem with these approaches is the potential occurrence of entropy leakage. In fact, the nonviable labels of all extended intervals (including the boundary intervals) permit an adversary to eliminate those codeword labels from his output-guessing range after either observing the helper data or identifying the “virtual” intervals through estimating the population distribution in each feature space.

Equal-probable quantization-based binarization partitions each feature space into S^d nonoverlapping intervals, where each interval encapsulates equal population probability mass $\frac{1}{S^d}$. Chen et al. [4] developed a user-specific dynamic equal-probable quantization-based binarization technique based on likelihood ratio:

$LR_j^d = \frac{p_j^d}{p_b^d}$, where p_j^d and p_b^d represent the j -th user and population feature distribution on the d -th feature space, respectively. For each feature space, the range of likelihood ratio values exceeding a prefix threshold p is taken to induce the j -th user’s genuine interval. Since the likelihood ratio of each single-dimensional user distribution is likely to be different, the different number of quantization intervals induced in each dimension leads to varied number of bits allocated to each dimension. Intervals other than the genuine are then constructed equal – probably with reference to the population probability mass captured by the genuine interval. The remaining boundary intervals usually contain insufficient probability mass and are wrapped into a single interval that is tagged with a common label from a BRGC code (i.e., $1_{10} \rightarrow 001_2$, $2_{10} \rightarrow 011_2$, $3_{10} \rightarrow 010_2$). However, from an adversarial standpoint, the boundary codeword (resp. the location of boundary intervals) can in fact be eliminated from adversarial guess in security (resp. privacy) violation, since the boundary intervals are unlikely to be the genuine interval. Thus, the adversary is granted a certain amount of guessing advantage due to such nontrivial entropy leakage. Furthermore, this binarization technique suffers from the same privacy weakness as Linnartz-Tuyts’s [12] binarization scheme as elaborated earlier, since the maximum likelihood ratio is also aligned to the center of the genuine interval when the underlying population and user distribution are assumed to be Gaussian.

Teoh et al. [14] presented a standard-deviation-based bit allocation scheme for binarization. This scheme searches for an optimal number of quantization intervals in order to well-capture user distribution in each feature dimension. This scheme initially estimates the user distribution for each dimension and allocates a certain number of bits to each dimension (e.g., n^d bits for the d -th dimension) depending on how discriminative the user distribution of that dimension is. The maximum n^d number of bits, which can generate 2^{n^d} equal-width intervals of width larger than twice the standard deviation σ_j^d of the estimated pdf, is chosen. Eventually, the

resultant n^d is likely to be unequal for different dimension and user, since σ_j^d is dimension and user specific. Upon concatenation of individual binary outputs of unequal length, the final binary representation of each user will be of unequal length too.

Another more effective bit allocation approach called “Detection Rate Optimized Bit Allocation” (DROBA) [5] uses *detection rate* δ as the bit allocation measure. Detection rate is referred to as the user probability mass captured by the genuine interval and it only corresponds to a specific bit allocation setting, such that $\delta(n^d) = \int p_j^d(v)dv$. DROBA maximizes the overall detection rate through finding maximum detection rates among all possible quantization settings in each dimension such that the overall bit allocation to all dimensions is optimal. In fact, maximizing the overall detection rates is equivalent to maximizing the probability of genuine features staying within the relative genuine intervals, thus attempting to achieve minimum intra-user variation in the final binary string with respect to the reference string. Similar to the other dynamic binarization approaches, DROBA aims to assign more bits to discriminative feature components and fewer bits to nondiscriminative feature components. In fact, such an optimal bit assignment is crucial in achieving promising matching performance.

Lim et al. [10] presented a bit allocation algorithm that uses BRGC to encode multiple measurements of each feature component of an identity and subsequently decides the quantity of bit allocation to each feature component (proportionate with the degree of interval merging) in accordance with how stable each bit of the encoded features is during training. This scheme bases upon a combination of bit statistics (reliability measure) and signal to noise ratio (discriminability measure) in performing feature selection and bit allocation procedures. Similar to DROBA, this scheme has the objective of accommodating every estimated user pdf optimally by using different amount of intervals merging so as to ensure the binary output derived from each feature component to be as stable as possible.

Semi-multivariate Static Approach

In general, semi-multivariate static approach allocates equal amount of bits to each component feature that is formed by multiple features of a user. A segmental vector quantization was introduced [11] to generate a feature descriptor (a short sequence of binary bits for releasing the correct share of binary key from a lookup table) by first segmenting sequence of voice frames in the utterance into roughly equal-length contiguous segments, which was deemed the best strategy to divide the sequence into component sounds. The frame sequence is then matched against a speaker-independent, text-independent model of speech (built from many different utterances from many different speakers), quantized into a bunch of different centroids representing different segments and associated to multivariate normal distribution. This centroids-deriving segmentation algorithm being very similar as segmental vector quantization is an iterative process, where the solution belongs to a near-optimal segmentation of the user’s utterance. Once the segmentation solution is obtained, this scheme partitions each segment into two partitions according to a preset threshold, which can be viewed as a high dimensional 2-segment threshold quantization. Based on the threshold, a binary bit is then mapped to each frame segment, and the feature descriptor can finally be formed upon concatenation.

Another semi-multivariate approach called the fuzzy genetic clustering (FGC)-based segmentation [13] uses a variable string representation to encode the cluster centers and adopts the XB criterion (a function of the ratio of the total intra-cluster variation to the minimum separation of the clusters) as the fitness function for selecting the best individuals in creating the population in the next generation of the evolution from the previous population and their offspring. During the evolution, the FGC algorithm sequentially selects parents for reproduction based on the k -fold tournament selection method, performs arithmetic crossover on the paired parents, applies Gaussian mutation to each offspring, and creates a new generation for evolution. These processes are repeated until the stopping criterion is met

(i.e., when the fitness value of the best population individual has not changed for a prespecified number of generations). Finally, the output of the algorithm will be the best clustering solution encountered during the evolution. In this way, each selected component feature (consists of multiple features) of a user will be assigned the binary label of the corresponding clustering outcome (based on DBR encoding) and thus contributes its share of the final binary representation.

Chen et al. introduced a pairwise polar quantization technique [2] in which every two feature components in Cartesian coordinates are paired up for extracting the corresponding polar coordinates (phase and magnitude features) for single-dimensional quantization. This quantization scheme seeks for an optimal feature pairing configuration so as to maximize the discrimination of the binary string between the genuine and the imposter Hamming distances, also defined as the ratio of inter-user scatter to intra-user scatter. It is speculated that the distance between the feature pair mean and the origin dominates the inter- and intra-user scatters and two feature pairing strategies are considered in determining how the feature components should be paired up in order to optimize the discrimination power of the binary output. The pairing strategies include: (a) long-short strategy that selects feature components with a large mean and a small mean as a pair, keeping their distance large, and (b) long-long strategy that selects either both with large means or both with small means, keeping their distance far away from the boundary. Long-short strategy was applied on phase, while long-long strategy was applied on magnitude in forming the feature pairs, and it was reported [2] that the former provides much better binarization performance than the latter.

Semi-multivariate Dynamic Approach

With the validated reliability of long-short strategy on the phase information of the feature pairs [2], Chen et al. presented a pairwise adaptive phase quantization technique [3] together with a long-short strategy to maximize the overall

detection rate of the features. This bit allocation scheme works in a very similar way as DROBA with the exception that the phase information of each feature pair is used for quantization rather than the Cartesian axis. This scheme can in fact be applied to any two-dimensional feature vector as long as its population distribution is circularly symmetric about the origin.

Multivariate Approach

Since biometric feature components are usually interdependent, separately considering feature components in binarization results in suboptimal binarized features (suboptimal security and performance). As such, multivariate binarization, which considers all feature components as a whole, is always more capable of capturing important interactions among the feature components when quantization is performed, thus leading to more meaningful binarization output. A multivariate binarization approach based on medoid-based segmentation and linearly separable subcode encoding [9] was presented [8], where a medoid-based clustering is carried out on the complete set of training data and the resultant clustering setting is employed during query. In this scheme, each feature vector representation is viewed as a point in the high-dimensional feature space and the binary label of the cluster that encloses this high-dimensional feature point will be taken to be the final binary representation of the user.

Summary

Binary biometric representation can be extracted via binarization: a sequential process of quantization and encoding. Biometric binarization can be classified in accordance with its quantization fashion: (a) univariate vs. semi-multivariate vs. multivariate and (b) static vs. dynamic. Among the numerous approaches in the literature, univariate binarization seems to be the most popular approach. However, in practice, the binary biometric representation

may not contain the expected amount of information due to the mismatch of independency assumption, thus resulting in lower output entropy than expected. The current development of biometric binarization is moving towards a binarization scheme that achieves optimal biometric recognition performance and output security. At this stage, more diverse binarization techniques could still be explored in terms of quantization and encoding techniques. Rigorous analyses on binarization schemes are also required to provide relevant performance and security guarantees.

Related Entries

- ▶ [Biometrics, Overview](#)
- ▶ [Template Security](#)
- ▶ [Privacy issues](#)

References

1. Y. Chang, W. Zhang, T. Chen, Biometric-based cryptographic key generation, in *Proceedings of IEEE International Conference on Multimedia and Expo (ICME'04)*, Taipei, vol. 3, 2004, pp. 2203–2206
2. C. Chen, R. Veldhuis, Binary Biometric Representation through Pairwise Polar Quantization, in *Proceedings of the 3rd International Conference on Advances in Biometrics (ICB'09)*, Sardinia Island, LNCS, vol. 5558, 2009, pp. 72–81
3. C. Chen, R. Veldhuis, Binary biometric representation through pairwise adaptive phase quantization. *EURASIP J. Inf. Secur.* **2011**, Article ID 543106, 16pp (2011)
4. C. Chen, R. Veldhuis, T. Kevenaar, A. Akkermans, Multi-bits biometric string generation based on the likelihood ratio, in *Proceedings of 1st IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS'07)*, Washington DC, 2007, pp. 1–6
5. C. Chen, R. Veldhuis, T. Kevenaar, A. Akkermans, Biometric quantization through detection rate optimized bit allocation. *EURASIP J. Adv. Signal Process.* **2009**, Article ID 784834, 16pp (2009)
6. F. Hao, C.W. Chan, Private key generation from online handwritten signatures. *Inf. Manage. Comput. Secur.* **10**(4), 159–164 (2002)
7. A. Kumar, D. Zhang, Hand Geometry Recognition using Entropy-based Discretization. *IEEE Trans. Inf. Forensics Secur.* **2**, 181–187 (2007)
8. M.-H. Lim, A.B.J. Teoh, Non-user-specific multivariate biometric discretization with medoid-based segmentation, in *Proceedings of 6th Chinese Conference on Biometric Recognition (CCBR'11)*, Beijing, LNCS, vol. 7098, 2011, pp. 279–287
9. M.-H. Lim, A.B.J. Teoh, A novel class of encoding scheme for efficient biometric discretization: linearly separable subcode. *IEEE Trans. Pattern Anal. Mach. Intell. (TPAMI)* **35**(2), 300–313 (2013)
10. M.-H. Lim, A.B.J. Teoh, K.-A. Toh, An efficient dynamic reliability-dependent bit allocation for biometric discretization. *Pattern Recognit.* **45**(5), 1960–1971 (2012)
11. F. Monrose, M.K. Reiter, Q. Li, S. Wetzel, Cryptographic key generation from voice, in *Proceedings of the IEEE Symposium on Security and Privacy (S&P'01)*, Oakland, 2001, pp. 202–213
12. J.-P. Linnartz, P. Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric templates, in *Proceedings of the 4th International Conference on Audio and Video Based Person Authentication (AVBPA'03)*, Guildford, LNCS, vol. 2688, 2003, pp. 393–402
13. W. Sheng, W.G.J. Howells, M.C. Fairhurst, F. Deravi, Template-free biometric-key generation by means of fuzzy genetic clustering. *IEEE Trans. Inf. Forensics Secur.* **3**(2), 183–191 (2008)
14. A.B.J. Teoh, W.K. Yip, S. Lee, Cancellable biometrics and annotations on BioHash. *Pattern Recognit.* **41**(6), 2034–2044 (2008)

Biometric Verification/Identification/ Authentication/Recognition: The Terminology

James L. Wayman
College of Engineering, San Jose State
University, San Jose, CA, USA

Synonyms

Biometric authentication; Biometric identification; Biometric verification

Introduction

There has been an inconsistency in the use of the terms like “recognition,” “authentication,” “identification,” and “verification” throughout

the literature of biometrics. Particularly, with the applications of automated human recognition technologies becoming more creative, older uses of these terms has become inadequate in describing new systems. In this article, the author will explore some of the historical uses of these terms and suggest some definitions consistent with recent applications of the technologies.

Dictionary Definitions

The entry begins with common, natural-language definitions of these four terms. The Oxford English Dictionary [1] provides definitions for the terms discussed in this entry:

- Authenticate: prove or show to be authentic
- Authentic: of undisputed origin or veracity; genuine
- Recognition: the action or process of recognizing or being recognized
- Recognize: identify as already known; know again
- Verification: process of verifying; the establishment by empirical means of the validity of a proposition
- Verify: make sure or demonstrate that (something) is true, accurate, or justified
- Identification: the action or process of identifying or the fact of being identified
- Identify: establish the identity of
- Identity: the fact of being who or what a person or thing is

Historical Usages

Since the earliest literature of biometrics, a difference in functionality of automated human recognition technologies has been discussed. In 1966, Li et al. [2] wrote:

To simplify this study, the problem was confined to the verification (or rejection) of an utterance as that of an expected informant. This process is defined as *speaker verification* (as opposed to *speaker identification*, which is the

selection of an actual speaker from a population) (*Italics in the original*)

Verification and identification are defined here as two, mutually exclusive applications for biometrics – verification as the recognition of an expected person and identification as the selection of a person out of a population. The 1960s biometrics literature, however, was far from consistent in the use of these terms [3–5].

In 1969, IBM [6] listed “four principal differences that distinguish a verification procedure from an identification procedure” as:

1. An alien class, for which a priori information is not available, is considered by the system.
2. Additional information, the class label, is available for the decision.
3. The class label that is entered can determine which parameters are to be extracted from the pattern.
4. The decision involves only two states, acceptance or rejection of the pattern.

In identification, all possible classes are presumed known, and the decision amounts to the best match of the pattern to a particular class.

The above quote uses the word “class” to mean a “person.” The IBM definitions attempt to be more precise, but limit “identification” to the case where all possible persons (“classes”) are known, though the more common case in practice accepts that previously and unknown persons can be encountered. Tosi [7] and Tosi et al. [8] differentiated identification into “closed trials” (all persons known) and “open trials” (unknown persons presumed to exist). Modern parlance calls these as “open-set” and “closed-set” identification. In closed-set identification, the question asked is “If any, which of the known persons are consistent with the encountered data?” and “None” is an appropriate response in open-set identification, but not a possible response with a closed-set. Closed-set identification is the easier task, as the person represented by the data is guaranteed to be among those known to the system.

Real-world applications are almost always open-set [9], allowing for the possibility of encountering someone who is not enrolled

(an “impostor”). Some academic communities within the field of biometrics, however, currently define identification solely as “closed-set.” This community reports, as the outcome of the identification task, an ordering of the enrolled biometric data by similarity to the submitted sample. A sample is considered to be “recognized” if it is among the highest k members of the list, where k is determined by the researcher [10–14].

US government standards in the 1970s [15] did not differentiate between open- and closed-set identification but differentiated between “‘absolute’ identification” and “verification of identification” – the former what is now called as “identification” and the latter as “verification.”

In the 1980s, the International Biometrics Association (IBA) attempted to create a standard set of definitions for use in biometrics [16]. This vocabulary defined verification saying, “Verification of identity is the operation of comparing a submitted biometric sample against a specific claimed biometric reference template to determine whether it sufficiently matches that template.” The IBA did not attempt a definition of “identification,” but offers the definition of “recognition” as “Recognition of identity is the operation of comparing a submitted biometric sample against the population of biometric reference templates to determine whether it belongs to the population and which member of the population it is.” This definition seems consistent with what has been called open-set identification in this entry.

The classical “verification” concept, as defined in [2] quoted above, can be implemented with either a centralized database of stored references for each enrolled user or with a tamper-proof token, such as a passport or card, that carries the reference. For centralized systems, data subjects (the users of the system) must point to their stored reference in some way – either with a PIN, a card, or a unique name. This pointer must refer to only the references of a single enrolled user. Therefore, data subjects cannot be free to choose their own identifiers, but each must be assigned a different identifier.

The Impact of New Algorithms on Terminology

By the mid-1990s, vendors had introduced the term “PIN-less verification” to denote access control systems that did not require data subjects to submit a user identifier with their biometric sample. These systems had the internal programming of an “identification system,” examining all enrolled references to determine if the submitted sample was similar to any, but had the external look and feel of a “verification” system. By the mid-1990s, all commercially available iris recognition access control systems were based on the “PIN-less verification” concept, allowing users physical and logical access without submission of a user identifier. Iris systems modified to allow the input of a user PIN would still search the entire database for a matching reference iris pattern and then compare the PIN stored with the matched pattern to the PIN submitted to further validate the match.

Other approaches in the 1990s [17], based on the concept from forensic fingerprinting of “binning” all similar fingerprints together, allowed users to choose their own identifying PIN or password (which would denote the “bin”) with the understanding that many users might choose the same one. The system would have to compare the submitted biometric samples against the stored references of all users within the “bin” denoted by the submitted PIN. As users would not know how many other references, if any, were identified by the same PIN, such systems would again have the look and feel of a “verification” system, though performing an open-set “identification” function against a group of users. In the case if there was only one user with a particular PIN, the system would degenerate into “verification” as defined in [2]. In other words, the system was performing either “verification” or open-set “identification” depending upon the number of users stored with the PIN that was entered.

By the end of the 1990s, it was clear that there were no longer clear boundaries between “verification” and “identification,” the differences depending upon the specifics of the algorithm and the stored data. Using the classic definitions,

many applications could not be clearly determined as “verification” or “identification.”

Clarifying Meanings

By the early 2000s, clarification of this confusion was clearly needed so that an application could be described independently of the details of the algorithms and data structures used to instantiate it. A study by the US National Research Council (NRC) sought to restore the usability of the terms “authentication” and “identification” [18] in discussion of general computer-based methods for determining user credentials. This study returned to the dictionary definitions above, defining “authentication” as “the process of establishing confidence in the truth of some claim” and “identification” as “the process of using claimed or observed attributes of an individual to infer who the individual is.” The term “verification” was considered by the NRC committee as a term used primarily within the biometrics community and synonymous with “authentication.”

Since at least the 1990s [19], it had been noted that biometric claims could be negative as well as positive – for example, “I am not data subject X” or “I am not enrolled in the biometric system.” Using the NRC definitions, the term “authentication” could be used to describe the process of establishing the truth of such a negative claim and “identification” could be used to describe the outcome of an access control system.

Applying these definitions leads to some clarity of language, restoring the dictionary, natural-language meanings of these terms. “Verification” and “authentication” can apply to positive or negative claims. A data subject, or some other party, need not specify an identifier, such as a PIN, pointing to an enrolled biometric reference. So, for example, biometrics can be used without a user identifier to verify that I am enrolled in the system or that I am not enrolled in the system. Examples of the former are biometric systems used to prevent issuance of multiple enrolment records to the same user. Examples of the latter are often called “watchlists.” With a claimed user identifier, biometric systems can verify that I

am enrolled (known to the system) as X or not enrolled as X. A consequence of this definition is that all biometric systems can be seen as verifying some kind of a claim, whether positive or negative, whether with or without a specified user identifier. The details of either the algorithm or the data structures need not be considered in applying the term “verification.” “PIN-less verification” systems are indeed “verification” systems.

Under the NRC definitions, “identification” is the process of “infer(ring) who the person is,” meaning to return an identifier (not necessarily a name) for that person. This process can include a claim to an identifier by the data subject or by someone else in reference to the data subject (i.e., “She is enrolled as user X”). By these definitions, “identification” and “verification” are not mutually exclusive. A biometric system can identify a person by verifying a claim to a known identity. This usage is consistent with the historical documents such as [4, 5].

At the time of writing this entry, the international standards committee on biometrics, ISO/IEC JTC1 SC37, has tentative definitions for the terms considered in this article [20], shown in the Box 1. The SC37 definitions are compatible with those of the NRC, although SC37 prefers “biometric verification” to “biometric authentication,” the latter being depreciated in the vocabulary corpus. The SC37 definitions do not include “recognition,” deferring to common dictionary definitions for the meaning of that term.

Box 1: Current International Definitions from ISO/IEC JTC1

Biometric verification (biometric application)

Application that shows true or false a claim about the similarity of biometric reference(s) and recognition biometric sample(s) by making a comparison(s)

Example: Establishing the truth of any of the claims “I am enrolled as subject X,” “I am enrolled in the database as an administrator,” and “I am not enrolled in the database” may be considered verification.

(continued)

Box 1: (continued)

Note: A claim of enrolment in a database without declaring a specific biometric reference identifier may be verified by exhaustive search.

Closed-set identification (biometric application)

Application that ranks the biometric references in the enrolment database in order of decreasing similarity against a **recognition** biometric sample

Note 1: Closed-set **identification** always returns a nonempty candidate list.

Note 2: Closed-set **identification** is rarely used within practical systems, but is often used experimentally.

Open-set identification (biometric application)

Application that determines a possibly empty candidate list by collecting one or more biometric samples from a biometric capture subject and searching the enrolment database for similar biometric references

Note: Biometric references may be judged to be similar on the basis of comparison score.

Authentication

Note 1: Use of this term as a synonym for “biometric **verification** or biometric **identification**” is deprecated; the term biometric recognition is preferred.

Related Entries

► [Biometrics, Overview](#)

References

1. J. Pearsall (ed.), *Concise Oxford English Dictionary*, 10th revised edn. (Oxford University Press, Oxford, 2002)
2. K.P. Li, J.E. Dammann, W.D. Chapman, Experimental studies in speaker verification using an adaptive system. *JASA* **40**(5), 966–978 (1966)
3. S. Pruzansky, Pattern matching procedure for automatic talker recognition. *JASA* **35**(3), 345–358 (1963)
4. A.J. Mauceri, Technical documentary report for feasibility study of personnel identification by signature verification, North American Aviation, Inc, Space and Information Systems Division, SID 65–24, Accession No. 00464–65, 19 Jan 1965
5. International Business Machines Corporation, The considerations of data security in a computer environment, IBM Corporation, White Plains, Form 520–2169, 1969
6. R.C. Dixon, P.E. Boudreau, Mathematical model for pattern verification, *IBM J. Res. Dev.* Nov 1969, 717–729. Available at <http://www.research.ibm.com/journal/rd/136/ibmrd1306I.pdf>
7. O. Tosi, H. Oyer, W. Lashbrook, C. Pedrey, J. Nicol, E. Nash, Experiment on voice identification. *JASA* **51**(6), 2030–2043 (1972)
8. O. Tosi, Experimental studies on the reliability of the voiceprint identification technique, in *Proceedings of Third National Symposium of Law Enforcement and Technology*, Chicago, 1970
9. G. Doddington, Speaker recognition evaluation methodology: a review and perspective, in *RLA2C*, Avignon, Apr 1998, pp. 60–66
10. F. Li, H. Wechsler, Robust part-based face recognition using boosting and transduction, in *IEEE Conference on Biometrics: Theory, Applications and Systems*, Washington, DC, 27–29 Sept 2007
11. D.S. Bolme, J.R. Beveridge, A.E. Howe, Person identification using text and image data, in *IEEE Conference on Biometrics: Theory, Applications and Systems*, Washington, DC, 27–29 Sept 2007
12. R.Y.L. Gross, L. Sweeney, X.Q. Jiang, W.H. Xu, D. Yurovsky, Robust hand geometry measurements for person identification using active appearance models, in *IEEE Conference on Biometrics: Theory, Applications and Systems*, Washington, DC, 27–29 September 2007
13. B. Arbab-Zavar, M.S. Nixon, D.J. Hurley, On model-based analysis of ear biometrics, in *IEEE Conference on Biometrics: Theory, Applications and Systems*, Washington, DC, 27–29 Sept 2007
14. S. Cadavid, M. Abdel-Mottaleb, Human identification based on 3D ear model, in *IEEE Conference on Biometrics: Theory, Applications and Systems*, Washington, DC, 27–29 Sept 2007
15. National Bureau of Standards, *Guidelines for Evaluation of Techniques for Automated Personal Identification*. Federal Information Processing Standards Publication 48, Apr 1977
16. International Biometrics Association (IBA), *Standard Biometric Industry Terminology and Definitions: Draft*. IBA Standard BSC 2.6–1987R, Washington, DC, 27 Oct, 1987
17. D.F. Pare Jr., N. Hoffman, J.A. Lee, Tokenless identification of individuals. US Patent 5,805,719, 8 Sep 1998

18. S. Kent, L. Millett, *Who Goes There? Authentication Technologies Through the Lens of Privacy* (National Academies Press, Washington, DC, 2003). Available at http://www7.nationalacademies.org/cstb/pub_authentication.html
19. J.L. Wayman, Fundamentals of biometric authentication technology, *Proceedings CardTech/Securtech*, Chicago, 11–14 May 1999. Available at http://www.engr.sjsu.edu/biometrics/publications_fhwa.html
20. Standing Document 2, Harmonized Biometric Vocabulary, version 7, ISO/IEC JTC 1/SC 37N1978, 12 Feb 2007

Biometric Vocabulary Standardization

Peter Waggett¹, Stephen Clarke², James L. Wayman³, and Rene McIver⁴

¹Emerging Technology, IBM United Kingdom Ltd, Portsmouth, Hampshire, UK

²Jebel Consultant Group, Belconnen, ACT, Australia

³College of Engineering, San Jose State University, San Jose, CA, USA

⁴SecureKey Technologies Inc., Toronto, ON, Canada

Definition

Vocabulary is defined as a “*terminological dictionary which contains a list of designations and definitions from one or more specific subject fields*” [1]. For the subject field of *biometrics*, while there are several publications of biometric vocabularies, historically there has been no single collection of biometric terms and definitions considered by the community as definitive. As a result, there are inconsistencies across biometric literature which negatively impact knowledge representation and transfer. A decade-long effort by ISO/IEC JTC 1 SC 37 has now resulted in a harmonized biometric vocabulary [2] of 121 terms that will surely become the definitive source for both biometric terms and concepts.

Principles of Terminology Development

Four ISO standards [1, 3–5] are currently in publication that provide guidance on terminology work useful both inside and outside the framework of standardization. ISO 1087-1 [1] consists of a set of terms and definitions required for terminology development. Of particular importance are the following:

Characteristic Abstraction of a property of an object or of a set of objects

Concept Unit of knowledge created by a unique combination of *characteristics*

Concept diagram Graphic representation of a *concept system*

Concept system Set of *concepts* structured according to the relations among them

Definition Representation of a *concept* by a descriptive statement which serves to differentiate it from related concepts

Subject field Field of special knowledge

Term General designation of a general *concept* in a specific *subject field*

Applying this vocabulary, ISO 704 [3] establishes a framework to be used in terminology development, outlining general principles of term and definition formulation beginning at the level of concept, with the exploration of the nature of objects within concepts, the relationships between concepts, and the clear and unambiguous representation of objects and concepts within the concept system.

Terminology development within a subject field involves:

- Identifying concepts and understanding their characteristics
- Grouping of related concepts into concept systems
- Representing concept systems through concept diagrams
- Defining concepts
- Attributing terms to each concept

It is important to understand the characteristics of each related concept on a concept diagram to ensure each is truly distinct and that concept dependencies have been identified. Once this is

accomplished, definition crafting becomes a simple matter of wordsmithing using only those characteristics deemed essential for the concept. This process occurs by community consensus within an individual subject field, so clearly the developed vocabulary will apply only to the extent that there is a common understanding of concepts and their relationships. Consequently, as a practical matter, no vocabulary can be completely free of controversy.

ISO 860 [4] specifies a methodology for the harmonization of concepts, definitions, and terms and gives the following definitions important in this endeavor:

Concept harmonization Activity for reducing or eliminating minor differences between two or more concepts that are already closely related to each other

Term harmonization Activity relating to the designation of one concept in different languages by terms that reflect the same or similar characteristics or have the same or slightly different forms

Concept and term harmonization can resolve terminology issues arising when concepts and terms have developed differently in individual languages or language communities or in emerging subject fields where new concepts are developing and terms and definitions appearing in the literature are inconsistent.

The overall objective of applying the methodologies outlined in [3] and [4] is to obtain a consensus-led, subject field-specific vocabulary in which a single term corresponds to a single concept and, conversely, a single concept corresponds to a single term. Moreover, definitions should be precise and noncircular, while terms should be concise and linguistically correct – prerequisites for improving the efficiency of communication in the subject field.

The Development of a Harmonized Biometric Vocabulary

In 2002 the standards body ISO/IEC JTC 1 established Subcommittee (SC) 37 for the purpose

of developing standards in the field of biometrics. As is the case with many JTC 1 Subcommittees, a working group (WG), in this case WG1, was established within SC 37 to develop a common vocabulary for use within the various biometric standards projects. For SC 37, this was a pressing concern as the industry it serves is rapidly evolving with little established agreement on concepts, terms, and definitions.

ISO/IEC 2382 is a multipart standard containing vocabulary developed in various ISO/IEC JTC 1 Subcommittees. The first edition of the SC 37 vocabulary for biometrics [2] has been published as ISO/IEC 2382 Part 37 and contains 121 harmonized terms. WG1 has always been cognizant that the industry has terms and definitions that are well-established in the technical and commercial literature and, consequently, must be respected. Additionally, most words have common meanings broader than the more narrow definitions applied when those words are used as “terms” as understood in [1]. Those common meanings, as found in general dictionaries, should also be respected when possible.

For these reasons, WG1 established some guidelines for its activity. These are:

1. To adhere to the ISO vocabulary development process documented in existing standards
2. To honor to the greatest extent possible current terms and usages within the biometric and broader scientific communities
3. To respect dictionary definitions whenever possible, using the Oxford English Dictionary [6] as a baseline
4. To recognize that terms will be translated into a wide range of languages and therefore must be developed in a context of cultural sensitivity

Further information on the process and philosophy adopted by WG1 has been documented in [7]. The current biometric literature contains a variety of definitions for any single biometric term, as well as a variety of terms for seemingly the same concept. The reasons for this diversity include:

- Terms being developed that have to cover a range of different types of biometric

technologies (e.g., some biometric modes use images; others use signals and the established scientific terminology used for processing each differ).

- The development of new applications and new concepts as the field evolves has led to disjointed attempts to use existing terms to express the new ideas.
- Terms are being applied to provide a technical description, and the same terms are also being used in a contractual context where the implications may vary.
- The biometric industry is truly global and some English terms in usage do not have exact translations into different languages. For this reason, some new terms have been introduced to the industry by WG1 (e.g., biometric probe) rather than using an established term which would have no clear translation.

As an example, consider the following definitions in common usage in the literature:

- **Template/reference template:** Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples
- **Template [8]:** A user's stored reference measure based on biometric feature(s) extracted from biometric sample(s)
- **Template [9]:** A synthesis of the relevant characteristics extracted from the source
- **Reference template:** Also referred to as simply a template, the data in a biometric security system that represents the biometric measurement of a specific person's identity
- **Template:** A mathematical representation of biometric data

While each of these definitions appears to refer to the same concept, different characteristics are introduced into the definitions:

- Data in a biometric security system
- Data used by a biometric system
- Mathematical representation
- Represents the biometric measurement of a specific person's identity
- Used for comparison against subsequently submitted biometric samples
- Stored

In addition, two different terms are presented (reference template and template) for the same concept. Many such examples permeate biometric literature:

- **Biometric feature [8]:** A representation from a biometric sample extracted by the extraction system
- **Biometric data:** The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data)
- **Feature extraction:** The automated process of locating and encoding distinctive characteristics from a biometric sample to generate a template

These definitions are further complicated by uncertainty in the literature around such terms as biometric data or biometric feature that underpin most definitions. It is easy to see how such diversity in designations and definitions for a single concept can compromise effective communication.

To resolve this, in creating [2], WG1 collected terms and definitions from a variety of sources and harmonized them from the concept level according to the guidelines in the ISO standards. For example, [2] gives the following for "biometric template."

- **Biometric template:** Set of stored biometric features comparable directly to probe biometric features.
- **Note 1:** A biometric reference consisting of an image or other captured biometric sample in its original; enhanced or compressed form is not a biometric template.
- **Note 2:** The biometric features are not considered to be a biometric template unless they are stored for reference.

The new biometric terminology standard [2] further defines:

- **Biometric feature:** Numbers or labels extracted from biometric samples and used for comparison.
- **Note 1:** Biometric features are the output of a completed biometric feature extraction.
- **Note 2:** The use of this term should be consistent with its use by the pattern recognition and mathematical communities.

- Note 3: A biometric feature set can also be considered a processed biometric sample.
- Note 4: Biometric features may be extracted from an intermediate biometric sample.
- Note 5: Filters applied to biometric samples are not themselves biometric features; however, the output of the filter applied to these samples may be. Therefore, for example, eigenfaces are not biometric features.

Even with the publication of [2], WG1 continues to consider new terms as captured in ISO/IEC JTC 1 SC 37 Standing Document 2. Since terminology development is an iterative process, existing concepts will continue to be refined as relationships among concepts are explored and new concepts are introduced.

Given that ISO/IEC JTC 1 SC 37 is an international organization, the members of WG1 represent several countries including Canada, France, Germany, Japan, Malaysia, Singapore, Spain, South Africa, the Russian Federation, and the United Kingdom. As a result, the translatability of terms and definitions into various languages is considered throughout the harmonization process. The currently published standard [2] only has terms in English, but this body of text has been the subject of several translation efforts during its progression, and some of these are available for future development, e.g., a German and French translation is listed [10].

Acronyms

JTC	Joint Technical Committee
IEC	International Electrotechnical Commission
ISO	International Standards Organization
SC	Subcommittee
WG	Working group

Related Entries

- ▶ [Biometric Data Interchange Format, Standardization](#)
- ▶ [Biometric Sample Quality, Standardization](#)
- ▶ [Biometric Technical Interface, Standardization](#)

- ▶ [Biometric Security Standards](#)
- ▶ [Performance Testing Methodology Standardization](#)

References

1. ISO/TC37/SC1, ISO 1087-1:2000, Terminology work – Vocabulary – Part 1: Theory and application
2. ISO/IEC JTC 1/SC 37, ISO/IEC 2382-37:2012, Information Technology – Vocabulary – Part 37: Biometrics
3. ISO/TC37/SC1, ISO 704:2009, Terminology work – Principles and methods
4. ISO/TC37/SC1, ISO 860:2007, Terminology work – Harmonization of concepts and terms
5. ISO/TC37/SC2, ISO 10241-1:2011, Terminological entries in standards – Part 1: general requirements and examples of presentation
6. Concise Oxford English Dictionary, Thumb Index Edition, 10th edn. revised, 2002
7. J. Wayman, R. McIver, P. Waggett, S. Clarke, M. Mizoguchi, C. Busch, N. Delvaux, A. Zudenkov, Vocabulary harmonization for biometrics: the development of ISO/IEC 2382 Part 37. *IET Biometrics* 2(3), 1–8 (2013)
8. Common Criteria Biometric Evaluation Methodology, v1.0, http://www.cesg.gov.uk/publications/Documents/bem_10.pdf. Accessed 21 Aug 2013
9. Wikipedia, <http://en.wikipedia.org/wiki/Biometrics>. Accessed 21 Aug 2013
10. German translation of SD2, <http://www.3dface.org/media/vocabulary.html>. Accessed 21 Aug 2013

Biometric Vulnerabilities, Overview

Andy Adler¹ and Stephanie A.C. Schuckers²

¹Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada

²Clarkson University, Potsdam, NY, USA

Definition

Biometric systems, like all security systems, have vulnerabilities. This entry provides a survey of the many possible points of attack against traditional biometric systems. The vulnerabilities of nontraditional systems, such as those based on encoded biometrics, are

surveyed in the article ► [Security and Liveness, Overview](#). Here, biometric system security is defined by its absence: a vulnerability in biometric security results in incorrect recognition or failure to correctly recognize individuals. This definition includes methods to falsely accept an individual (spoofing), to decrease overall system performance (denial of service), or to attack another system via leaked data (identity theft). In this entry, each stage of biometric processing is analyzed and the potential vulnerabilities discussed. Techniques to structure the analysis of vulnerabilities, such as *Attack Trees*, are described, and four application scenarios and their vulnerabilities are considered.

Introduction

This entry surveys the many types of security vulnerabilities in traditional biometric systems. For a more general survey of security issues in biometric systems, including those for novel and encrypted biometric schemes, see ► [Security and Liveness, Overview](#). Biometric system vulnerabilities are defined as avenues of attack against a biometric system that involve an active attacker. The resistance of a biometric system to zero-effort attack is the system false acceptance rate (FAR), and this value is generally considered to be the *performance* of the biometric system. Since there are many configurations for biometric systems and many possible ways to attack each, the topic of biometric system vulnerabilities is necessarily very broad; this entry describes classes of biometric applications and reviews the vulnerabilities of each.

Note that this entry concentrates on system vulnerabilities which are part of the biometric processing itself. Since biometric systems are implemented on server computers, they are vulnerable to all cryptographic, virus, and other attacks which plague modern computer systems [5]; we point out these issues, but do not cover them in detail.

Biometric Subsystems and Vulnerabilities

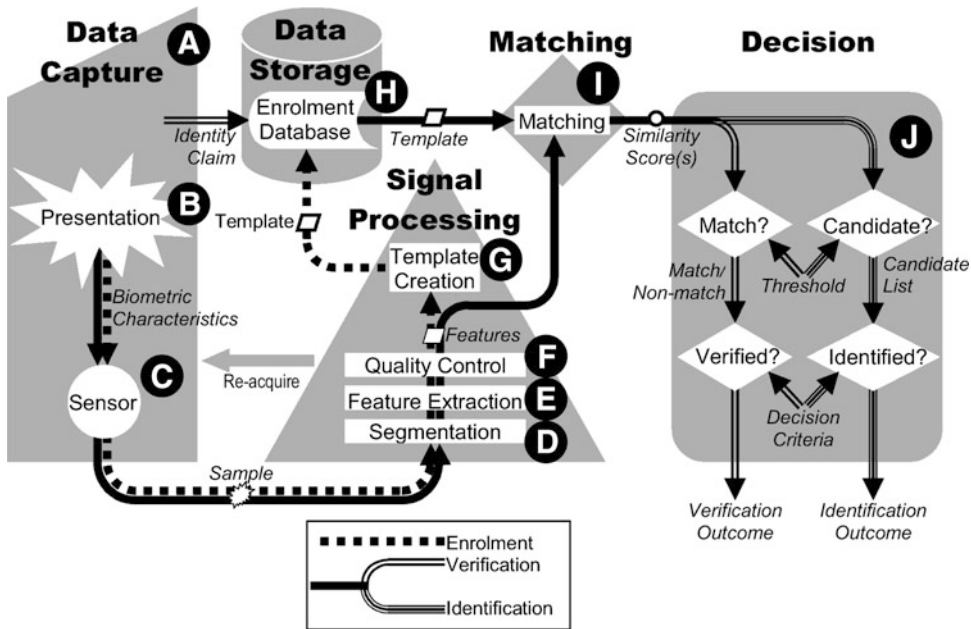
In order to classify biometric security vulnerabilities, it is typical to study each subsystem and interconnection in a system diagram (Fig. 1). Early work is presented in [15], with later contributions coming from [3, 21, 22]. We consider each system module in turn.

Identity Claim (A)

Identity claims are not biometric properties, but form an essential part of most biometric security systems. Exceptions are possible: an example is verifying a season ticket holder; the person's identity does not matter, as long as they have paid. Identity claims are primarily based on links to government-issued identity documents and are thus vulnerable to all forms of fraud of such documents. This is a problem even for highly secure documents, such as passports, which are often issued on the basis of less secure "breeder documents" [17] such as birth certificates issued by local government, hospital, or even religious authorities.

Presentation (B)

An attack on the biometric sensor provides a false biometric sample into the system. Such attacks are designed to either avoid detection (false negative) or masquerade as another (false positive). The latter attack is typically called spoofing, but spoofing can also be used more generally to mean both cases. Clearly, avoiding detection is easier than masquerading, since features simply need to be changed enough to confuse the segmentation or feature extraction module. Changing makeup, facial hair, and glasses or abrading or wetting fingers is often successful, although recent progress in biometric algorithms has reduced the effectiveness of such techniques. There have been reported examples of altering fingerprints including cuts, destruction, or surgical replacement of the fingerprint [23]. Knowledge of the details of algorithms can make such attacks easier; for example, rotating the head will confuse some iris recognition algorithms that do not expect image rotation of more than a few degrees.



Biometric Vulnerabilities, Overview, Fig. 1 Biometric system block diagram (from [8]). Steps A–H are analyzed in detail in this entry. Each presented sample (B) is acquired by a sensor (C) processed via segmentation (D) and feature extraction (E) algorithms. If available, a sample quality (F) assessment algorithm is used to indicate a need to reacquire the sample. Biometric features are encoded into a template, which is stored (H) in a database, on an identity card, or in secure hardware. For biometric

encryption systems, a code or token is combined with the biometric features in the template. During enrollment, biometric samples are linked to a claimed identity (A), and during subsequent verification or identification, samples are tested against enrolled samples, using a matching algorithm (I), and an identity decision (J) is made, either automatically or by a human agent reviewing biometric system outputs

An artificial biometric which copies that of an authorized user is called a “spoof.” The most well-known artificial biometrics or “spoofs” are for fingerprint, through relatively simple techniques using casts of a finger with molds made of household materials [13, 20]. A morbid concern is the use of dismembered fingers, which can be scanned and verified against enrolled fingers. Other modalities may be spoofed: face using pictures or high-resolution video, iris with contact lenses, and voice recordings for voice biometrics [20]. Techniques to make spoofing more difficult include *liveness*, layered biometrics, and use of biometrics in combination with a challenge response, passwords, tokens, or smart cards. The goal of liveness detection is to determine if the biometric being captured is an actual measurement from a live person who is present at the time of capture [12]. Liveness detection is a subset of presentation attack detection methods, broader

category which also includes altered biometric detection and methods to detect spoofing which do not necessarily rely on liveness of the individual. Standards are under development by the International Standards Organization under the Subcommittee on Biometrics [9]. Typically, liveness is a secondary measure after biometric authentication which must be met in order to achieve a positive response. Liveness detection examples may include specialized hardware such as pulse oximetry based or software such as measuring texture information in the fingerprint [19].

Sensor (C)

Attacks on the biometric sensor include any technique which subverts or replaces the sensor hardware. In some cases subverting the sensor allows complete bypassing of the biometric system. For example, in some biometric door locks, the sensor module includes the entire biometric system

including a Wiegand output or relay output to activate the solenoid in a door lock. Subverting such a system may be as simple as physically bypassing the biometric system.

In many cases, an attack on the sensor would take the form of a replay. The connection between the biometric sensor and the biometric system is subverted to allow input of arbitrary signals, and images from legitimate users are input into the system. In order to obtain the signals, several strategies may be employed. Eavesdropping requires accessing the wiring of the sensor. For biometrics using contactless smart cards such eavesdropping becomes more feasible (see [2]). Another approach is to record signals from a sensor under the control of the attacker. Protection typically requires cryptographic techniques to prevent capture and relay of signals and replacement of the sensor [5]. This imposes a larger cost for sensors with integrated cryptographic capability and for management of the security and key infrastructure.

Segmentation (D)

Biometric segmentation extracts the image or signal of interest from the background, and a failure to segment means the system does not detect the presence of the appropriate biometric feature. Segmentation attacks may be used to escape surveillance or to generate a denial of service (DoS) attack. For example, consider a surveillance system in which the face detection algorithm assumes faces have two eyes. By covering an eye, a person is not detected in the biometric system. Another example would be where parts of a fingerprint core are damaged to cause a particular algorithm to mislocate the core. Since the damaged area is small, it would not arouse the suspicion of an agent reviewing the images.

Feature Extraction (E)

Attacks of the feature extraction module can be used either to escape detection or to create impostors. The first category raises issues similar to those in segmentation. Knowledge of the feature extraction algorithms can be used to design

special features in presented biometric samples to cause incorrect features to be calculated.

Characterizing feature extraction algorithms: In order to implement such an attack, it is necessary to discover the characteristics of the feature extraction algorithm. Are facial hair or glasses excluded (face recognition)? How are the eyelid/eyelash regions detected and cropped (iris recognition)? Most current high-performing biometric recognition algorithms are proprietary, but are often based on published scientific literature, which may provide such information. Another approach is to obtain copies of the biometric software and conduct off-line experiments. Biometric algorithms are likely susceptible to reverse engineering techniques.

Biometric “zoo”: There is great variability between individuals in terms of the accuracy and reliability of their calculated biometric features. Doddington et al. developed a taxonomy for different user classes [4]. *Sheep* are the dominant type, and biometric systems perform well for them. *Goats* are difficult to recognize. They adversely affect system performance, accounting for a significant fraction of the FRR. *Lambs* are easy to imitate – a randomly chosen individual is likely to be identified as a lamb. They account for a significant fraction of the FAR. *Wolves* are more likely to be identified as other individuals and account for a large fraction of the FAR. The existence of lambs and wolves represents a vulnerability to biometric systems. If wolves can be identified, they may be recruited to defeat systems; similarly, if lambs can be identified in the legitimate user population, either through correlation or via directly observable characteristics, they may be targets of attacks.

Quality Control (F)

Evaluation of biometric sample quality is important to ensure low biometric error rates. Most systems, especially during enrollment, verify the quality of input images. Biometric quality assessment is an active area of research, and current approaches are almost exclusively algorithm specific. If the details of the quality assessment module can be measured (either through trial and error

or through off-line analysis), it may be possible to create specific image features which force classification in either category. Quality assessment algorithms often look for high-frequency noise content in images as evidence of poor quality, while line structures in images indicate higher quality. Attacks on the quality control algorithm are of two types: classifying a good image as poor and classifying a low-quality image as good. In the former case, the goal of the attack would be to evade detection, since poor images will not be used for matching. In the latter case, low-quality images will be enrolled. Such images may force internal match thresholds to be lowered (either for that image or, in some cases, globally). Such a scenario will create “lambs” in the database and increase system FAR.

Template Creation (G)

Biometric features are encoded into a template, a (proprietary or standards-conforming) compact digital representation of the essential features of the sample image. It has been claimed that, since template creation is a one-way function, it is impossible or infeasible to regenerate the image from the templates [6]; however it has been shown that it is generally possible to regenerate versions of biometric sample images from templates [10]. These regenerated images may be used to masquerade at the sensor or to generate a spoofed biometric for presentation (see ► [Template Security](#)).

Interoperability: Government applications of biometrics need to be concerned with interoperability. Biometric samples enrolled on one system must be usable on other vendor systems if a government is to allow cross-jurisdictional use and to avoid vendor lock-in. However, studies of biometric interoperability have revealed it to be difficult, even when all vendors conform to standards. Tests of the International Labour Organization seafarer’s ID card [1] showed incompatibilities with the use of the minutiae type “other” and incompatible ways to quantize minutiae angles. Such interoperability difficulties present biometric system vulnerabilities, which could be used to increase FRR or for a DoS attack.

Data Storage (H)

Enrolled biometric templates are stored for future verification or identification. Vulnerabilities of template storage concern modifying the storage (adding, modifying, or removing templates), copying template data for secondary uses (identity theft or directly inputting the template information at another stage of the system to achieve authentication), or modifying the identity to which the biometric is assigned.

Storage may take many forms, including databases (local or distributed), on ID documents (into a smart card [2] or 2D barcode [1]) or on electronic devices (a hardened token [7], laptop, mobile telephone, or door access module). Template data may be in plaintext, encrypted, or digitally signed. In many government applications, it may be necessary to provide public information on the template format and encryption used, in order to reassure citizens about the nature of the data stored on their ID cards, but this may also increase the possibility of identity theft. Vulnerabilities of template storage are primarily those of the underlying computer infrastructure and are not dealt with in detail here.

Template transmission: The transmission medium between the template storage and matcher is similarly vulnerable to the template storage. In many cases, attacks against template data transmission may be easier than against the template storage. This is especially the case for passive eavesdropping and recording of data in transit for wireless transmission (such as contactless ID cards). Encrypted transmission is essential, but may still be vulnerable to key discovery [2].

Matching (I)

A biometric matcher calculates a similarity score related to the likelihood that two biometric samples are from the same individual. Attacks against the matcher are somewhat obscure, but may be possible in certain cases. For biometric fusion systems extreme scores in one biometric modality may override the inputs from other modalities. Biometric matchers which are based on Fisher discriminant strategies calculate global thresholds based on the between class covariance,

which may be modified by enrolling specifically crafted biometric samples.

Decision (J)

Biometric decisions are often reviewed by a human operator (such as for most government applications). Such operators are well known to be susceptible to fatigue and boredom. One of the goals of DoS attacks can be to force operators to abandon a biometric system or to mistrust its output (by causing it to produce a sufficiently large number of errors) [5].

Attack Trees

Complex systems are exposed to multiple possible vulnerabilities, and the ability to exploit a given vulnerability is dependent on a chain of requirements. Vulnerabilities vary in severity and may be protected against by various countermeasures, such as supervision of enrollment or verification, liveness detection, template anonymization, cryptographic storage and transport, and traditional network security measures. Countermeasures vary in maturity, cost, and cost-effectiveness. In order to analyze such a complex scenario, the factors may be organized into *attack trees*. This analysis methodology was developed by Schneier [18] and formalized by Moore et al. [14]. In [18], the example attack “Open Safe” is analyzed to occur due to “Pick Lock,” “Learn Combo,” “Cut Open Safe,” or “Install Improperly.” “Learn Combo” may, in turn, occur due to

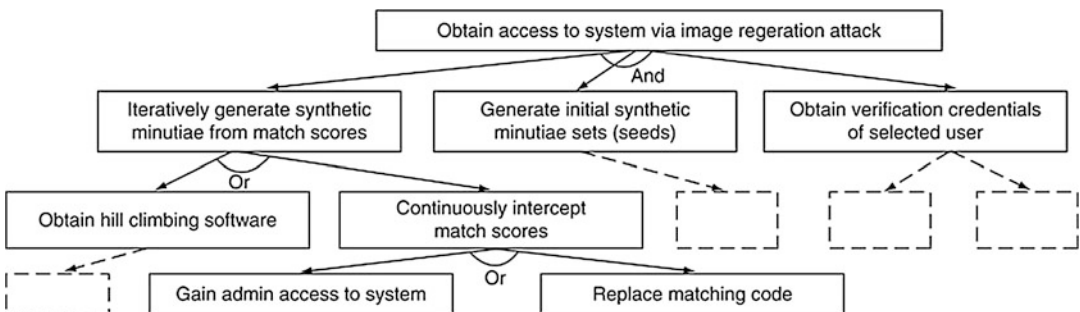
“Eavesdrop,” “Bribe,” or other reasons, which in turn depend on further factors. The requirements for each factor can be assessed (eavesdropping requires a technical skill, while bribing requires an amount of money). Attack trees may be analyzed by assigning each node with a feasibility, the requirement for special equipment, or cost.

Attack tree techniques for biometric system security have been developed by Cukic and Barlow [3]. Figure 2 shows a fraction of the attack tree of [3] for image regeneration from templates [22].

Application Profiles and Vulnerabilities

This entry reviews a large list of possible vulnerabilities in biometric security systems. Such a large list can perhaps give the impression that biometric systems are extremely insecure. In this context, it is important to clarify that many potential vulnerabilities are not a concern in many biometric applications. For example, in a particular application, if security is one of the primary reasons for choosing a biometric (over, say, convenience), it is also important to look at the context of the security mechanism it is replacing. One could certainly argue that biometrically enabled passports (even with weaknesses as discussed below) have improved security in this application over conventional passports.

In order to clarify the security requirements of various biometric implementations, four dif-



Biometric Vulnerabilities, Overview, Fig. 2 Attack tree fraction adapted from [3] (dotted blocks represent removed tree portions) to implement the template regener-

ation attack of [22]. AND/OR nodes indicate that *all/one* of the subblocks are/is required

ferent biometric application scenarios are considered: government ID cards, physical access, computer and network access, and digital content protection.

Government Identity Cards

Perhaps the most widely discussed applications for biometrics are for government identity cards. For example, the ICAO machine-readable passport standards require biometric data in passports. Passports have an embedded contactless smart card, into which face recognition (mandatory) and fingerprint or iris (optional) biometric templates are stored encrypted in a standardized format.

In order to allow data interchange, the encryption key is based on information available in machine-readable zone. For example, it was possible to contactlessly read the UK passports [2]. This raises the concern that biometric and biographical data may be surreptitiously copied and used for identity theft. Biometric-enabled passports have been strongly criticized by privacy advocates (e.g., [16]). Given the privacy concerns associated with a large government database, several authors have questioned whether the additional security is worth it [17].

Government ID applications of biometrics are characterized by the following requirements and concerns:

- *Interoperability and standards compliance:* Interoperability is difficult to achieve for complex systems such as biometrics (e.g., [1]); systems which do not interoperate well give poor performance and are vulnerable to attacks such as denial of service.
- *Cryptographic compatibility:* In order to allow interchange of encrypted documents, public key cryptographic systems are required, in which the public keys are made available to receiving governments. Considering the wide distribution of keys, it must be assumed that the public keys will be fairly easily available to attackers.
- *Large databases of vulnerable data:* Identity document data is typically stored in large centralized databases; however, these become vulnerable and high-value targets for attack.

Several high-profile cases of compromise of government databases have occurred.

- *Secondary use of government IDs:* Government identity cards often have secondary uses; for example, driver's licenses are used to prove name, age, and even citizenship. This means that biometric documents designed for a narrow range of security concerns may be used in very different threat environments, with inadvertent side effects.
- *Typically supervised use:* For most applications of government biometric identity, the point of application will be supervised (e.g., immigration control). This makes spoofing more difficult for these applications.

Physical Access

Physical access systems for biometrics are typically for government and industrial applications. In "time and attendance systems," biometrics measure arrival and departure times of staff. In physical access security systems, secure spaces are controlled by biometric sensors. These spaces may be an entire site or restricted parts of a worksite.

Physical access applications are characterized by the following requirements and concerns:

- *Concern about privacy:* Staff are often concerned that biometric records will be controlled by the employer and may be provided to police. It is important to address this concern both technically and by clear communication with staff.
- *Unsupervised sensors:* Physical access sensors are typically unsupervised. This means that there is a potential vulnerability to spoofing and other attacks at the presentation and sensor.
- *Workarounds:* It is well known that busy staff see security as a burden to work around. Biometrics have the advantage that staff often see it as more convenient than keys or identity cards, encouraging compliance. However, if the system is implemented in a cumbersome way, there is an incentive to work around burdensome infrastructure, by propping open doors, sharing keys, and manual overrides.

Computer and Network Access

A biometric system can facilitate secure access to computer systems and networks; this is an important requirement in government, health care, and banking applications, as well as many others. Biometric sensors are currently delivered with some laptop computers and mobile telephones. These applications are characterized by the following requirements and concerns:

- *Assurance levels*: The biometric system security needs to be matched to the security level (or assurance level) of the overall system. An excellent review of the security of biometric authentication systems is [7]. Each assurance level from “passwords and PINs” to “hard crypto token” is analyzed to determine whether (and which type of) biometric devices are suitable.
- *Network attacks*: Biometric systems for network access are vulnerable to many of the attacks which can be mounted across a computer network. Examples are relay of issued credentials, and virus and other security compromises of the desktop computers (to which biometrics are often attached). Security must therefore include computer security and cryptographic protection of biometric data and security tokens.
- *Password caching*: Many biometric software solutions do not actually replace passwords, but simply keep a cache of security keys. A valid biometric sample will make the software search for the appropriate key to unlock the application. However, this means that cracking the software will release both the security keys and the biometric template of the user.

Digital Content Protection

Biometrics have been considered as a way to protect copyright content, such as music and videos. In such a scenario, the content is encrypted and bound to the biometric of the purchaser [11]. It may be assumed that biometrically locked digital documents will be subject to attacks, especially since both the documents and the software to access them will be widely distributed [11]. These applications are characterized by the following concerns:

- *Incentive to crack systems*: Digital content protection systems are under the control of a (often hostile) user population which creates an incentive to crack the security systems. Additionally, any such security breaches tend to be published on the Internet resulting in wide-scale use and potential poor publicity for the content providers.
- *Privacy and identity theft concerns*: Locking of digital content with biometrics tends to create concerns about privacy among users, since breaches of the security can potentially compromise the biometric security for large numbers of users.

Summary

This entry provides a broad overview of vulnerabilities in biometric systems. Vulnerabilities are defined in terms of possible active attacks against biometric systems. A model of biometric processing [8] is considered in detail, and the potential vulnerabilities at each stage of processing are considered: identity claim, presentation, sensor, segmentation, feature extraction, quality control, template creation, data storage, matching, and decision. In order to understand the vulnerabilities of a large biometric system, attack tree methods are explained. Finally, four example scenarios are given for biometric applications; the vulnerabilities are considered: government identity cards, physical access, computer and network access, and digital content protection. However, in addition to the vulnerabilities specific to the biometric technology, it is important to note that the vulnerabilities of any networked computer security system continue to be a concern; specifically, such systems are vulnerable to *social engineering* and all the security issues which plague modern computer networks. Finally, biometric vulnerabilities must be compared to those of the systems they are designed to replace. In many cases, the biometric system, with the vulnerabilities considered in this entry, will still be dramatically more secure than identity cards, passwords, or other tokens. Additionally combinations of biometrics with traditional methods (e.g., biometric and pin)

may provide additional security as each may have different vulnerabilities.

Related Entries

- ▶ [Biometric System Design, Overview](#)
- ▶ [Cancelable Biometrics](#)
- ▶ [Encryption, Biometric](#)
- ▶ [Fraud Reduction, Overview](#)
- ▶ [Security Issues, System Design](#)

References

1. Biometric testing campaign report (addendum to part i), Technical report, International Labour Organization, Geneva, 2005, <http://www.ilo.org/public/english/dialogue/sector/papers/maritime/sid-test-report2.pdf>
2. Cracked it! *The Guardian*, 17 Nov 2006, <http://www.guardian.co.uk/idcards/story/0,,1950229,00.html>
3. B. Cukic, N. Barlow, Threats and countermeasures, in *Biometrics Consortium Conference*, Washington, DC, 2005
4. G. Doddington, W. Liggett, A. Martin, N. Przybocki, D. Reynolds, Sheep, goats, lambs and wolves: an analysis of individual differences in speaker recognition performance, in *Proceedings of the International Conference on Auditory-Visual Speech Processing*, Sydney, 1998
5. N. Ferguson, B. Schneier, *Practical Cryptography* (Wiley, New York, 2003)
6. Generating images from templates, Technical report, 2002, http://www.ibgweb.com/reports/public/reports/templates_images.html
7. InterNational Committee for Information Technology Standards (INCITS), Study report on biometrics in e-authentication, technical report incits m1/06-0693. Technical report, 2006, http://www.incits.org/tc_home/m1htm/2006docs/m1060693.pdf
8. ISO, Standing document 2, version 5 – harmonized biometric vocabulary. Technical report, 2006. Technical report ISO/IEC JTC 1/SC 37 N 1480
9. ISO/IEC Working Draft 30107, *Information Technology – Anti-Spoofing and Liveness Detection*, ISO/IEC JTC 1/SC 37 Biometrics
10. A.K. Jain, A. Nagar, K. Nandakumar, Biometric template security. *EURASIP J. Adv. Signal Process.* Article ID 579416, 17p (2008)
11. D. Kundur, C.-Y. Lin, B. Macq, H. Yu, Special issue on enabling security technologies for digital rights management, in *Proceedings of the IEEE Conference*, vol. 92, 2004, pp. 879–882
12. Liveness detection in biometric systems, Technical report, 2002, <http://www.ibgweb.com/reports/public/reports/liveness.html>
13. T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, Impact of artificial “gummy” fingers on fingerprint systems, *Proceedings of SPIE*, vol. 4677 (2002)
14. A.P. Moore, R.J. Ellison, R.C. Linger, Attack modeling for information security and survivability. Technical report, Carnegie Mellon University, Pittsburgh, 2001
15. N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **40**, 614–634 (2001)
16. P.E. Ross, Loser: passport to nowhere. *IEEE Spectr.* **42**, 54–55 (2005)
17. M.B. Salter, Passports, mobility, and security: how smart can the border be? *Int. Stud. Perspect.* **5**, 71–91 (2004)
18. B. Schneier, Attack trees. *Dr. Dobbs’s J.* **24**, 21 (1999)
19. B. Tan, S. Schuckers, Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. *Pattern Recognit.* **43**(8), 2845–2857 (2010)
20. L. Thalheim, J. Krissler, Body check: Biometric access protection devices and their programs put to the test. *c’t Mag.* (2002). www.heise.de/ct/english/02/11/114/
21. C. Tilton, Biometrics in e-authentication: threat model, in *Biometrics Consortium Conference*, Baltimore, 2006, http://www.biometrics.org/bc2006/presentations/Wed_Sep_20/Session_III/Biometrics_and_EAuth/20_Tilton_e-auth_threat.pdf
22. U. Uludag, A.K. Jain, Attacks on biometric systems: a case study in fingerprints, in *Proceedings of SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI*, San Jose, 2004, pp. 622–633
23. S. Yoon, J. Feng, A.K. Jain, Altered fingerprints: analysis and detection. *IEEE Trans. Pattern Anal. Mach. Intell.* **34**(3), 451–464 (2012)

Biometric Zoo Menagerie

Kevin O’Connor¹ and Stephen John Elliott²

¹Purdue University, West Lafayette, IN, USA

²International Center for Biometric Research, Purdue University, West Lafayette, IN, USA

Synonyms

Zoo Menagerie; Biometric Zoo Effect

Definition

The biometric zoo menagerie was developed to address the impact of individuals on performance

of a biometric system, although Tabassi [1] concentrated on the image as opposed to the individual. There are three main types of zoo classifications:

Doddington's Zoo Menagerie Terms

Goats are defined as below the 2.5 percentile of average match score. Wolves have match scores above the 97.5 percentile. Lambs are individuals who are particularly easy to imitate and have characteristics similar to others in the dataset. These animals generate scores similar to everyone that could lead to false accepts. Sheep are individuals who have high genuine scores and low impostor scores, giving low false match rates and low false accepts. Wolves are successful at imitating other speakers and receive high match scores and provide high false accepts [2].

Dunstone and Yager's Zoo Menagerie Terms

Doves, the best performing individuals, are in both the top 25% of the genuine distribution and the bottom 25% of the impostor distribution. Chameleons are in the top 25% of the genuine distribution and the top 25% of the impostor distribution. This means they look similar to others in the dataset as well as themselves. Phantoms are in the bottom 25% of the genuine and impostor distributions. These individuals are not easy to match against anyone in the dataset, including themselves. Worms, which are the worst performing classification, are in the bottom 25% of the genuine matches and the top 25% of the impostor matches, indicating they do not look like themselves but look like others [3].

Tabassi's Zoo Menagerie Terms

For clear ice, the image false non-match rate is less than the minimal false match rate. These images are in the lower left quadrant of the plots, similar to the zoo animal phantom. Black ice images, similar to the chameleons, are in the upper right portion of the plots, due to their higher matching ability to others as well as themselves. Blue goats are images that are in the top left quadrant that have an image false non-match rate greater than the nominal false non-match rate. Blue wolves are images that are in the bottom

right of the plots due to their ability to produce higher false matches and capability to be easily identified [4].

Introduction

This entry will expand on the different types of biometric menagerie classifications of performance that have been discussed in the literature. In the biometric literature [5–7], there are four main methods of displaying and discussing performance. These typically are centered on the trade-offs of the false match rates (FMR) and false non-match rates (FNMR) and the false accept rates (FAR) and false reject rates (FRR) that are graphically displayed on score histograms, receiver operating characteristic (ROC) curves, and detection error trade-off (DET) curves. The zoo menagerie was popularized by Doddington, Liggett, Martin, Przybocki, and Reynolds [2], who coined the following animals: sheep, wolves, lambs, and goats. Others have suggested alternatives such as Yager and Dunstone [3], who characterized the relationship between genuine and impostors – chameleons, worms, doves, and phantoms. Tabassi [1] proposed different metrics based on the image as opposed to the subject – blue wolves, clear ice, blue goats, and black ice.

Discussion

The work by Doddington et al. has served as a foundation for later literature that examined individual performance in the biometric menagerie [2]. This work was a meta-analysis as it used tests from a 1998 speaker evaluation test to determine the matching relationships between individuals when assessing performance. The paper examined how recognizable different speakers were depending on the behavior of one another. In doing so, they created a biometric menagerie that highlighted a way to categorize an individual's ability to perform. This zoo menagerie classified the individuals in order to provide a deeper understanding of the likelihood of false accepts and false rejects. The four classifications in the "Doddington's zoo" are goats, sheep, lambs, and

wolves. Goats are individuals who are particularly difficult to match. These are defined as below the 2.5 percentile of average score. Wolves have match scores above the 97.5 percentile. Lambs are individuals who are particularly easy to imitate and have characteristics similar to others in the dataset. These animals generate scores similar to everyone that could lead to false accepts. Sheep are individuals who have high genuine scores and low impostor scores, giving low false match rates and low false accepts. Wolves are successful at imitating other speakers and receive high match scores and provide high false accepts [2].

Yager and Dunstone built on the concepts associated with Doddington. In their work, they posed the following research questions: what is the relationship between a user's genuine and impostor match scores? Does this relationship exist across different biometric modalities such as fingerprint, iris, etc.? Is there a possibility of exposing weaknesses in the biometric algorithms (i.e., comparing one algorithm with another) to see their different match rates [3]? Yager and Dunstone created four new classifications of animal. Doves, the best performing individuals, are in both the top 25% of the genuine distribution and the bottom 25% of the impostor distribution. Chameleons are in the top 25% of the genuine distribution and the top 25% of the impostor distribution, meaning they look similar to others in the dataset as well as to themselves. Phantoms are in the bottom 25% of the genuine and impostor distributions. While these individuals are not easy to match against anyone in the dataset, they are also not easy to match to themselves. Worms, who are the worst performing classification, are in the bottom 25% of the genuine matches and the top 25% of the impostor matches, indicating they do not look like themselves but look like others [2].

Tabassi [1] examined the performance of a particular image as a metric for further biometric performance analysis. Tabassi suggested a new way of examining biometric images based upon the characteristics of the image rather than the subjects themselves. Tabassi concluded that there was a difference in comparing the correlations

of quality with image error over different algorithms. This could mean that an unknown variable is causing errors other than the image itself or the subject. Additional metrics for measuring these errors were proposed. For clear ice, the image false non-match rate is less than the minimal false match rate. These images are in the lower left quadrant of the plots, similar to the zoo animal phantom. Black ice images, similar to the chameleons, are in the upper right portion of the plots, due to their higher matching ability to others as well as themselves. Blue goats are images that are in the top left quadrant that have an image false non-match rate greater than the nominal false non-match rate. Blue wolves are images that are in the bottom right of the plots due to their ability to produce higher false matches and capability to be easily identified [1].

Many have challenged or proved the existence of the zoo; therefore, a selection of references for review have been included in this entry, for example, Paone, Biswas, Aggarwal, and Flynn [8]; Tabassi [1]; Wittman et al. [9]; and Yager and Dunstone [3]. Wittman et al. indicated that the majority of errors were due to image quality or data collection mistakes, as opposed to the subject [9]. Paone et al. alluded to the impact of covariates, as well as the environment in which the data collected (they separated out covariates and environment) [8]. The zoo methodology has also been tested on a number of different modalities, such as fingerprint, keystroke dynamics, and iris [1, 3], voice [2], and face [8]. Probably the hardest critique of the zoo was from Schuckers, who theorized that the zoo does not need to be considered because the collected data is what has been analyzed [10].

Others have also examined existence tests: Wittman, Davis, and Flynn examined the impact of covariates in face recognition to see the effect of these variables in performance [9]. The underlying reason to do this was to examine whether these covariates – lighting or facial expression – impacted the matching ability of the individual. The authors indicated that covariates may provide some change in classification from one animal to another.

Another paper examined the existence of the zoo. In this paper, several zoo orders were pre-

sented [11]. The zeroth order is the genuine and impostor scores from one modality and one test database. The first order is described as the randomized sampling of genuine and impostor scores within the test database. The second order illustrates covariates, controlled and uncontrolled capture. The third order shows algorithms and covariates, and the fourth order is defined by different modalities. Their analysis followed the same methodologies as Doddington and Dunstone. There were two methods of finding the existence of a biometric zoo. The first was the methodology by Doddington et al. and the second was by Yager and Dunstone. There was strong evidence of the first-order zoo in Doddington animals but not in Dunstone and Yager's menagerie. The majority of cases in the rest of the hierarchy of zoo classifications did not exist.

Summary

Understanding the performance of a biometric system and the impact of an individual in that biometric system is of interest to many. The biometric zoo menageries provide a structure to describe the performance of individuals or specific images.

Related Entries

- ▶ [Biometric Verification/Identification/Authentication/Recognition: The Terminology](#)

References

1. E. Tabassi, Image specific error rate: a biometric performance metric, in *2010 International Conference on Pattern Recognition*, Istanbul, 2010, pp. 1124–1127
2. G. Doddington, A. Liggett, A. Martin, M. Przybocki, D. Reynolds, Sheep, goats, lambs and wolves: a statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation, in *Proceedings of the International Conference on Spoken Language Processing*, Sydney, 1998
3. N. Yager, T. Dunstone, The biometric menagerie. *IEEE Trans. Pattern Anal. Mach. Intell.* **32**(2), 220–30 (2010)
4. P. Phillips, P. Grother, M. Bone, R. Micheals, D. Blackburn, E. Tabassi, Face recognition vendor test 2002, in *IEEE International Workshop on Analysis and Modeling of Faces and Gestures, 2003 (AMFG 2003)*, Nice (DARPA/NIST/DoD/NAVSEA, 2003), p. 278
5. T. Dunstone, N. Yager, *Design, Evaluation, and Data Mining* (Springer, New York, 2008), p. 288
6. ISO/IEC JTC 1/SC 37 Biometrics N908, Geneva, 2005
7. J. Wayman, A generalized biometric identification system model, in *Conference Record of the Thirty-First Asilomar Conference on Signals, Systems and Computers (Cat. No.97CB36136)*, Pacific Grove, vol. 1, 1997, pp. 291–295
8. J. Paone, S. Biswas, G. Aggarwal, P. Flynn, Difficult imaging covariates or difficult subjects? An empirical investigation, in *2011 International Joint Conference on Biometrics (IJCB)*, Washington, DC, Oct 2011, pp. 1–8
9. M. Wittman, P. Davis, P.J. Flynn, Empirical studies of the existence of the biometric menagerie in the FRGC 2.0 color image corpus, in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, New York, 2006, pp. 33–33
10. M.E. Schuckers, *Computational Methods in Biometric Authentication* (Springer, London, 2010), pp. 293–300
11. M. Teli, J. Beveridge, Biometric zoos: theory and experimental evidence, in *International Joint Conference on Biometrics (IJCB)*, Washington, DC, 2011

Biometrics on Mobile Devices

Ramón Blanco-Gonzalo^{1,2} and
Raul Sanchez-Reillo³

¹Departamento de Tecnología Electronica,
University Carlos III of Madrid, Leganes,
Madrid, Spain

²Electrical and Electronic Department,
Universidad Publica de Navarra, Pamplona,
Navarra, Spain

³GUTI (University Group for Identification
Technologies), University Carlos III of Madrid,
Leganes, Madrid, Spain

Synonym

Mobile biometrics

Definition

Biometrics on mobile devices includes the use of any feasible biometric modality in mobile environments, including smartphones, tablets, tablet PCs, laptops, and embedded portable devices. Therefore the aim is to achieve the same biometric functionality than traditional systems, but with the addition of portability. This means that the biometric mobile solutions should present an equivalent level of error rates and throughput, but with some additional constraints such as lower processing power, reduced power consumption, and novel user interfaces for obtaining an acceptable human-device interaction. These constraints lead to a holistic modification of the biometric subsystem, including optimization of the algorithms, consideration of new scenarios and use cases, and the adaptation of biometric sensors. Smartphones are the most widespread mobile devices, and their characteristics are in continuous improvement (CPU, RAM, connectivity, integrated devices, operating system, etc.). Therefore they are the perfect platform for easing the integration of new technologies and procedures, being nowadays the focus of many research works in the field of the application of biometrics.

Introduction

Mobile devices are playing a significant role in daily life, not only for communications but also for entertainment, working activities, or social relationships. Along with the high increase of the use of smartphones and mobile devices in daily life, the amount of sensitive data that these devices store is also increasing (e.g., bank accounts, personal e-mails, photographs, etc.). This situation leads to the need of protecting the access to such sensitive data, and biometrics is offered as an alternative mechanism for such protection [1]. According to the latest improvements in smartphones, the range of possibilities for integrating biometrics is promising, with potential applications such as signing documents univo-

cally, secured access to websites, execution of administration procedures, etc. Furthermore, the use of other traditional authentication schemas based on passwords, is considered by users as cumbersome due to the necessity to remember a large variety of alphanumeric codes, which usually drives users to re-use the same password for several, if not all, services accessed. The use of biometrics allows the user authentication through “something she/he is” or “something she/he does” avoiding the use of “something she/he knows”. Therefore, the possibility to use biometrics to manage and protect sensitive data arouses the interest of users and researchers, furthermore if it is considered a protection mechanism easy to use and secure.

It is important to note some other facts that encourage the work in including biometrics into mobile devices. The first one is the large amount of devices already deployed, which has reached the situation that it is difficult to find someone that does not possess and use daily devices such as smartphones or tablets. The second one is that for some biometric modalities, the capture device is already included within the mobile device (e.g., camera for face recognition, touch screen for handwritten signature recognition, microphone for speaker recognition, or the inclusion of some swipe sensors for fingerprint verification). This leads to an important reduction in the cost of the deployment, as users already have those devices and they should only acquire the application. Other important factors are the necessity of having ID portable devices by security forces (e.g., for suspects identification) or for signing documents on the spot.

Also, as users are already familiar with this kind of devices, the usability level achieved could be improved, although, as it will be mentioned below, mobility also creates new usability challenges. Due to marketing needs, mobile devices are improving every day, which will allow powerful biometric algorithms in the near future.

As an important drawback, mobile devices present security concerns related to how the operating system controls the way that installed applications access memory data and communication buffers. A lack of a strict control compromises the

integration of biometrics as sensitive data may be endangered.

Usability and accessibility problems can appear also. For example, the use of inadequate interfaces or the adaptation to different user disabilities has to be addressed from scratch in order to offer universality: if the technology is not easy to use or hard to understand, users will reject its use. Moreover, not all the biometric modalities fit perfectly in mobile environments or the migration is far from being easy or cheap. For instance, nowadays the smartphone screen does not allow capturing the fingerprint and then an extra sensor is needed. Therefore many research fields are opened.

Background

The idea of integrating biometrics into mobile devices started several years ago, while biometric technology started to acquire an acceptable level of maturity and societal acceptance. For instance, in 2005 there is an example of biometric recognition in a rudimentary mobile phone with iris [2]. In other approaches, various biometric modalities are implemented in mobile devices: palm print, knuckle [3], or fingerprint. Nowadays biometrics is proposed as one of the best solutions to guarantee security within mobile environments. Good examples of it are studies in secure mobile voting [4], mobile banking, and online transactions.

As biometrics was proposed to be used for multiple purposes (e.g., e-commerce, e-government, etc.), some manufacturers started to create prototypes with fingerprint sensors, as a mean to unlock the device in a comfortable way. This situation also led to the approval of several R&D projects.

The SecurePhone European project (IST-2002-506883 active in 2004–2006, <http://www.secure-phone.info>) was focused on this topic. Its main target was to develop a biometric recognition system for mobile phones based on face, voice, and handwritten signature [5]. This project integrated a biometric recognizer in a 3G-enabled PDA, which allowed users to mutually recognize each other and securely

authenticate messages (text or audio). This enabled users to sign legally binding contracts on their PDA/mobile phone.

Two years later, in 2008, the European project Mobio (Mobile Biometry, FP7-214324 <http://www.mobioproject.org/>) started [6]. In this project the incorporation of biometrics (voice and face) on a mobile device was proposed. Furthermore, it was focused on specific aspects such as the remote biometric identification or the computational limitations of the microprocessor. The intention of the project was to develop new mobile services secured by biometric authentication mechanisms. Its objectives included robust-to-illumination face authentication, robust-to-noise speaker authentication, joint bimodal authentication, biometric reference adaptation, and system scalability.

Regarding the integration of biometrics in mobile devices the future is promising: many companies are betting big on it and the technology seems to be accepted by users. According to Goode Intelligence: “*The mobile biometric security market would grow to 39 million users by 2015*” [7]. Attending to this forecast and the quantity of improvement possibilities that experts can overcome, the big amount of research works that exist in this way is justified.

The purchase of the company PittPatt by Google in 2011 and the posterior adaptation to Android is a clear example of the advances in this field, suggesting the facial recognition as a comfortable method for unlocking the smartphone. More recently, Apple bought the company AuthenTec in 2012, showing their clear inclination for the fingerprint authentication. Furthermore they granted a patent for a two-step unlock screen feature that has yet to be implemented.

There are several biometric modalities that fit well in mobile environments, like face recognition, ear shape recognition [8], or handwritten signature recognition [9]. At the same time, along with the migration to mobile environments, new modalities emerged, such as keystroke recognition or recognition by the touch screen input.

Probably the most attractive modality to be applied is fingerprint recognition, but as the inte-

gration of a fingerprint sensor requires industrial product development, some studies have also analyzed the possibility of acquiring fingerprints with the mobile camera. That work is in addition to the obvious use of using the camera for facial recognition [10]. Also, the use of the accelerometer represents a good chance to implement behavioral biometrics too [11]. Furthermore, biometric recognition is being used in conjunction with some other communication protocols in smartphones such as NFC [12]. Authors have made a concept proof enrolling and verifying fingerprints from a specific device connected to a smartphone as it is shown in Fig. 1.

But smartphones are not the only kind of mobile devices that can be used. Mobile devices, when being integrated with biometrics, can be divided in several categories although these three are the main, according to market trends and popularity:

- PDAs (Personal Digital Assistants) are handheld devices that combine elements of computing, telephone, Internet, and networking. Typically, they are designed to be managed with a stylus, which fits perfectly for handwritten signature recognition.
- Smartphones include phone and computer functions in addition to different sensors



Biometrics on Mobile Devices, Fig. 1 Biometric fingerprint obtained with a fingerprint sensor connected to a smartphone

allowing capture image, sound, or positioning. This makes the biometric integration easier.

- Tablet and tablet PCs are a type of notebook computers including sometimes phone functions. The big difference with the smartphones is the screen size that is bigger, providing users with more space to interact with the device. In [13] authors made an evaluation of handwritten signature recognition with an iPad signing with the fingertip and with different styluses (Fig. 2)
- Portable devices proposed by the industry, including handheld terminals specially made for biometric recognition. These devices support common modalities such as fingerprint, face, or iris recognition.

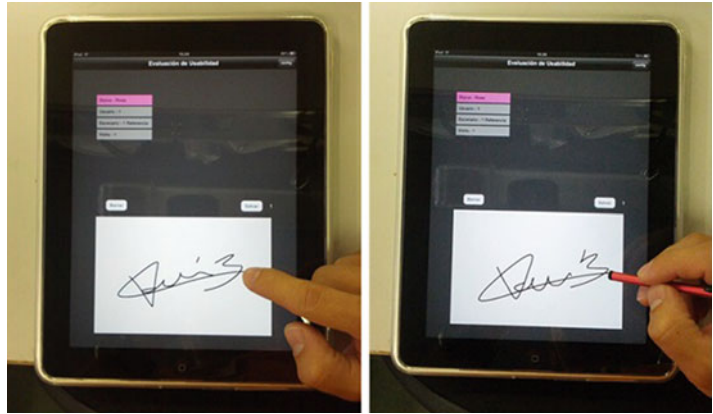
Migration Requirements

The extraordinary advances that portable devices have experienced have converted them in small computers whose host processors are capable of work in the GHz range, with memory capacities larger than 256 MB and a variety of sensors (touch screen, camera, microphone, accelerometer, etc.). These sensors are suitable to capture many of the users' biometric features, but its performance or acquisition variables differ with respect to those obtained with conventional capture devices. For example, cameras included in smartphones work within the visible spectrum, unlike commercial iris capture cameras that operate in the infrared band. On the other hand, capacitive touch screens incorporated in most of the smartphones nowadays do not allow extracting the pressure exerted on the surface. This parameter is used in most of the handwritten signature recognition algorithms. Though, in order to offer reliability, migrating biometrics to mobile environments requires several modifications to address all these new constraints. The transition from PC to mobile devices is not direct or easy to deploy, and it brings new challenges that have to be covered. These new challenges are:

- Adapting the device to acquire the selected biometric modality

Biometrics on Mobile Devices, Fig. 2

Handwritten signature recognition in mobile devices [14]



- Defining the application architecture to better fit the scenario (e.g., local authentication vs. remote authentication)
- Fine-tuning the biometric algorithm for improving performance considering the execution platform and the acquisition properties
- Evaluating the impact on performance of the implementation of the solution in a variety of platforms
- Evaluating the impact on performance of the different ways and situations of using mobile devices, including not only the positioning of the user but also the environmental conditions surrounding (e.g., light, humidity, noise, vibration, etc.)
- Evaluating the usability of the new applications and redesigning them according to the results obtained

Furthermore, accessibility problems using biometrics in mobile devices can arise to some groups of users. On one hand, users with the so-called *fat fingers* problem are sometimes not able to point accurately in a smartphone touch screen. Also users with disabilities such as arthritis or Parkinson's disease can find uncomfortable or impossible to handle a mobile device. Elderly would find some complications also at the time to complete repetitive procedures or understand some steps. Additionally, not all the biometric recognition modalities fit perfectly in mobile environments or work in all the scenarios. For instance, to use hand geometry recognition, the only approach of using a peg-free image with variable background is viable [14] as shown

in Fig. 3. Also gait recognition will not work properly if the device is not in the trousers pocket (most probable in the same pocket, and sometimes even on the same trousers), or voice recognition systems would have problems to work well in spaces where the ambient noise is loud.

Inconveniences

Currently, smartphones can also access data services offered by mobile phone companies, a market that is rapidly expanding due to the growing demand from existing users. Through the data service a user can connect to the Internet and look up information of all kinds (e.g., e-mail, banking operations, etc.). The data security handled by applications is trusted to the operating system (OS) of the portable device.

For instance, in the Android OS, the user is responsible for authorizing the permissions (access to sensors, data, or other applications activities) requested by each application during installation, so that they run in a "Sandbox" that keeps the data (contained in the memory and files) isolated from other applications.

The flexibility that these smartphones offer to users for modifying and/or updating the OS, or the installation of new applications and authorization permissions, allows access to sensitive data via several attacks like rootkits [15], privilege escalation, appPhishing, or appJacking. As a consequence, sensitive data such as biometric references or private keys in a PKI solution are

Biometrics on Mobile Devices, Fig. 3 Hand geometric recognition using a peg-free image [14]



not totally safe within the mobile device, which is a major drawback in this kind of devices.

Another concern that has to be considered is the limitation of the development platforms when accessing biometrics information in client/server architectures, such as through web services. Some technologies, such as Java Applets, ActiveX Controls, JavaScript, or Flash that are essential to capture biometric data in PC platforms, are not fully available in some web browsers installed in mobile devices.

One of the possible solutions to these mobile devices vulnerabilities is the use of other technologies jointly with biometrics. One example is the use of smart cards and biometrics altogether. Unlike mobile devices, the smart card eliminates any possibility of reading and/or modification of the biometric traits as a consequence of the SO vulnerabilities, although does not have the computational power or sensors of the mobile device. Therefore, it can be said that while a correctly implemented smart card is considered a tamper-proof system, a mobile device is far from achieving that status.

In other words, the need of improving security in mobile platforms is pushing forward the development of Trusted Execution Environments (TEE), either by implementing them in software or by using Trusted Platform Modules (TPM) that include Secure Elements (SE), such as smart

cards or other kind of hardware module that will help in the accomplishment of the security requirements.

Next Steps in Mobile Biometrics

The company Validity which develops solutions for mobile biometrics has recently designed a fingerprint sensor for being embedded underneath the smartphone screen. The fingerprint capture is made with a finger swipe, so this avoids having to reserve space in the smartphone housing for another sensor (and simplifies the process: unlock and fingerprint recognition can be made at the same time).

Another step forward in the biometrics mobile field is the agreement between the US Defense Department and the company AOptix to develop a hardware peripheral and a software suite that turns a commercially available smartphone into a device that scans and transmits data from users' eyes, face, thumbs, and voice. The intention is to have the possibility (soldiers, marine, or special operators) to record the biometric information of suspicious people on the spot.

In addition, biometrics is being integrated in mobile devices in order to facilitate everyday tasks (automation, bank transactions, etc.) for people with disabilities.

One of the trending topics in mobile biometrics is the introduction of NFC which permits fast data wireless interchange saving time. Moreover, most of the new mobile devices being manufactured are equipped with this technology, which gained its popularity in Japan, as it started to being used for daily payments.

Summary

The use of biometrics in mobile scenarios is gaining popularity along with the increase of the use of smartphones. At the same time, new biometric modalities and/or improvements of traditional biometrics, arise according to the new possibilities that smartphones bring. The transition of biometrics to mobile environments is being softer according to the several improvements of these devices' characteristics, though for various modalities this migration is still not satisfactory. Care shall be taken when deploying a solution, because limitations appear and they have to be considered during design, development, and deployment. If not, an early deployment may impact negatively the whole biometric sector. It is important to remember that security is a must and that both biometrics have to help user's privacy, but also biometric data shall be protected. If this is not accomplished, privacy directives and data protection laws could limit the deployment of these solutions in several countries.

The main drawback in migrating biometrics to mobile solutions is the vulnerability of the mobile devices to sensitive data attacks, which supposes a big inconvenience to biometric systems deployment. The use of biometrics in mobile devices in conjunction with other approaches to secure data such as smart cards shows to be a viable solution. Therefore, further research is needed for assuring security, reliability, and acceptable performance.

Related Entries

- ▶ [Embedded Systems](#)
- ▶ [On-Card Matching](#)
- ▶ [User Acceptance](#)

References

1. S. Mansfield-Devine, Biometrics for mobile devices struggle to go mainstream. *Biom. Technol. Today* **2011**(9), 10–11 (2011)
2. D. Cho, K. R. Park, D. W. Rhee Real-time iris localization for iris recognition in cellular phone, in *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005. Sixth International Conference on*, vol., no., pp.254,259, 23-25 May 2005
3. K. Cheng, A. Kumar, Contactless finger knuckle identification using smartphones, in *BIOSIG*, Darmstadt, 2012, pp. 1–6
4. D. Gentles, S. Sankaranarayanan, Biometric secured mobile voting, in *Second Asian Himalayas International Conference on Internet (AH-ICI)*, Kathmundu, 2011, pp. 1–6, 4–6 Nov. 2011
5. <http://www.secure-phone.info/>. 30 Apr 2013
6. <http://www.mobiproject.org/>. 30 Apr 2013
7. A. Goode, *Mobile Phone Biometric Security. Analysis and Forecasts*, *Goode Intelligence Reports 2011–2015* (2011)
8. P.N. Fahmi, E. Kodirov, D.J. Choi, G.S. Lee, A.M.F. Azli, S. Sayeed, Implicit authentication based on ear shape biometrics using smartphone camera during a call, in *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Seoul, 2012, pp. 2272–2276
9. R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, J. Liu-Jimenez, Performance evaluation of handwritten signature recognition in mobile environments, *Institution of Engineering and Technology*. doi:10.1049/iet-bmt.2013.0044 (On-line, pending printed publication)
10. J. Vazquez-Fernandez, H. Garcia-Pardo, D. Gonzalez-Jimenez, L. Perez-Freire, Built-in face recognition for smart photo sharing in mobile devices, in *IEEE International Conference on Multimedia and Expo (ICME)*, Barcelona, 2011, pp. 1–4
11. J.G. Casanova, C.S. Ávila, A. de Santos Sierra, G.B. del Pozo, V.J. Vera, A real-time in-air signature biometric technique using a mobile device embedding an accelerometer, in *Networked Digital Technologies*, Prague (Springer, Berlin/Heidelberg, 2010), pp. 497–503
12. M.O. Derawi, H. Witte, S. McCallum, P. Bours, Biometric access control using near field communication and smart phones, in *5th IAPR International Conference on Biometrics (ICB)*, New Delhi, 2012, pp. 490–497
13. R. Blanco-Gonzalo, L. Diaz-Fernandez, O. Miguel-Hurtado, R. Sanchez-Reillo, Usability evaluation of biometrics in mobile environments, in *IEEE International Conference on Human System Interaction (HSI)*, Gdańsk, 2013, pp. 123–128

14. A. de Santos Sierra, C.S. Ávila, G.B. del Pozo, J.G. Casanova, Unconstrained and contactless hand geometry biometrics. *Sensors* **11**, 10143–10164 (2011)
15. J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy, L. Iftode, Rootkits on smart phones: attacks, implications and opportunities, in *Proceedings of the 11th International Workshop on Mobile Computing Systems and Applications (HotMobile)*, Annapolis, 2010, pp. 49–54

Biometrics, Overview

Arun Ross¹ and Anil K. Jain²

¹Michigan State University, East Lansing, MI, USA

²Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA

Synonyms

Biometric recognition; Biometric system

Definition

Biometrics is the science of establishing the identity of a person based on the physical (e.g., fingerprints, face, hand geometry, and iris) or behavioral (e.g., gait, signature, and keyboard dynamics) attributes associated with an individual. A typical biometric system uses appropriately designed sensors to capture the biometric trait of a person and compares this against the information stored in a database to establish identity. A biometric system can operate in two distinct modes: in the verification mode, the system *confirms or negates* a claimed identity, while in the identification mode, it *determines* the identity of an individual.

Introduction

A wide variety of systems require reliable authentication schemes to confirm the identity of an

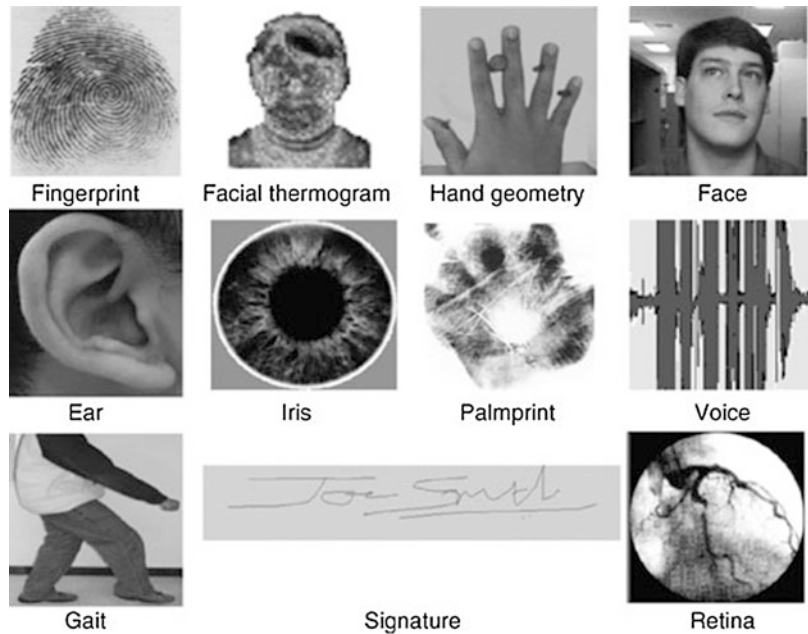
individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust authentication schemes, these systems are vulnerable to the wiles of an impostor.

Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. However, security can be easily breached in these systems when a password is divulged to an unauthorized user or an ID card is stolen by an impostor. Further, simple passwords are easy to guess (by an impostor), and complex passwords may be hard to recall (by a legitimate user). The emergence of *biometrics* has addressed the problems that plague these traditional security methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physical or behavioral traits associated with the person. By using biometrics, it is possible to establish an identity based on “who you are,” rather than by “what you possess” (e.g., an ID card) or “what you remember” (e.g., a password). Current biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermograms, signature, voiceprint, etc. (Fig. 1) to establish a person’s identity [1–5]. While biometric systems have their limitations (e.g., additional cost, temporal changes in biometric traits, etc.), they have an edge over traditional security methods in that they cannot be easily stolen, shared, or lost.

Biometric systems also introduce an aspect of user convenience that may not be possible using traditional security techniques. For example, users maintaining different passwords for different applications may find it challenging to recollect the password associated with a specific application. In some instances, the user might even forget the password, requiring the system administrator to intervene and reset the password for that user. Maintaining, recollecting, and resetting passwords can, therefore, be a tedious and

Biometrics, Overview,

Fig. 1 Examples of some of the biometric traits used for authenticating an individual



expensive task. Biometrics, however, addresses this problem effectively: a user can use the same biometric trait (e.g., right index finger) or different biometric traits (e.g., fingerprint, hand geometry, iris) for different applications, with “password” recollection not being an issue at all.

Operation of a Biometric System

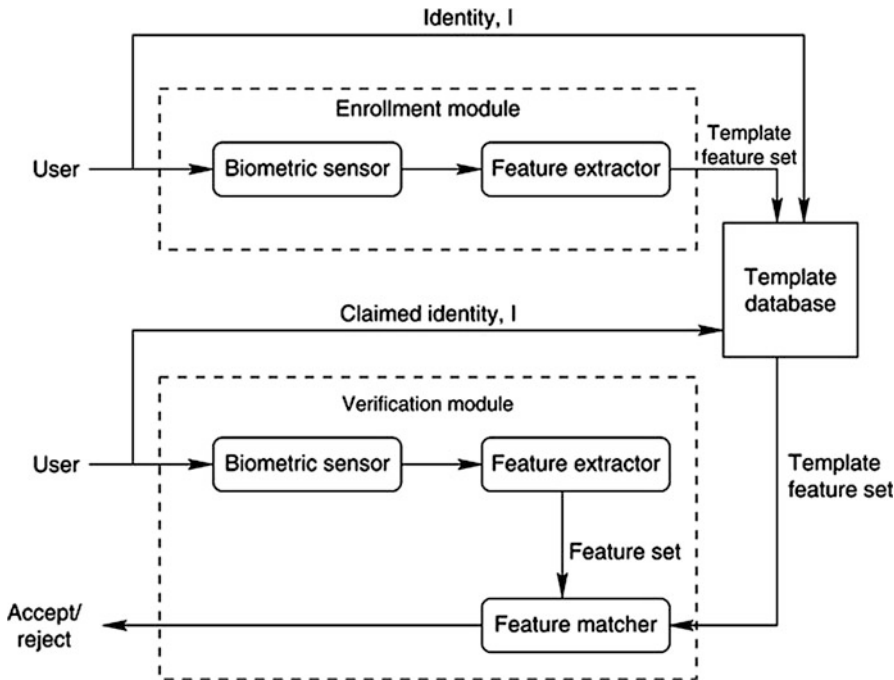
A typical biometric system operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template feature set stored in the database (Fig. 2). In an *identification* scheme, where the goal is to recognize the individual, this comparison is done against templates corresponding to all the enrolled users (a one-to-many matching); in a *verification* scheme, where the goal is to verify a claimed identity, the comparison is done against only those templates corresponding to the claimed identity (a one-to-one matching). Thus, identification (“Whose biometric data is this?”) and verification (“Does this biometric data belong to Bob?”) are two different problems with different inherent complexities. The templates are typically created at the time

of enrollment and, depending on the application, may or may not require human personnel intervention.

Biometric systems are being increasingly deployed in large-scale civilian applications. The Schiphol Privium scheme at the Amsterdam airport, for example, employs iris scan cards to speed up the passport and visa control procedures. Passengers enrolled in this scheme insert their card at the gate and look into a camera; the camera acquires the image of the traveler’s eye and processes it to locate the iris and compute the Iriscode; the computed Iriscode is compared with the data residing in the card to complete user verification. A similar scheme is also being used to verify the identity of Schiphol airport employees working in high-security areas. Thus, biometric systems can be used to enhance user convenience while improving security.

A simple biometric system has four important modules [6]:

- (1) *Sensor module* which acquires the biometric data of an individual. An example would be a fingerprint sensor that images the fingerprint ridges of a user;
- (2) *Feature extraction module* in which the acquired biometric data is processed to extract



Biometrics, Overview, Fig. 2 The enrollment module and the verification module of a biometric system

a feature set that represents the data. For example, the position and orientation of ridge bifurcations and ridge endings (known as minutiae points) in a fingerprint image are extracted in the feature extraction module of a fingerprint system;

- (3) *Matching module* in which the extracted feature set is compared against that of the template by generating a match score. For example, in this module, the number of matching minutiae points between the acquired and template fingerprint images is determined, and a matching score reported.
- (4) *Decision-making module* in which the user's claimed identity is either accepted or rejected based on the matching score (verification). Alternatively, the system may identify a user based on the matching scores (identification).

Quantifying Performance

Unlike password-based systems, where a perfect match between two alphanumeric strings is

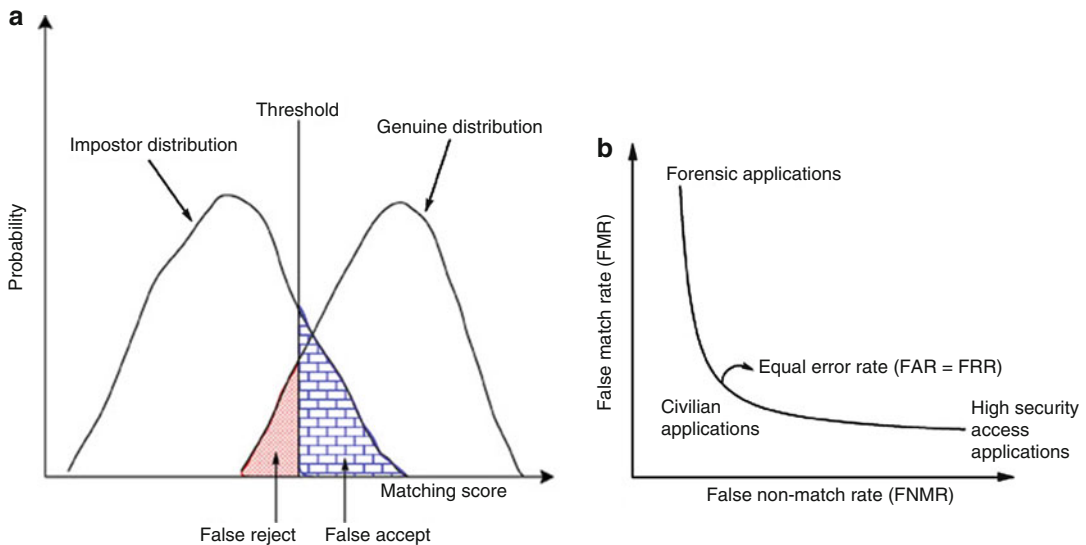
necessary to validate a user's identity, a biometric system seldom encounters two samples of a user's biometric trait that result in exactly the same feature set. This is due to imperfect sensing conditions (e.g., noisy fingerprint due to sensor malfunction), alterations in the user's biometric characteristic (e.g., respiratory ailments impacting speaker recognition), changes in ambient conditions (e.g., inconsistent illumination levels in face recognition), and variations in the user's interaction with the sensor (e.g., occluded iris or partial fingerprints). The variability observed in the biometric feature set of an individual is referred to as *intra*class variation, and the variability between feature sets originating from two different individuals is known as *inter*class variation. A useful feature set exhibits small *intra*class variation and large *inter*class variation.

A similarity match score is known as a genuine score or authentic score if it is the result of matching two samples of the same biometric trait of a user. It is known as an impostor score if it involves comparing two biometric samples originating from different users. To analyze the

performance of a biometric system, the probability distribution of genuine and impostor matching scores is examined. A genuine matching score is obtained when two feature sets corresponding to the *same* individual are compared, and an impostor matching score is obtained when feature sets from two *different* individuals are compared. In the case of verification, when a matching score exceeds a certain threshold, the two feature sets are declared to be from the same individual; otherwise, they are assumed to be from different individuals. Thus, there are two fundamental types of errors associated with a verification system: (i) a false match, which occurs when an impostor matching score exceeds the threshold, and (ii) a false nonmatch, which occurs when a genuine matching score does not exceed the threshold. The error rates of systems based on fingerprint and iris are usually lower when compared to those based on voice, face, and hand geometry. A Receiver Operating Characteristic (ROC) curve plots the False Non-match Rate (FNMR – the percentage of genuine scores that do not exceed the threshold) against the False Match Rate (FMR – the percentage of impostor scores that exceed the

threshold) at various thresholds. The operating threshold employed by a system depends on the nature of the application. In forensic applications, for example, a low FNMR is preferred, while in high-security-access facilities like nuclear labs, a low FMR is desired (Fig. 3).

In the case of identification, the input feature set is compared against all templates residing in the database to determine the top match (i.e., the best match). The top match can be determined by examining the match scores pertaining to all the comparisons and reporting the identity of the template corresponding to the largest similarity score. The *identification rate* indicates the proportion of times a previously enrolled individual is successfully mapped to the correct identity in the system. Here, assume that the question being asked is “Does the top match correspond to the correct identity?” An alternate question could be “Does any one of the top k matches correspond to the correct identity?” (see [7]). The rank- k identification rate, R_k , indicates the proportion of times the correct identity occurs in the top k matches as determined by the match score. Rank- k performance can be summarized using



Biometrics, Overview, Fig. 3 Evaluating the matching accuracy of a biometric system operating in the verification mode. (a) Histograms of genuine and impostor matching scores and the two types of errors (False Accept and False Reject) that are possible in a verifi-

cation system. (b) A Receiver Operating Characteristic (ROC) curve indicating the operating point (threshold) for different types of applications. Note that FMR and FNMR are often used as synonyms for FAR and FRR, respectively

Biometrics, Overview, Table 1 Authentication solutions employing biometrics can be used in a variety of applications which depend on reliable user authentication mechanisms

Forensics	Government	Commercial
Corpse identification	National ID card	ATM
Criminal investigation	Driver's license; voter registration	Access control; computer login
Parenthood determination	Welfare disbursement	Mobile phone
Missing children	Border crossing	E-commerce; Internet; banking; smart card

the Cumulative Match Characteristic (CMC) that plots R_k against k , for $k = 1, 2, \dots, M$ with M being the number of enrolled users.

Besides FMR and FNMR, other types of errors are also possible in a biometric system. The Failure to Enroll (FTE) error refers to the inability of a biometric system to enroll an individual whose biometric trait may not be of good quality (e.g., poor-quality fingerprint ridges). Similarly, a biometric system may be unable to procure good-quality biometric data from an individual during authentication resulting in a Failure to Acquire (FTA) error.

A biometric system is susceptible to various types of attacks [8]. For example, an impostor may attempt to present a fake finger or a face mask or even a recorded voice sample to circumvent the system. The problem of fake biometrics may be mitigated by employing challenge-response mechanisms or conducting liveness detection tests. Privacy concerns related to the use of biometrics and protection of biometric templates are the issues that are currently being studied [9–11].

Applications

Establishing the identity of a person with high confidence is becoming critical in a number of applications in our vastly interconnected society. Questions like “Is she really who she claims to be?,” “Is this person authorized to use this facility?,” or “Is he in the watchlist posted by the government?” are routinely being posed in a variety of scenarios ranging from issuing a driver's license to gaining entry into a country. The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication, and mobility. Thus, biometrics is

being increasingly incorporated in several different applications. These applications can be categorized into three main groups (see Table 1):

1. Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM or credit card use, physical access control, mobile phone, PDA, medical records management, distance learning, etc.
2. Government applications such as national ID card, managing inmates in a correctional facility, driver's license, social security, welfare disbursement, border control, passport control, etc.
3. Forensic applications such as corpse identification, criminal investigation, parenthood determination, etc.

Summary

The increased demand for reliable and convenient authentication schemes, availability of inexpensive computing resources, development of cheap biometric sensors, and advancements in signal processing have all contributed to the rapid deployment of biometric systems in establishments ranging from grocery stores to airports. The emergence of multibiometrics has further enhanced the matching performance of biometric systems [12, 13]. It is only a matter of time before biometrics integrates itself into the very fabric of society and impacts the way we conduct our daily business.

Related Entries

- ▶ [Biometric Applications, Overview](#)
- ▶ [Remote Authentication](#)
- ▶ [Soft Biometrics](#)

References

1. A.K. Jain, P. Flynn, A. Ross (eds.), *Handbook of Biometrics* (Springer, New York, 2007)
2. J.L. Wayman, A.K. Jain, D. Maltoni, D. Maio (eds.), *Biometric Systems: Technology, Design and Performance Evaluation* (Springer, New York, 2005)
3. R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior, *Guide to Biometrics* (Springer, New York, 2003)
4. H. Wechsler, *Reliable Face Recognition Methods: System Design, Implementation and Evaluation* (Springer, New York, 2006)
5. D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition* (Springer, New York, 2003)
6. A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Technol. Spec. Issue Image- Video-Based Biom.* **14**(1), 4–20 (2004)
7. H. Moon, P.J. Phillips, Computational and performance aspects of PCA-based face recognition algorithms. *Perception* **30**(5), 303–321 (2001)
8. N.K. Ratha, J.H. Connell, R.M. Bolle, An analysis of minutiae matching strength, in *Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Halmstad, 2001, pp. 223–228
9. S. Prabhakar, S. Pankanti, A.K. Jain, Biometric recognition: security and privacy concerns. *IEEE Secur. Priv. Mag.* **1**(2), 33–42 (2003)
10. M. Rejman-Greene, Privacy issues in the application of biometrics: a european perspective, in *D. Biometric Systems: Technology, Design and Performance Evaluation*, ed. by J.L. Wayman, A.K. Jain, D. Maltoni Maio (Springer, New York, 2005), pp. 335–359
11. S. Kenny, J.J. Borking, The value of privacy engineering. *J. Inf. Law Technol.* **7**(1) (2002). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/
12. A.K. Jain, A. Ross, Multibiometric systems. *Commun. ACM, Spec. Issue Multimodal Interfaces* **47**(1), 34–40 (2004)
13. A. Ross, K. Nandakumar, A.K. Jain, *Handbook of Multibiometrics*, 1st edn. (Springer, New York, 2006)