Chapter 3
Biometric Data

Biometric data has well defined relationships between its various data elements: people, templates, samples and matches. An understanding of the associated structure is fundamental to both building robust biometric systems and the analysis of data relationships. However, many systems that are developed do not appropriately reflect these foundations, and as a consequence are less flexible than desired. The ongoing evolution of biometric standards is also helping to enforce data quality standards, and facilitate interoperability and data exchange between different biometric systems.

Every biometric has unique properties. In addition to the wide variety of physiological differences, the acquisition process introduces many differences in sample appearance and quality. Determining the variations that lead to poor performance is vital to the analysis of any biometric system. According to the Pareto principle, it is likely that 80% of problems in a system are due to just 20% of poor quality enrollments and acquisitions. Consequently, examining issues related to biometric data is useful and informative, as it gives an appreciation for real world challenges in deploying a biometric solution.

The goals of this chapter are to:

- Explain the inherent relationships between people, templates, biometric data and matches (Sect. 3.1).
- List some published biometric standards in data interchange, applications and testing (Sect. 3.2).
- Show examples of quality variation for several commonly used biometrics (Sect. 3.3).

3.1 Storage of Biometric Data

Biometric information comes in many forms including personal biographic details, match results, acquisition and enrollment times, sensor types, raw biometric sam-

ples, errors, templates, quality information and scores. Structuring this information to allow for any type of system use and expansion is an important part of biometric system design.

3.1.1 Primary Biometric Data Elements

The relationship between the different primary data elements in a biometric system is shown in Fig 3.1. This structure holds true regardless of the biometric or whether the system is used for identification or verification. Databases conforming to this Primary Biometric Data Element (PBDE) structure will have increased flexibility.

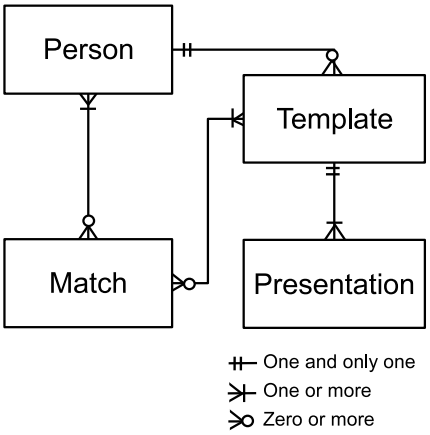


Fig. 3.1 Primary Biometric Data Elements (PBDE) structural relationship.

- **Person**: The top level entity is the 'Person', from which all other data is derived. Each person may have associated with them biographic data that does not change, such as sex, date of birth and ethnicity. A person entity can be associated with zero or more match records and zero or more templates. For example, they may have templates from several different characteristics or templates acquired at different times.
- **Template**: Each person may have one or more biometric templates. These templates contain both enrollment, and potentially verification, information.[1] Associated with each template can be a variety of data including a quality measure, the date of capture and information specific to the biometric or environment such as the ambient lighting or if a person is wearing glasses. A template belongs to one

[1] The term template is used in a slightly different manner than from the ISO definition since it may refer to a "template" generated from a verification sample as well as from an enrollment sample.

and only one person, but may be constructed from multiple biometric samples. A match is the comparison of two templates.

- **Presenation**: A template may be created from the sample data aquired during one or more biometric presentations. When multiple samples are used as part of the template this is usually created using several presentations of a biometric over a short time period during enrollment. A system may also hold biometric presentations from different modalities (e.g. finger and iris). Generally, one particular presentation only contributes to a single template.
- **Match**: A match record contains the score result from a comparison of two template records. It can be either a genuine match, where the templates are from the same person and instance, or an impostor match, where they are known to be from different people. The record also needs to record matching errors (such as a failure to acquire). A match may belong to either one person, for a genuine match, or two people, for an impostor match.

3.1.2 Transactions

An authentication using biometrics may be comprised of a series of matching attempts, known as a transaction, rather than a single match. In other words, the decision to accept or reject the identity claim may involve multiple matches. One example is a system that allows a second (or even third) attempt to verify if the first attempt fails. Alternatively, there may be sequential matches that take place during authentication, such as in a speaker verification system that asks several questions for verification. Finally, some systems are multimodal, and these systems use more than one biometric, and hence more than one match must be conducted (see Chap. 4). A transaction record must group all these matches into a single logical unit along with a single verification decision (i.e. accept or reject). In the entity relation structure (Fig. 3.1) this can be accomplished by the use of a transaction identifier for each match record.

3.1.3 Errors and Quality

For each match or enrollment there are a variety of possible errors that may occur. Most biometric errors come in the form of a Failure To Acquire (FTA) or a Failure To Enroll (FTE). Recording the reasons for failure, often due to quality factors, can assist in determining how to improve overall system performance. Note that recording failures may result in needing to create a place holder for a “failed” template, since the template was not created. Recording the quality of the sample in the template record is also recommended since this allows for modification of system thresholds to fine tune matching results for marginal quality cases, and is particularly useful when a new or updated algorithm is introduced.

The calculation of a quality score is the subject of much research. As shown in Sect. 3.3, there are many factors that can influence quality, and these are specific to the biometric being used. In general, a quality score should reflect a sample's expected matching performance. A unified quality score may involve the combination of many individual aspects of the biometric sample (such as for the ICAO face quality), or in many cases the matching engines will produce quality score as part of the matching process. Quality scores are discussed further in Sect. 8.1.3.

3.1.4 Upgrades

Biometric algorithms are constantly evolving and the design of databases to store biometric data should consider the impact of a requirement to upgrade or change engines. A new engine may have a different template structure from older engines. In this case, if the original template data has been discarded all users will need to be re-enrolled, which is a potentially costly process. Where match results are labeled with the engine and version, any analysis or audit can determine which algorithm was used for the creation.

3.1.5 Data Security and Integrity

Data security and integrity are vital to ensure trust in large scale biometric systems. Recent large scale identity thefts and losses have illustrated how important it is to consider the protection of the data. Many of the security techniques suggested are best practice for any information technology based system [1] (see Chap. 12). Physical and logical controls on systems storing biometric data can be used to prevent system breaches. Examples of these data security techniques include:

- **Data De-identification**: When possible, it is recommended that name and contact information is removed and held in a physically separate storage system than the biometric data. One advantage of this is that it reduces the impact of a system breach. It should be considered mandatory that before data is transferred over an untrusted link all records are de-identified.
- **Data preservation and signing**: Information should not be destroyed, and where possible the originals should be preserved. This is particularly important if the data may be used as evidence at a later time. Data should also be securely signed to detect any alteration.
- **Data Encryption**: Encryption is a process by which data is rendered difficult to read by unauthorized parties. Encryption targets may include any sensitive records, such as the sample data and the templates. The encryption process must include the proper management of encryption keys through a certificate authority, or similar mechanism. Encryption can also act as a barrier to the addition of identification searches when the requirements were only for verification, also

known as function creep[2], since it is more difficult to undertake a one-many search on a database where each template has been encrypted separately.

Cryptographic Approaches

Encryption is undertaken using cryptographic algorithms. These algorithms fall into two classes: symmetric and public key.

- Symmetric algorithms are where the same key is used for both encryption and decryption. This key must hence be tightly protected and cannot be shared with untrusted parties.
- Public key algorithms use two keys: a public encryption key and a private decryption key. The public encryption key may be shared, because if the message is intercepted it cannot be read without the private key. This allows much tighter controls around data security since the points at which encryption is required, such as biometric readers, do not need to store sensitive keys to securely transmit data.

Other useful cryptographic techniques include digital signatures, that can be used to prove the authenticity of the message as originating from a particular sender, and one way hashing functions that can provide assurance that the message has not been tampered with. The use of cryptographic approaches should be applied with appropriate specialized expertize, as it is easy to provide an apparently secure solution that has significant vulnerabilities, as several large companies have learned the expensive way.

- **Audit controls**: Strong audit controls can be implemented to ensure that any operations undertaken are recorded and traceable to a particular authorized individual. Audit logs should be sent securely to an unalterable data repository and digitally signed on a regular basis. They should also be recorded in an easily read non-proprietary format.
- **Data removal**: Data should be removed when it no longer needs to be held for archival or operational purposes. Possible reasons for data removal include expiry after a particular time period, due to an event such as the removal of an enrolled person, or as a result of information redundancy.

[2] Function creep is the addition non-intended functionality after a project is complete. For example, identification facilities when the original requirements were only for verification.

Storing Raw Data

The raw sample data used for the creation of templates is often deleted to protect privacy and reduce storage requirements. However, without the source data changing or upgrading the matching algorithm will be more difficult, or even impossible in some cases. Also, forensic use of the data as evidence may not be possible without the original biometric sample. A compromise is to store the original data using protected write-only or offline storage facilities, such that the data is archived but cannot be accessed on demand.

3.2 Standards

There has been a significant amount of work in the development of standards for the interoperable storage, transport and use of biometric data [13]. The standards come in three forms: those dealing with generic biometric services and data, the interoperability of different biometric characteristics and the standards on the testing of biometric systems. The standards are constantly developing, with some still in a draft stage and others, such as the BioAPI 2.0 specification, being quite mature. Standards frequently start as national standards (e.g. ANSI, American National Standards Institute) and progress to become international (ISO, International Standards Organization). The ISO Joint Technical Committee One (JTC1) contains the relavent subcommittee SC37 for biometrics, other subcommittees of interest include SC17, for cards and personal identification, and SC27 for IT security techniques. The following sections provide a snapshot of a selection of some relevant standards.[3]

3.2.1 Formats for Data Interchange

- **Finger Pattern**: An interchange format for the exchange of pattern-based fingerprint recognition data is defined by this standard. It includes both the conversion of a raw fingerprint image to a cropped and down-sampled finger pattern, and the representation of the finger pattern image. *M1 ANSI INCITS 377-2004*
- **Finger Minutiae**: The representation of fingerprint information using minutiae (ridge endings and bifurcations) is defined by this standard. It includes the placement of the minutiae, a record format, and optional extensions for ridge count and core/delta information. *M1 ANSI INCITS 378-2004*

[3] Where only ANSI standard numbers are given the standards also exist as parts standards under ISO/IEC SC37

- **Finger Image**: Image-based fingerprint and palm print recognition data exchange formats are defined by this standard. This standard is intended for those identification and verification applications that require the use of raw or processed image data. *M1 ANSI INCITS 381-2004*
- **Iris**: This standard defines iris attributes, a record format, sample records and conformance criteria. Two alternative formats for iris image data are described, one based on a Cartesian coordinate system and the other on a polar coordinate system. *M1 ANSI INCITS 379-2004*
- **Face Recognition**: Photographic (environment, subject pose, focus, etc.) properties, digital image attributes and a face interchange format for relevant applications are defined in this standard. This includes both human examination and computer automated face recognition. *M1 ANSI INCITS 385-2004*
- **Signature/Sign Data**: A Signature/Sign Data interchange format is defined containing definitions of raw, time-series based signature/sign sample data and signature/sign feature data as well as a data record format. *M1 ANSI INCITS 395-2005*
- **Hand Geometry**: A hand geometry data interoperable interchange format is defined. *M1 ANSI INCITS 396-2005*
- **Speaker Recognition**: Draft standard to define an interoperable data format for speaker verification systems. *ISO/IEC JTC 1/SC 37 N 1973*

3.2.2 General Standards

- **The BioAPI 2.0 Specification**: The BioAPI provides a high-level generic application programming interface and service provider interface for any biometric technology. It is designed to allow 'seamless' connection of different biometric sensing equipment and algorithms. An increasing number of manufactures have products that are compliant. *M1 ANSI INCITS 358-2002, ISO/IEC FDIS 24708*
- **Common Biometric Exchange Formats Framework (CBEFF)**: The Common Biometric Exchange Formats Framework (CBEFF) is a standard to allow the generic holding and transmission of biometric information along with associated metadata in a standard form. It does not attempt to specify the format of the biometric template, and acts primarily as a container. It is used as the transport encapsulation for BioAPI. An XML version of CBEFF also exists. *M1 ANSI INCITS 398-2005*
- **Multimodal and other multi-biometric fusion**: Describes standardization to support multi-biometric systems using various multi-biometric fusion techniques. *ISO/IEC TR 24722:2007*
- **Biometrics Tutorial**: Describes the main biometric technologies and applicable international standards for biometrics. *ISO/IEC TR 24741:2007*
- **Jurisdictional and societal considerations for commercial applications**: This standard looks at issues relating to the introduction of biometrics including acceptance, eduction and privacy. *ISO/IEC DTR 24714-1*

3.2.3 Applications Interoperability and Data Interchange

- **Transportation Workers (Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers**): This standard defines standards for applications where tokens are used for access control and identification of employees. It is intended for use in the transportation industry and other industries where identification and verification of employees is necessary. *M1 ANSI INCITS 383-2004*
- **Physical access control for employees at airports**: Support of token-based biometric identification and verification of employees for physical access within an airport. *ISO/IEC 24713-2:2008*
- **Border Management (Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management**): Border management applications using biometrics to authenticate the identity of non-citizens as they enter, stay in, and leave the United States. *M1 ANSI INCITS 394-2004*
- **Defense Implementations (Interoperability and Data Interchange – DoD Implementations**): Military biometric application profile settings are defined for processing and storing biometric data on enemy prisoners, detainees, internees, and persons of interest with respect to national security. *M1 ANSI INCITS 421-2006*
- **Commercial Access Control (Application Profile for Commercial Biometric Physical Access Control**): This standard defines standards in applications that use biometrics to authenticate the identity of users requesting access to a facility. It establishes minimum conformity requirements for the biometric parts of such systems. *M1 ANSI INCITS 422-2006*
- **Financial Industry (Security framework for Biometrics in Financial services):** Describes a security framework for using biometrics for authentication of individuals in financial services. Describes the architectures for implementation, specifies the minimum security requirements, and provides control objectives and recommendations. *ISO 19092:2008*
- **ANSI X9.84**: Describes the security features needed to implement biometric verification for financial services. It focues on the integrity, authentication and confidentiality of biometric transactions. Requirements for enrollment, verification, storage, transmission, and termination procedures are documented,

3.2.4 Biometric Testing Standards

- **Biometric Performance Testing and Reporting Part 1 - Principles Framework**: This standard specifies a common set of methodologies and procedures to be followed for conducting technical performance testing and evaluations. *M1 ANSI INCITS 409.1-2005, ISO/IEC 19795-1*

- **Biometric Performance Testing and Reporting Part 2 - Technology Testing Methodology**: Procedures for conducting offline tests of the performance of biometric technologies. *M1 ANSI INCITS 409.2-2005*
- **Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies**: Requirements for scenario-based biometric testing and reporting. *M1 ANSI INCITS 409.3-2005*
- **Biometric Performance Testing and Reporting Part 4 - Operational Testing Methodologies**: Requirements for operational-based biometric testing and reporting. *M1 ANSI INCITS 409.4-2006*

3.3 Biometric Data Examples

Perhaps one of the best ways to appreciate a particular biometric is to look at the marginal or boundary cases for sample quality. Obtaining high sample quality at both enrollment and verification is vital for ensuring good performance in operation. The types of poor quality samples tend to fall into the following broad, overlapping categories:

- **Distortions**: Elastic distortions are non-linear distortions (e.g. stretched skin, dilated pupil), while inelastic distortions result from the distance, translation and rotation of objects relative to the sensing equipment.
- **Occlusions**: Occlusion, where part of the biometric cannot be sensed due to obstruction, can be be caused by body parts, shadows, clothing, etc.
- **Medical**: Some medical conditions result in a reduced ability to read the biometric sample. This may be due to behavioral reasons (e.g. blindness leading to difficulties operating equipment), a degradation of the biometric characteristic (e.g. a sore throat altering one's voice biometric) or the complete loss of a biometric (e.g. a missing finger).
- **Antiquity**: The process of aging can cause an enrolled biometric to differ from the verification sample, varying in degrees depending on the time since enrollment.
- **Clothing**: Clothing such as hats, glasses and contact lens can obscure or introduce sample artifacts.
- **Environment**: The environment can affect acquisition of a biometric through the introduction of noise and additional artifacts.
- **Ergonomics**: The position and ergonomics of a sensor can directly affect the quality of samples through increased difficulty of the user in presenting a good biometric sample. Examples of this include fixed height iris systems where tall or short people have difficulty using the system, or fingerprint sensors that do not have finger guides or have small sensing areas. Often poor ergonomics will lead to increased system failures through distortions or occlusions.

The following sections look at a number of common biometrics and give examples of poor quality biometric samples. Not all of the listed factors will affect a given system since it is dependent on the particular algorithm and sensor in use.

3.3.1 Fingerprint

Each of the intricate patterns on your fingers is unique. In fact, even for identical twins the corresponding fingerprints will be different. Fingerprints have traditionally been used for identification purposes by law enforcement agencies. This is typically done by matching latent fingerprints found at crime scenes against large fingerprint databases. For example, the FBI maintains a database that contains hundreds of millions of prints.

In recent years, fingerprints have been adopted for use in the field of biometric authentication (see Sect. 1.2.1). In this case, special scanners are used to capture the fingerprint. There are many mechanisms for acquiring a fingerprint image. For example, many laptops now come with a thermal or capacitance fingerprint scanner. This derives fingerprint information by reading the ridges as a person sweeps their fingerprint over the top of a silicon sensor. Technologies used for fingerprint recognition include optical sensors (essentially taking a photo of the finger), solid-state sensors that use a silicon chip to measure capacitance, thermal, electric field or piezoelectric differences on the fingerprint, and ultrasonic readers that measure ridge position using acoustic reflections.

Fingerprints have a number of structures that can be used for identification [11]:

- **Holistic ridge flow**: The overall pattern of ridges and valleys of a fingerprint can be used to classify it into one of several common categories. The most common categories are whorl, arch, left and right loop, and tented arch. Automated matching techniques tend not to rely on these classes for recognition as they are not very distinctive and are easily misclassified.
- **Minutiae**: Minutiae are locations where fingerprint ridges split or terminate. Much of a fingerprint's individuality is captured by the distribution of its minutiae points. Each minutia has a well-defined position and orientation, and comparing the relative minutiae locations between two prints forms the basis of most traditional fingerprint matching algorithms.
- **Other characteristics**: Some features, such as wrinkles, creases and warts, may also be useful for identification, however they may be transitory so should not be relied upon.
- **Pores**: With sufficient magnification and resolution, sweat pores can be seen on fingerprint ridges. The pattern produced by these pores is highly distinctive for each fingerprint.

The quality of a fingerprint image is closely related to its suitability for matching. In other words, matching poor quality images will lead to unreliable results. The following is a list of some factors that impact the quality of a fingerprint image:

(a) Good quality (b) Too little pressure (c) Too much pressure

(d) Wet or sweaty (e) Swiped at angle (f) Poor placement

Fig. 3.2 Examples of fingerprint quality variation. (a) **Good quality**: Minutiae clearly present and ridges are well defined. (b) **Too little pressure**: Many minutiae are missing or hard to distinguish. (c) **Too much pressure**: Ridges definition is poor leading to heavy distortion and overlapping ridges. (d) **Finger wet or sweaty**: Features are obscured by moisture. (e) **Finger swiped at angle** (line-sensor): Features are distorted by the scanning process. (f) **Poor placement**: The fingerprint is highly rotated and off-center. Images (a), (b), (c), (e), and (f) are from the FVC competitions,

- **Inconsistent and unreproducible contact**: Every time a finger is pressed against a surface, it is applied with a certain amount of pressure at a particular angle. The actual amount of pressure used and the contact angle will vary from time to time, resulting in a different (and incomplete) portion of the print being captured. This is especially problematic for fingerprint scanners with a small scanning surface. In Fig. 3.2 (f), the finger is highly rotated.
- **Noise**: Even under ideal conditions, noise will be present to some degree in all fingerprint images. This is an inevitable consequence of taking discrete measurements of the physical environment. More commonly, wet or dirty fingers can lead to noisy images. Furthermore, moisturizer or other hand creams can lead

to residue being left of the sensor. Figure 3.2 (d) is noisy due to smudging and moisture.

- **Incomplete ridge structure**: There are several reasons why the entire ridge structure of a fingerprint may not be captured. If the skin is dry, sweaty, diseased or injured, some parts of the ridges may not make contact with the capturing surface, while some valleys may touch the surface. It is important for a verification system to be robust against incomplete ridge structures, and this issue is usually addressed during the prepossessing stage. In Fig. 3.2 (b), the finger has been pressed lightly against the scanner, so the ridge structure is incomplete.
- **Elastic distortions**: When a fingerprint is captured, a 3D finger is being mapped to 2D image. This introduces nonlinear deformations due to elastic distortion of the skin. This is troublesome as most matching algorithms are based on aligning fingerprint images and comparing corresponding features. When nonlinear deformations are present, a rigid alignment will be unable to align accurately all corresponding areas of the prints. Figure 3.2 (c) is a fingerprint image that is distorted due to excessive pressure.
- **Medical conditions**: Large changes in weight can affect the quality of some biometric characteristics. Some users may have medical conditions that make finger placement difficult, such as arthritis or Parkinson's, and this can be lead to poor quality captures or a complete inability to use the sensor. There are some rare disorders that result in very poor fingerprint definition.
- **Occupation**: In some professions where there is a high use of abrasive substances, such as building, fingerprints can be worn away or significantly scarred.

3.3.2 Facial Image

Two dimensional facial recognition is the use of information extracted from an image for enrollment and identification. It is self-evident from the ability to recognize people known to us in photos, regardless of wide variation in age and quality, that faces have some features that are distinctive and stable. However, there is evidence to suggest that people may not be as good as they expect in the recognition of non-familiar faces [14].

Face recognition systems do not usually use ratios of distances between facial landmarks, such as the inter-eye distance or length of the nose, as these are not particularly distinctive. Most recognition algorithms rely on pattern recognition using statistical learning techniques calibrated using large sets of data [22]. Significant advances in accuracy have come about over the previous years, particularly through the use of higher resolution images and algorithms that are more robust to environmental changes.

The stable and distinctive information contained in the face is focused in regions of the face that are unlikely to change - these tend to be around the central features of the eyes, nose and mouth. Many parts of the head tend to be unreliable in terms of visibility, as they may be covered by hair, hats or otherwise obscured due to

rotation. Face recognition can be used with existing photos that are of poor quality or low resolution, or with images taken from variety of different camera types, so there tends to be a particularly wide range of image qualities as compared to other biometrics.

(a) Good quality (b) Poor lighting (c) Expression

(d) Glare on glasses (e) Pose (f) Low Resolution

Fig. 3.3 Facial images, examples of quality variation: (a) **Good quality**: Even lighting, neutral expression, good focus. (b) **Poor lighting**: Heavy shadowing from on the right side of the face. (c) **Expression**: Mouth smiling and eyes closed. (d) **Glare on glasses**: Lighting glare obscures left eye. (e) **Pose**: Head rotated slightly to the left (f) **Low resolution**: 22 pixels from eye to eye. Images (a)-(e) used with permission J. Phillips [15]

- **Antiquity**: The duration between the time the enrollment image was taken and the verification image was obtained can affect performance. This is because the structure of the face continues to develop, particularly during adolescence, and aging changes our skin elasticity and the surface suffers environmental damage. Hence, the effect of the antiquity on a facial image depends on both the time separation and on the age of the person enrolled. It has been observed that the older

a person is, the more stable their facial characteristics for a given duration are, and the better scores that are achieved due to an increase of surface "features".

- **Pose** (inelastic distortion): The angle of the face relative to the camera introduces 3D variation in the relative position of facial features. This rotation also often causes some occlusion in facial features particularly around the nose and eye area. Ideally, the face is close to straight-on (e.g. ± 5 degrees) to the camera. In some modern systems rotated images are synthetically generated during enrollment, which improves recognition accuracy when the verification image is also rotated. In Fig. 3.3 (e) the head is rotated to the left and in Fig. 3.3 (f) the head is both highly rotated and tilted.
- **Expression** (elastic distortion): The face has a large number of muscles that control the wide range of expressions that are used for human communication. A specific methodology called the Facial Action Coding System (FACS) [5] can be used to define human facial expressions. In this system there are 32 major facial variations. Each of these expressions causes an elastic distortion of the face, and the more extreme the difference in expression between the enrollment and verification images, the more difficult the matching process. Most systems recommend that the expression should be neutral at enrollment time (with no teeth shown) since this expression is likely to be common and more easily reproducible during verification. Figure 3.3 (c) has an extreme expression, with both the eyes closed and the mouth in an open smile, and Fig. 3.3 (e) has a smile showing teeth.
- **Inner Features**: The parts of the face which are most stable are commonly used as the primary recognition information. Generally, this is the inner features bounded by the eyes, nose and mouth. When these features are obscured recognition becomes significantly more difficult**.** For this reason most systems recommend that both eyes should be open and clearly visible, and the mouth closed with a neutral expression.
- **Outer Features**: Despite being less stable in terms of visibility, the outer features can be particularly useful for distinguishing between similar looking individuals. For example, the ear lobes and chin shape are useful and distinctive identifiers. Furthermore, when not covered by hair, even creases on the forehead or around the eyes can be used. This data is particularly useful in situations where the images are of poor quality, such as for surveillance data.
- **Image Source**: A primary measurement of source quality for the facial image is the number of pixels between the eyes, also known as the inter-eye distance. The larger this distance is in pixels the more information there is available for recognition. In particular, some face recognition systems use the skin texture given sufficient resolution. Facial features should be sharp (in focus) and have appropriate tonal information (gray levels). In most systems color information is not used since it is highly variable dependent on camera settings and environment. However, it may be useful for human recognition. The images in Fig. 3.3 all have approximately 80 pixels inter-eye distance, except for (f) which has only 22 pixels.

- **Compression Effects**: Facial images are often stored and transmitted in a compressed form. The compression process is usually lossy[4], e.g. JPEG, which creates image artifacts that can affect recognition. Where compression is used it should be set to give the best image quality practical for the storage available. Also, it should be kept in mind that if images are altered and re-compressed the information loss is incremental.
- **Lighting and Glare**: Performance can be quite sensitive to lighting conditions, particularly when there is significant variation in illumination between enrollment and verification images. The effects of uncontrolled environment lighting on the human face manifests as shadows and luminance gradients across the face. Where a single strong light source is used to create an even light, this can create significant glare on forehead or glasses, cause washout of images due to the contrast between the background and the face, or if the user is not positioned exactly in front of the light it will cause shadows. In Fig. 3.3 (b) there is strong lighting coming from the top right causing shadows on the nose and chin. In Fig. 3.3 (d) the glasses have glare reflecting from the strong light source. The best light sources are diffuse and set at an intensity that causes even lighting with no glare.
- **Glasses**: Generally clear glasses with light rims will not cause significant recognition issues. However, glasses do cause problems when they obscure the inner features by glare (see Fig. 3.3 (d)), thick rims, or tinted lenses such as sunglasses.
- **Cosmetics**: Cosmetics are used to deliberately alter the appearance. For instance, makeup may be used to make the skin look smoother, creating the appearance of higher cheek bones, or highlight the eyes or mouth. All of these actions have an effect on the facial appearance and can impact matching performance, particularly where the enrollment and verification images differ in the level or style of makeup. In large population samples, women are often less distinctive than men since they attempt to present a more uniform appearance.
- **Weight change**: Significant weight change can alter the appearance of the face, although certain facial features around the nose and eyes are less affected.
- **Natural Variants**: There are a number of demographics factors that may affect performance. These factors include ethnicity, age, beards, caps, glasses and medical conditions such as eye-patches.[5] In many cases these challenges can be addressed procedurally, such as by asking for the removal of sun-glasses and hats (see Chap. 9).

3.3.3 Iris

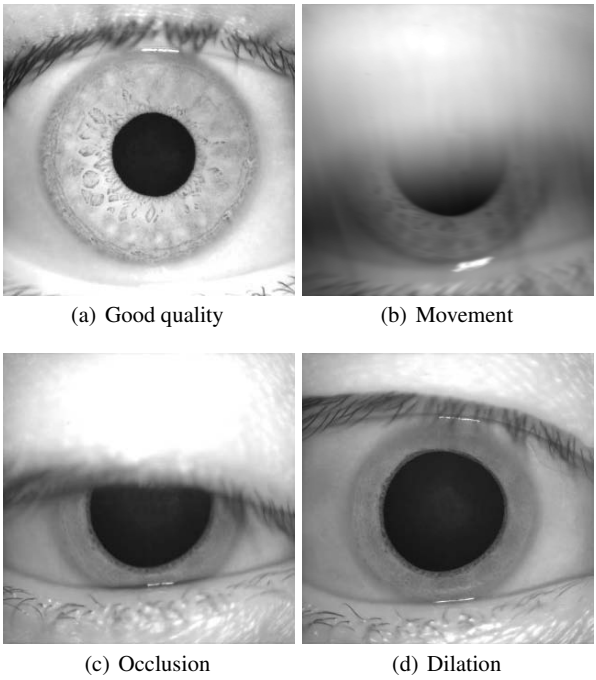
Iris systems use the random pattern of filaments on the front of a person's eye that regulate the size of the pupil (the iris) for identification. It has been shown that the

[4] The term 'lossy' refers to data compression techniques that result in a loss of information, not just file size. When lossy compression is used, it is only possible to recover an approximation of the original data.

[5] In some cases religious grounds may prevent revealing a face fully in public.

iris pattern on each eye is a highly distinctive and stable biometric characteristic. The patterns are complex and consist of a large variety of features including collagenous fibers, crypts, color, rifts and coronas. The iris pattern is set prior to birth where the iris muscle goes through folding and then de-generation [8]. After the first to second year after birth, it varies little except due to eye disease. Since the patterns are so stable, it is possible to apply specialized matching techniques to produces highly accurate results [20].

Traditionally iris cameras are set to capture an image of the iris in the near infrared range, since it is at this wavelength that the iris structure is most apparent. Registration and alignment of the iris images previously relied on substantial user cooperation (e.g. head alignment), however recent advances now make usage much simpler. Iris systems are also starting to be combined with face recognition systems to enhance accuracy, particularly for surveillance applications. Since these images are taken under less controlled conditions it has been necessary to handle images with lower quality.



(a) Good quality (b) Movement

(c) Occlusion (d) Dilation

Fig. 3.4 Iris images, examples of quality variation (a) **Good quality**: fibrous structure clearly visible eye centered. (b) **Movement**: blur caused by movement during capture. (c) **Occlusion**: partially closed eye obscures some of the iris, glare on iris. (d) **Dilation**: filaments distorted and compressed to edge.

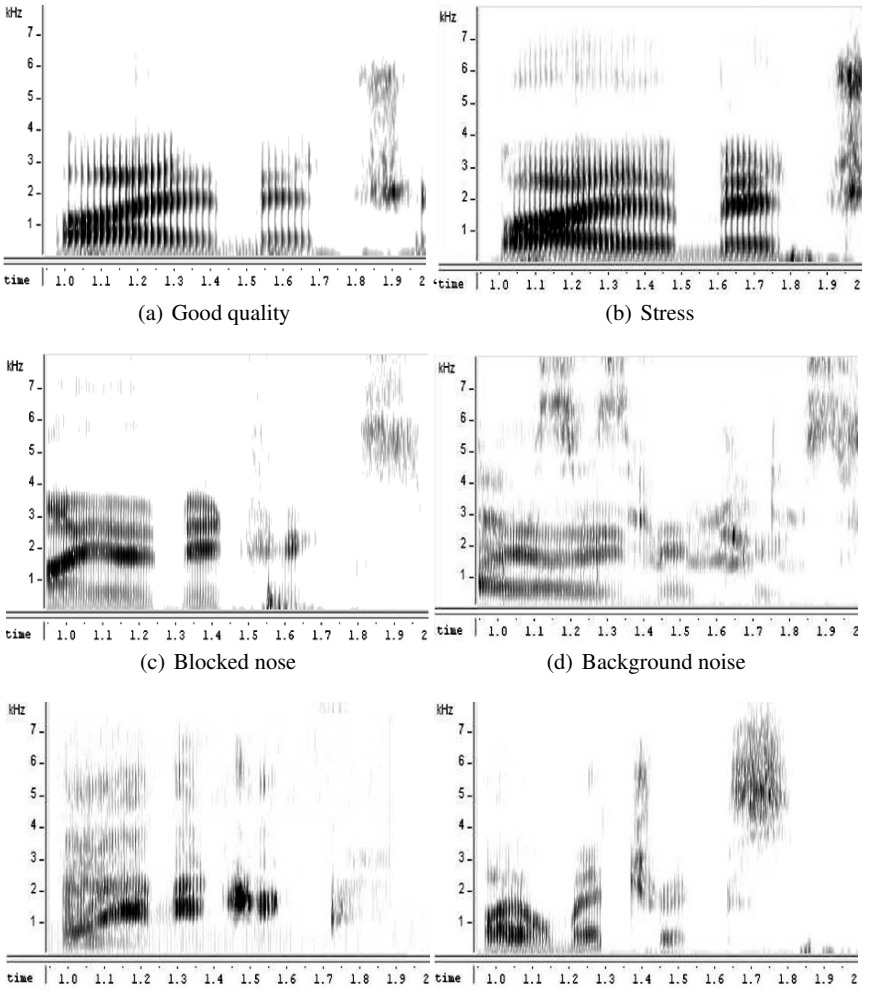
- **Contact Lens**: Contact lenses come in many forms, and not all are optically clear. Since the contact lens sits in front of the iris it will distort, to some degree, the visible filaments. If a person enrolls with a contact lens and then verifies without one this may cause performance difficulties.
- **Eye Rotation**: If the eye is not looking directly at the camera when the image is taken it may rotate about an axis. This may cause some of the filaments in the eye to be distorted.
- **Dilation**: Pupil dilation occurs when the iris muscle contracts, leading to the iris filaments being compressed. Pupil dilation can occur due to lighting extremes, arousal or drugs. Figure 3.4 (d) shows a highly dilated pupil.
- **Occlusion**: Some or all of the iris may be occluded by either the eye lid blinking, the person squinting or glasses getting in the way. In Fig. 3.4 (c) the eye is partially closed.
- **Movement**: The eye is rarely completely still due to what is known as saccades. These are fast motions in the human eye with a peak motion up to 1000 degrees per second. The movement ensures that the blind spot at the center of our vision is not noticed and allows greater visual acuity. However, it can make imaging the iris more difficult. Certain medical conditions also make these saccades more frequent. Movement can also be introduced due to normal head motion. In Fig. 3.4 (b) an iris is captured in motion.
- **Environment**: Where the iris is captured in a surveillance situation the lighting environment may cause over or under exposure of the image, making distinguishing the iris filaments difficult.
- **Eyelashes**: Long eyelashes can obscure part of the iris, causing sections of the iris to be unreadable.
- **Medical conditions**: Common medical conditions that can cause problems with iris recognition through distorting the iris include cataracts and glaucoma.
- **Glasses**: When a person is wearing glasses this can affect the optical properties of reading through the lens, particularly if the lens is tinted or has a gradient power. Glasses also collect dust and scratches which can obscure parts of the iris.
- **Glare**: Glare from lighting or environment reflection can obscure part of the iris.
- **Natural Variants**: There is a wide range of different iris variants. For example, some racial subgroups have very dark eyes, and subsequently have little visible iris structure.
- **Height**: Some iris cameras are fixed in position and require the head to be placed carefully within the capture zone. People who are shorter or taller than average, or in a wheelchair, may have difficulty positioning such that they have correct alignment.

3.3.4 Speech

Speaker verification is the use of the distinctive patterns of a person's speech for recognition. Vocal characteristics are based on both the physical aspects of the vocal

chords and the episodic nature of the local accent. One of its primary uses is for the verification of telephone transactions. As speaker verification is behavioral as well as physiological, there are two types of authentication. Text-dependent recognition [21] relies on the same word or words to be spoken as were enrolled, and text-independent [2] recognition which attempts to identify a speaker regardless of what they are saying. Many complex biological factors go into the production of speech including the movement of tongue, lips, and larynx, and the relative sizes of the nasal and oral cavities. In addition, speech accent is affected by both regional and societal factors.

- **Stress**: The fundamental frequency of voice can be significantly elevated under stress conditions [17]. This is seen in raised pitch and a change in speaking cadence. Some systems have sought to use this as a simple lie detection mechanism, however since the reaction to stress varies greatly it is a rough guide at best. In Fig. 3.5 (b) the stress can be seen in higher frequency components.
- **Colds**: Colds which affect the nasal passage or the throat will have some impact on the quality of vocal data depending on severity. Where the vocal characteristics are dramatically changed it makes recognition from a good quality enrollment almost impossible. Figure 3.5 (c) shows the effect of a blocked nose on frequency response.
- **Background noise**: Most speaker systems do not operate in an acoustically isolated environment, and background noise is always likely to be present to some degree. Where the volume levels of the background are significant, the vocal frequencies can become obscured. Noises that operate in the same spectrum as the human voice will cause the worst distortion. Figure 3.5 (d) demonstrates the masking effect of a loud background noise.
- **Mobile Phones and VoIP (Voice over IP)**: Mobile phones and calls made through the Internet are highly compressed to transmit vocal data efficiently. The compression codecs causes artifacts in the vocal signal that can reduce recognition performance. In addition, drop outs caused by transmission delays or blockages also create artifacts. The effect of a poor quality mobile phone call is illustrated in Fig. 3.5 (e).
- **Channel Mixing**: When a person enrolls on one type of device (e.g. a fixed line phone) and then verifies on a different line type (e.g. a cellular phone) this is called mixing channels. Because of the different characteristics of the channels, the frequency information can be quite different. For this reason some systems require separate enrollments for each channel.
- **Speaker Phones**: Speaker phones change the audio qualities of the voice and are more likely to be effected by background noise.
- **Text recognition**: Text-dependent recognition is concerned mainly with distinguishing one speaker from another as opposed to ensuring that the enrolled word or words are actually spoken. If a similar sounding, but different, word is spoken it may still match successfully. To address this issue it is often the case that a speech recognition system must be incorporated.



(a) Good quality (b) Stress

(c) Blocked nose (d) Background noise

(e) Mobile Phone (f) Different Speaker

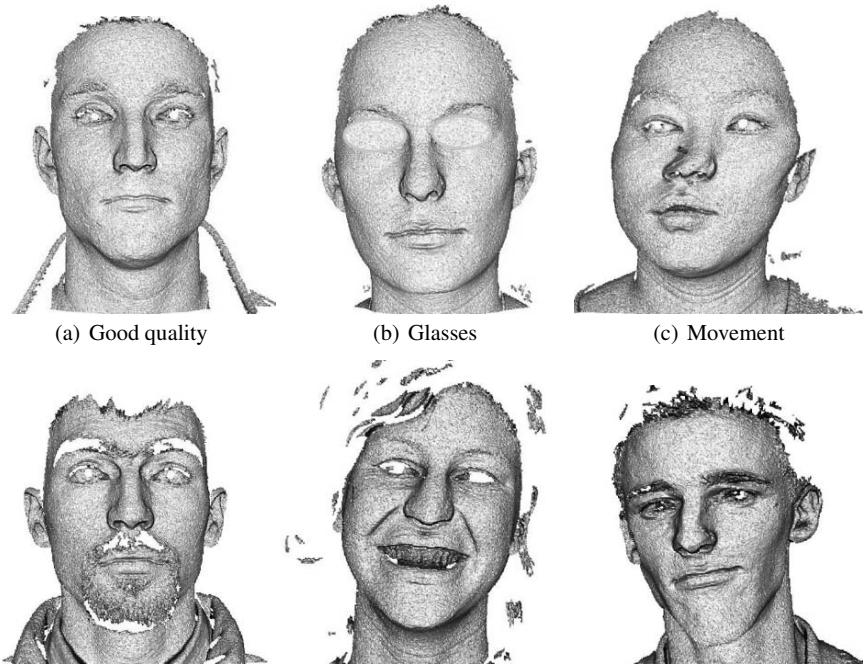
Fig. 3.5 Speech, examples of quality variation. The spectrogram show windowed (250Hz bandwidth) frequency versus time in seconds. Graphs (a)-(d) are from the same male with an Australian accent saying the word 'biometrics'. (a) **Good quality**: clear definition of vocal formant's. (b) **Stress**: higher frequency components and louder. (c) **Blocked nose**: some higher frequency components with less intensity. (d) **Background noise**: additional frequencies obscure the signal. (e) **Bad mobile phone call**: Mobile codecs compress the speech before transmission and so some frequencies are obscured. (f) **Different speaker**: a male with Canadian accent also saying 'biometrics'.

- **Mimics**: Some people are very talented at mimicking others voices. Whilst these individuals sound similar, the vocal signature still contains traces of the underlying physiology.
- **Relations**: People who are closely related to each other or are of the same gender and similar age may have very similar vocal physiology and speech style. Some testing results suggest that these individuals, whilst at an elevated risk of miss-identification, can still be distinguished from one another.
- **Age**: Speech changes with age for all people, however it is particularly apparent for males during puberty [18].

3.3.5 3D Facial geometry

Three dimensional face recognition uses various sensing technologies to determine the geometry of the face. This structure reflects the underlying skeletal foundations of the face more directly than can be obtained using two dimensional face data. Various sensing schemes have been used for acquisition, falling into three classes: passive sensing - stereo cameras that look for pixel to pixel correlation using two cameras separated by a fixed distance; active sensing - projecting a structured light onto the face (e.g. a grid) and noting the distortions in position that are caused by the facial geometry; and hybrid sensing that combines aspects of both passive and active sensing [3, 7]. The technology is still in its relatively early phase of adoption, with a small number of commercial vendors.

- **3D Rotation**: Depending on the geometry, reader information on range may be obtained from a single direction. This will cause occlusions as the head is rotated around its axis away from the camera. This effect is illustrated in Fig. 3.6 (f) where information on the left side of the nose is obscured and distorted by head tilt.
- **Noise**: Depending on the technology used to sense the geometry there may be spikes, pits and holes in the acquired surface geometry.
- **Movement**: The sensing of 3D geometry may be slower than a camera frame rate, hence it may lead to artifacts if the subject moves during acquisition. In Fig. 3.6 (c) the effect of the head moving during capture is shown.
- **Expression**: Facial expressions can radically change the geometry of the cheeks, mouth and nose. The effects of this are similar to two dimensional face recognition (see Sect. 3.3.2), however in some cases the effects are more drastic since the information available is only structural, not tonal. Figure 3.6 (e) shows the large effect that expression can have on distorting areas of the face and creating geometry holes.
- **Glasses**: Glasses cause the eye region to be occluded, since many range sensors are not able to sense through glass. The effect of this has been simulated in Fig. 3.6 (b).
- **Beards and hair**: 3D geometry systems are more capable of effectively using the structure of the jaw for recognition than two dimensional face recognition. As a



(a) Good quality (b) Glasses (c) Movement

(d) Beard (e) Expression (f) Pose

Fig. 3.6 3D Facial geometry, examples of quality variation: (a) **Good quality**: Even distance, neutral expression (b) **Glasses** (simulated): Effect of glasses on image. (c) **Movement**: Because of slow scan rates facial movement can skew source data. (d) **Beard**: Hair and beards can cause artifacts. (e) **Expression**: Mouth smiling and eyes closed. (f) **Pose**: Head rotated slightly to the left. Images (a)-(b) captured using Vivid 910 by Minolta, (c)-(e) FRGC v2 [19]. ©2008 IEEE

result, beards may affect performance. Figure 3.6 (d) shows the effect of facial hair on the image sensor - since the surface of a beard is uneven it can create holes in the data model.

- **Antiquity**: During growth years, the facial bones and structure change significantly. Furthermore, the muscles of the face become less tight, which leads to sagging. Both of these effects will alter the apparent geometry of the face.
- **Weight change**: Significant weight change can alter the 3D geometry of the face, although the geometry of facial features around the nose and eyes are less affected.

3.3.6 Vascular

The vascular network found just under the skin has been shown to be distinctive. Systems using veins for recognition are increasing in popularity. They work using a near infrared light transmitted or reflected through a biometric sample, such as a hand [4], palm [6] or finger [10], to map the pattern made by veins. As these systems are non-contact they are less susceptible to damage than most fingerprint sensors.

- **Exercise**: After and during exercise blood is pumped around the body faster. When this is the case, veins are more prominent and warmer, altering their appearance.
- **Stress**: When the body is under stress it can restrict the flow of blood to extremities. This will reduce the near infrared signature of the veins.
- **Environment**: A hot and humid environment, particularly where the user is sweating, may cause distortion of the near infrared signature.
- **Orientation and Positioning**: The positioning of the veins under the sensor is subject to three dimensional rotations which will distort their relative positions.
- **Clothing**: For palm vein recognition, the use of wrist straps or tight watches can change the amount of bloody flowing through veins.
- **Weight change**: Changes in subcutaneous fat after enrollment can potentially alter the appearance and relative position of veins.
- **Dermatological damage**: Recent trauma, scars and disease may all change the apparent position and location of the vein pattern,

3.3.7 Keystroke

Keystroke recognition is the use of inter-key timing and keystroke patterns for recognition [12]. It may also involve analysis of typing peculiarities or even word usage. Generally, a large sample of keystrokes is required in order to provide sufficient accuracy since individual keystrokes have high variability in timing.

- **Timing accuracy**: The timing of keystrokes needs to be at least at millisecond resolution. Therefore, recognizing keystrokes over a chat client is not practical due to inherent transmission delays (unless timing information is encoded into the character transmission).
- **Program Usage**: The type of data available for typing recognition depends on the way the computer is being used. For example, using email or a word processor may provide different keystroke patterns than when using a chat client.
- **Experience Level**: As a user gains experience with a keyboard or program their typing pattern is likely to change. In particular, keystroke timing becomes more precise and faster as familiarly increases.
- **Keyboard location and type**: The type of keyboard used (e.g. laptop, ergonomic or full-size) and where it is being used (e.g. desk, lap or train) will have an impact on performance.

3.3.8 Signature

Signature recognition is familiar to most people from its use with documents and credit cards. Dynamic, or online, signature recognition is a method that uses a device to capture the pressure and velocity of the pen movements in real-time for a more robust form of recognition [9].

- **Enrollment quality**: Signatures vary greatly in terms of their length and complexity, and hence the information content available for recognition varies. For example, someone with a short signature may be very easy to spoof.
- **Consistency**: Depending on the context when the signature was written, for instance when the writer is in a hurry, there can be a wide variation in the appearance, speed and pressure applied.
- **Surface angle**: The angle of the pen to the surface, depending on whether a person is seated or if they are standing, will affect the signature properties.

3.3.9 Hand Geometry

Hand geometry systems take an image of the hand inside a controlled enclosure and measure certain aspects of the geometry [16]. Distance measures include the lengths, widths and heights of the fingers, and the distance between knuckles.

- **Medical**: Arthritis can alter the appearance of the hands and joints, as well as make these devices difficult or painful to use.
- **Hand Placement**: The user is commonly required to align their hand using a series of pins. Misalignment of the hand can cause enrollment or acquisition errors.
- **Rings**: If rings are worn they may cause the finger geometry to be altered.
- **Weight change**: Weight gain or loss can affect the width of fingers and other hand dimensions.

3.4 Conclusion

This chapter has looked at biometric data from a number of different perspectives: the relationship between biometric entities, standards for biometric data storage, and quality issues affecting selected biometrics. The storage, management, protection and exchange of biometric data are important issues for consideration in any biometric implementation. The secure storage and proper management of biometric data has benefits beyond preventing external attack, as it can also help to enhance privacy protection and ensure smooth system operation.

Biometric standards have been under development for a number of years; however, until recently the adoption has been relatively slow. As the industry matures, the importance of standards compliance is being more widely appreciated. A particularly important development is the creation of a glossary of standard definitions. This will help ensure that customers, vendors and researchers are communicating using common terms and with accepted meanings. Efforts have been made to ensure that the terms used in this book (see Chap. 6) are consistent with the developing consensus around these definitions.

The old adage of 'garbage in, garbage out' applies particularly well to the relationship between data quality and matching performance. Therefore, measuring and monitoring the quality of biometric samples is of vital concern for the implementation and maintenance of any biometric system. The relationship of biometric quality scores and the suitability of a sample for authentication is an currently an active area of research. There are likely to be many further developments in techniques for quality control and assessment that will result in improved and more robust matching algorithms.

References

[1] Communications security establishment certification body canadian common criteria evaluation and certification scheme. http://www.cse-cst.gc.ca/documents/services/ccs/ccs_biometrics121.pdf (2001)

[2] Bimbot, F., Bonastre, J., Fredouille, C., Gravier, G., Magrin-Chagnolleau, I., Meignier, S., Merlin, T., Ortega-Garcia, J., Petrovska-Delacretaz, D., Reynolds, D.: A Tutorial on Text-Independent Speaker Verification. EURASIP Journal on Applied Signal Processing **2004**(4), 430–451 (2004)

[3] Bowyer, K., Chang, K., Flynn, P.: A survey of approaches and challenges in 3D and multi-modal 3D+ 2D face recognition. Computer Vision and Image Understanding **101**(1), 1–15 (2006)

[4] Cross, J., Smith, C.: Thermographic imaging of the subcutaneous vascular network of theback of the hand for biometric identification. Security Technology, 1995. Proceedings. Institute of Electrical and Electronics Engineers 29th Annual 1995 International Carnahan Conference on pp. 20–35 (1995)

[5] Ekman, P., Friesen, W.: Facial action coding system: A technique for the measurement of facial movement. In: Consulting Psychologists Press. Palo Alto (1978)

[6] Fan, K., Lin, C.: The use of thermal images of palm-dorsa vein-patterns for biometric verification. Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on **4** (2004)

[7] Heseltine, D.: Face recognition: Two-dimensional and three-dimensional technique. http://www-users.cs.york.ac.uk/~nep/research/3Dface/tomh/PhD-Heseltine.pdf (2003)

[8] Hill, M.: Anat2310: Eye development. http://anatomy.med.unsw.edu.au/cbl/teach/anat2310/Lecture06Senses(print).pdf (2003)
[9] Jain, A., Griess, F., Connell, S.: On-line signature verification. Pattern Recognition **35**(12), 2963–2972 (2002)
[10] Lian, Z., Rui, Z., Chengbo, Y.: Study on the Identity Authentication System on Finger Vein. Bioinformatics and Biomedical Engineering, 2008. ICBBE 2008. The 2nd International Conference on pp. 1905–1907 (2008)
[11] Maltoni, D., Maio, D., Jain, A., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer (2003)
[12] Monrose, F., Rubin, A.: Authentication via keystroke dynamics. Proceedings of the 4th ACM conference on Computer and communications security pp. 48–56 (1997)
[13] NIST: Published american national standards developed by incits m1 - biometrics. http://www.itl.nist.gov/div893/biometrics/documents/April%206_%20FP_Published_INCITS_M1_Standards.pdf (2007)
[14] O'Toole, A.J., Phillips, P.J., Jiang, F., Ayyad, J., Penard, N., Abdi, H.: Face recognition algorithms surpass humans matching faces over changes in illumination. In: IEEE Transactions on Pattern and Machine Intelligence, vol. 29, pp. 1642–1646 (2007)
[15] Phillips, P.J., Wechsler, H., Huang, J., Rauss, P.: The FERET database and evaluation procedure for face recognition algorithms (1998)
[16] Sanchez-Reillo, R., Sanchez-Avila, C., Gonzalez-Marcos, A.: Biometric Identification through Hand Geometry Measurements (2000)
[17] Scherer, K.R.: Effect of stress on fundamental frequency of the voice. In: The Journal of the Acoustical Society of America, vol. 61, pp. S25–S26 (1977)
[18] Sungbok, L., Alexandros, P., Shrikanth, N.: Analysis of children's speech. pitch and formant frequency. In: The Journal of the Acoustical Society of America, vol. 101, p. 3194 (1997)
[19] T.C. Faltemier, K.B., Flynn, P.: A region ensemble for 3-d face recognition. In: IEEE Transactions on Information Forensics and Security, vol. 3, pp. 62–73 (2008)
[20] Wildes, R.: Iris recognition. Biometric Systems: Technology, Design and Performance Evaluation, JL Wayman, AK Jain, D. Maltoni, and D. Maio, Eds. London: Springer-Verlag pp. 63–95 (2005)
[21] Yu, K., Mason, J., Oglesby, J.: Speaker recognition using hidden Markov models, dynamic timewarping and vector quantisation. Vision, Image and Signal Processing, IEE Proceedings- **142**(5), 313–318 (1995)
[22] Zhao, W., Chellappa, R., Phillips, P.J., Rosenfeld, A.: Face Recognition: A Literature Survey. ACM Computing Surveys **35**(4), 399–458 (2003)