Multimodal Biometric Personal Identification and Verification

Mohamed Elhoseny, Ahmed Elkhateb, Ahmed Sahlol and Aboul Ella Hassanien

Abstract Security systems using one identification tool are not ideal. Multisystem security, which using two or more types of security levels like for example using identification password and card, can increase the security of a system, however it is not an ideal security system. Password maybe hacked or forgotten, and Identification card is something we have and could be stolen. This chapter proposes a cascaded multimodal biometric system using fingerprint and iris recognition based on minutiae extraction for fingerprint identification and encoding the log-Gabor filtering for iris recognition. The experiments compare FAR, FRR, and accuracy evaluation metrics for a unimodal biometric system based on either fingerprint or iris and the cascaded multimodal biometric system that sequentially utilizes the fingerprint and iris traits. The proposed system has FAR = 0, FRR = 0.057, and accuracy 99.86%. The results show the superior performance of the proposed multimodal system compared to the unimodal system.

M. Elhoseny (✉) · A. Elkhateb
Faculty of Computers and Information, Mansoura University, Mansoura, Egypt
e-mail: mohamed_elhoseny@mans.edu.eg

A. Elkhateb
e-mail: ahmed_elkhateb@mans.edu.eg

A. Sahlol
Faculty of Specific Education, Damietta University, Damietta, Egypt
e-mail: atsegypt@du.edu.eg

A.E. Hassanien
Faculty of Computers and Information, Information Technology Department, Cairo University, Giza, Egypt
e-mail: aboitcairo@gmail.com

M. Elhoseny · A. Sahlol
Scientific Research Group in Egypt (SRGE), Cairo, Egypt

A.E. Hassanien and D.A. Oliva (eds.), *Advances in Soft Computing and Machine Learning in Image Processing*, Studies in Computational Intelligence 730,
https://doi.org/10.1007/978-3-319-63754-9_12

1 Introduction

Security systems using one identification tool are not ideal. Multisystem security, which using two or more types of security levels like for example using identification password and card, can increase the security of a system, however it is not an ideal security system. Password maybe hacked or forgotten, and Identification card is something we have and could be stolen. Another way for increasing security is using biometrics, which everyone owns unique biometrics data and cannot be forgotten or stolen. Single biometric systems suffer from some problems like noise in sensed data, non-universality, spoof attacks, intra-class variations, and inter-class similarities. Fusion in multimodal biometric systems can be performed using data accessible in any of the modules. Fusion can happen at these levels: (i) sensor level (ii) feature level (iii) score level (iv) rank level and (v) decision level. Different biometric data sources can be utilized as a part of a multimodal biometric system. In view of these sources, multimodal biometric systems could be classified into six distinct classifications: multi sensor, multi algorithm, multi instance, multi sample, multimodal and hybrid. The motivation for working on this chapter is to solve these problems, using an implementation of the multimodal biometric system. Multimodal biometric system is the use of a combination of two or more biometric types to increase the security of a system. In this chapter, a multimodal biometric system using fingerprint and iris recognition system with fusion at cascaded advanced decision level will be introduced.

2 Related Work

Multimodal biometric systems become one of the best security system solutions for most applications in present time. Many researchers have been working on multimodal biometric system. A good survey of the multimodal biometric system was provided by Ross et al. [1]. In this survey, the researchers focused on levels of fusion and score level fusion. Analysis and descriptions on recent multimodal biometric system fusion are contained in the ISO/IEC Technical Report [2]. The report explains requirements supporting multimodal biometric systems. Many research papers explained the types of levels of fusion in multimodal biometric systems. A composite fingerprint image, combining multi part fingerprints, which the user puts finger on a fingerprint sensor surface proposed by Ratha et al. [3]. A face recognition system combining visible and thermal Infrared (IR) images at sensor level was proposed by Singh et al. [4]. Another face recognition system performing a fusion of visual and thermal infrared images without eyeglass at sensor level was proposed by Kong et al. [5]. Fusion of face and iris at feature level was proposed by Son et al. [6]. fusion of hand and face at feature level was performed by Ross et al. [7] and the experiments were performed in three different scenarios. A theoretical framework for combining classifiers was developed by Kittler et al. and various classifier

combination strategies were discussed in [8]. Three different classifiers based on the k-nearest-neighbor (k-NN) classifier, logistic regression and decision trees were used to compare the performance at score level fusion by Verlinde et al. [9]. Linear discriminant function and the decision trees at the fusion of match scores were used by Jain et al. [10]. The performance of different fusion methods and normalization techniques in a fusion scenario involving fingerprint, hand geometry and face modalities studied by Jain et al. [11].

Many researchers represented the various types of multimodal biometric frameworks according to the sources of biometric data being fused. A multi-sensor fingerprint system using two sensors (optical and capacitive sensors) was discussed by Marcialis et al. [12]. A multi-algorithm biometric system integrating three different minutiae-based fingerprint matchers was proposed by Jain et al. [13]. Another multi-algorithm gait recognition framework which uses different gait classifiers based on different environmental circumstances was introduced by Han and Bhanu [5]. A multi-instance iris recognition system using a combination of right iris and left iris for the same person is introduced by Wang et al. [14]. A multi-sample system using a composite fingerprint template from multi imprints of the same finger using mosaicking algorithm is proposed by Jain et al. [15]. A hybrid system using multi-sensor and multi-sample of face recognition system is introduced by Bowyer et al. [16]. A multimodal biometric system using face, fingerprint, and voice traits is proposed by Jain et al. [17]. Another multimodal biometric system using face and palmprint is introduced by Yao et al. [18].

Ross and Jain proposed multimodal biometrics system in 2003 [19]. Fusion levels of multimodal biometric systems were introduced in details in Chap. 3. Fingerprint and iris fusion attracted the attention of many researchers. In 2009 Baig et al. [20] presented a multimodal biometric system based on iris and fingerprint using single hamming distance matcher. They used database of WVU containing 400 images and set the threshold equal to EER, the purpose was to improve the percentage of ERR. In 2010 Jagadeesan et al. [21] created a 256-bit cryptographic key using fingerprint and iris based on minutiae extraction and Daugman's approach respectively. Jagadeesan used CASIA database for iris and puplicly available database for fingerprint and make the fusion of the multimodal system at the feature level.

Radha et al. [22] in 2012, proposed a multimodal biometric system using fingerprint and iris at feature extraction fusion level. The proposed system used a combined feature vector from both fingerprint and iris. The proposed system was built using log Gabor filter feature vectors extraction of both modalities.

The final match score generated by Hamming distance. Using database of 50 users the experimental results of FAR, FRR, and execution time were 0%, 4.3, 0.14 s respectively. Abdolahi et al. [23] in 2013 proposed a multimodal biometric framework with two modalities; fingerprint and iris, using fuzzy logic and weighted code. Fusion at decision level combines results after binarizing fingerprint and iris images. Fingerprint and iris codes are weighed as 20% and 80% respectively. The FAR, FRR and accuracy results achieved from this system were 2%, 2%, and 98.3% respectively.

3 Biometric System Process

As an intelligent system [24, 25], the general structure of any biometric framework includes five operations as illustrated in Fig. 1 and listed below.

3.1 Biometric Data Acquisition

This process is responsible for collecting a biometric sample from the suitable sensors or devices. A sensor is converting the captured raw signal into a biometric sample, e.g. a unique finger impression picture, iris picture or voice recording.

3.2 Feature Extraction

This process is in charge of extracting a set of distinguished features from each biometric sample. These features should be discriminatory enough to represent each individual. The extracted features will be used as a reference during the recognition phase.

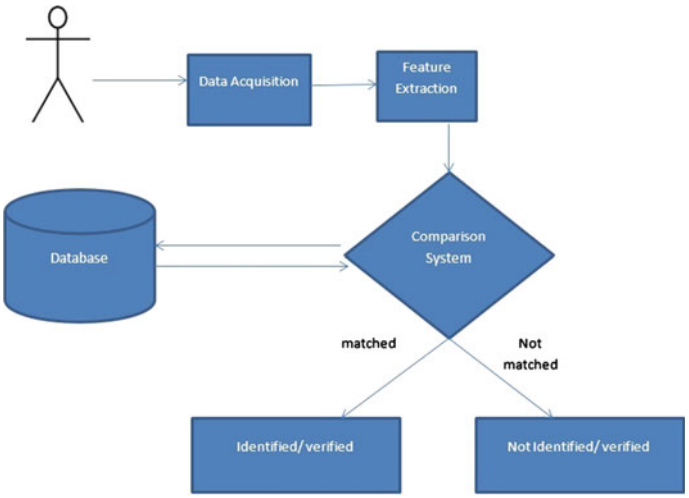

Fig. 1 General structure of biometric system

3.3 Data Storage

All the extracted features during enrollment stage are saved in a data storage system. Along with these features, some other information that related to each individual are also saved such as ID, name, privileges. Biometric and non-biometric data are frequently saved in a distinctive database for security and protection concerns.

3.4 Comparison or Matching Process

In this process, the features are extracted from the input trait are compared to all registered biometric information in the database. There are two main processes: verification or identification. Verification means, an inquiry is addressed "Is this individual who he claims to be?" When doing verification process, a matching score is computed between the input biometric and the corresponding registered biometric information. In an identification process, the inquiry being addressed is "Who is this individual?" So that, the input biometric is compared to all enrolled biometrics for all individual and return the matching scores.

3.5 Decision Subsystem

In light of the matching score(s), the decision process figures out whether the acquired biometric and the enlisted data represent one individual. In verification, the choice is made based on the matching score is either acceptable or not. In the identification scenario, one enrolled identity corresponds to the enrolled biometrics and has the best matching score coincide with the selected choice strategy.

4 Biometric System Errors

The combination of two single biometric qualities is once in a while read precisely the same. This happens because of different reasons, for example, modifications in user's biometric qualities, damaged sensing condition, user's sensor communication and modifications in surrounding conditions. In this way, the result of a biometric system is a matching score calculates the similarity comparing tested template with the stored template.

The biometric system decision relies on a set of threshold t. When the decision score s is greater than the threshold t the test template and stored template are referred to as matched and they both belong to the same user. Otherwise, when decision score s is smaller than threshold t, the test template and stored template are referred

to as not matched and the input template does not belong to an authorized user. This can lead us to the definitions of genuine distribution, and imposter distribution. Genuine distribution occurrs when the test template and stored template are matched with matching score s greater than the threshold t. Imposter distribution occurred when the test template is not matched with the stored template or matching score s is smaller than the threshold t (Fig. 2).

False Acceptance Rate (FAR) is the percentage of frauds that were incorrectly recognized over the total number tested. Sometimes it is referred to as False Match Rate FMR.

False Reject Rate (FRR) is the percentage of users that are not recognized falsely to the total numb er tested. Sometimes it is referred to as False Non Match Rate FNMR. Consolidating the FAR and FRR represents the Total Error Rate using the following equation: TER = (Number of False Accepts + Number of False Rejects)/(Total Number of Access).

When increasing the threshold t for high system security, the False Reject Rate FRR increases as well. When decreasing the threshold t to make system tolerant, the False Accept Rate FAR increases as well too. Hence, there is a need to balance between FAR and FRR. The Receiver Operating Characteristics curves (ROC) can be used for measuring the performance of the biometric system. ROC draw the relation between FAR and sensitivity (which equals to 1-FRR) (Fig. 3).

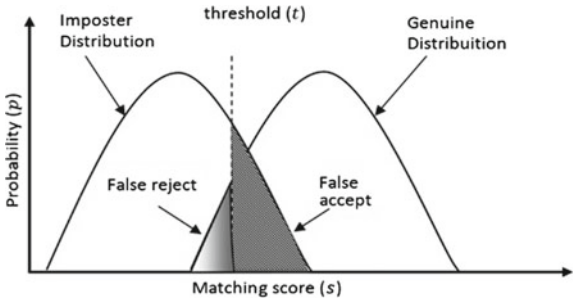

Fig. 2 Biometric system error rates: The *curves* show FAR and FRR for a given threshold t over the genuine and imposter distributions [26]

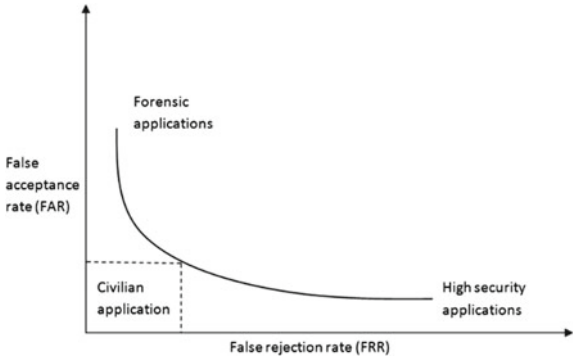

Fig. 3 Receiver Operating Characteristic curve [27]

5 Privacy Issues and Social Acceptance

Acceptability of biometric systems depends on its simplicity and comfort of use. Other factors like cultural, ethnic, and religious also affect the acceptability of the biometric system. As an instance is utilizing biometric traits that do not need contact such as voice, iris, or face reflect high acceptability. Users are more convenient with systems that require less interaction from the user. Biometric traits that acquired with no user interaction may be acquired with no user knowledge and this could be dangerous to privacy of the user. "Privacy is the ability to lead life free of intrusions to remain autonomous, and to control access to ones personal information" [26].

Biometric traits utilization considers some security issues [28, 29] that should be tended to be mentioned. Biometric system users need assurance that their biometric data is secured and protected against misuse and used only for the planned reasons. Most companies using biometric systems store the biometric data in a decentralized encoded database to ensure the security and protection of the biometric data [26].

6 Biometric Systems Challenges

In these days several biometric recognition systems rely only on using one single biometric characteristic to recognize users. Although single biometric systems can offer reliable applications for verification and identification, some limitations and vulnerabilities challenging these single biometric systems like [7]:

Noisy Data The captured biometric data usually contains noise according to, for example, imperfect acquisition conditions or variants in biometric characteristic itself like dirt on fingerprint sensor or a scratch on a fingerprint image. Genuine users always rejected as a result of noise in sensed data.

Non Universality According to some reasons biometric recognition systems sometimes are not capable of capturing perfect biometric data from genuine users resulting in an error named Failure To Enroll (FTE). For instance, drooping eyelids, long eyelashes or certain pathological conditions of eyes may prohibit the iris recognition system from capturing perfect iris data from users.

Spoof Attacks Imposters can try to mimic behavioral biometrics like signature and voice for an enrolled user. Also, creating biometric artifacts can spoof attack physical biometrics such as iris or fingerprint. However, physical traits such as fingerprints and iris are also vulnerable to spoof attacks by creating biometric artifacts. In 2002, Matsumoto et al. [30] explained how fingerprints could be spoof attack as imposters can create gummy fingers using easily obtainable tools and cheap materials. These gummy fingers are granted with high degrees using several fingerprint recognition applications [30]. In 2004, Uludag et al. [31] suggested different ways to protect biometric systems from spoof attacks like liveness detection and detection of known artifacts. Another way by challenging user response like repeating some words "please repeat after beep: 1-5-9-8".

Intra-class variations Some biometric traits change over time like hand geometry and wrong interaction from the user with the sensor represent the main reasons representing intra-class variation. In 2004, Uludag, [31] introduced a solution for intra class variation by storing multiple templates and update these templates periodically over time for each user.

Inter-class similarities Individuals' feature spaces overlapping introduce inter class similarity. The inter-class variation appears in large population identification systems and can result in bigger false acceptance rate. A solution for this problem is to identify the upper bound capacity of users that can be identified effectively using the biometric system.

7 Multibiometric Systems Fusion Levels

Multimodal systems can be constructed in several different ways, based on the biometric information sources and design of the system. Multimodal as usual refers to the system where two or more different biometric sources are in use (such as Iris and fingerprint), however the term multibiometrics is more common. Multibiometric systems include multimodal systems, and also number of different settings.

In the multimodal biometric system, fusion schemes can be performed at any of these different levels; at the sensor level, at the feature-extraction level, at the matching-score level, rank level and at the decision level. Chapter 3 discusses in details the different levels fusion.

8 Multibiometric Systems Evidence Sources

Different biometric data are utilized as part of a multimodal biometric system. In view of these sources, multimodal biometric systems are classified as six distinct classifications [1]: multi-instance, multi-sensor, multi-algorithm, multi-modal systems and hybrid.

Multi-sensor biometric systems acquire the same biometric trait from two or more different sensors. Multi-instance biometric systems use one sensor to capture two or more different instances of the same biometric modality. Multi-algorithm biometric systems process the acquired biometric trait by more than one algorithm. Multimodal biometric systems can use one or more sensors to capture more than one different traits of biometric. Hybrid system means mixing more than one of the above types. Chapter 4 will represent in details sources of evidence in multibiometric systems.

9 Multimodal Biometric Advantages Over Single Biometric

This part represents multimodal biometric systems advantages over single biometric systems [7].

Non-universality is addressed by Multibiometric systems. For instance, when the fingerprints of a user have a poor quality it prevents the user from being enrolled to the system; so usage of other biometric modalities like voice, face, iris, etc. allow systems to utilize other biometric modality and to register an individual to the system.

Multibiometric also addressed the spoof attack as it becomes more difficult for an imposter to spoof multi biometrics of a genuine user at the same time. Using the appropriate fusion technology can possibly help finding if an individual is an imposter or a genuine user. More difficulties could be added to prevent imposters to be enrolled in the system like; the system can ask the user to present modalities in random order, or the system may ask the user to pronounce certain words or numbers to make sure that the user is really alive.

Multibiometric applications report the noisy sensed data effectively. The possibility to depend on data obtained from other traits can come over the noisy sensed data from one biometric trait. Even if many multibiometric systems consider the quality of the sensed data while executing the fusion process and this is a challenging problem itself, multibiometric systems can significantly use these benefits.

Multibiometric systems addressed the problem of fault tolerant by remaining to work even if the information of a certain biometric source is unreliable according to software or sensor faults. In identification systems with large user population usually exist fault tolerance.

The accuracy of biometric systems is improved by fusing evidence from multi biometric sources. Using the suitable sources of evidence and the best fusion technique assures the matching accuracy improvement.

10 Biometric Systems Applications

Applications of Biometrics can be organized as three main groups [26]:

1. Business applications, for example, PC system login, e-trade, Internet access, ATMs or credit cards, physical access control, mobile telephones, personal digital assistant (PDA)s, medical records management, distance learning, and so on.
2. Administration applications, for example, national ID card, driver's license, social security, border control, passport control, welfare-disbursement, and so forth.
3. Legal applications, for example, body identification, criminal examination, terrorist identification, parenthood determination, and so forth.

11 Proposed Multimodal Biometric System Using Fingerprint and IRIS

In multimodal biometric systems, two or more biometrics are employed (e.g. IRIS, fingerprint, face etc.) to enhance system performance and accuracy. The proposed system uses two biometrics; Fingerprint and IRIS. The Proposed system works at two levels; at first level the extracted Fingerprints features are extracted and compared with stored finger prints templates stored in the database, second level the IRIS features are extracted, compared and matched with stored IRIS templates stored in the database. Level-II works only if Level-I is not passed. The fusion is accomplished at cascaded advanced decision level. If Level I is matched, the system avoids for matching IRIS extracted further at level II Fig. 4.

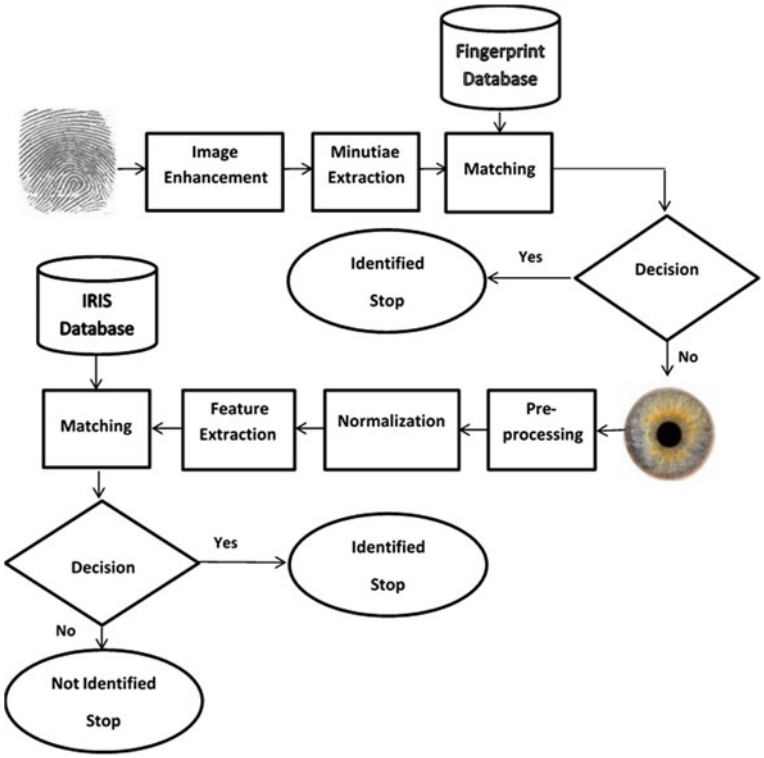

Fig. 4 Proposed system overview

11.1 Level I: Fingerprint

11.2 The Human Fingerprint [27]

Most human body skin is smooth, and contains oil glands and hair, but palm and finger's skin contain no oil glands or hair. Palms and fingers contain a flow pattern of valleys and ridges. Finger ridges (also called friction ridges) help in catching objects, and improve sensing surfaces. Two layers form the friction ridges; Inner layer called dermis, and outer layer called epidermis. Ridges that appear on epidermis enhance the friction between hand and surfaces. Uniqueness of friction ridges even with identical twins helps using it in fingerprint recognition systems for human identification and verification (Fig. 5).

11.3 Fingerprint Recognition

One of the most used single biometrics is fingerprint because it is the most proven modality for user identification. Fingerprint is composed of ridges and valleys found on finger surface. After fingerprint image acquisition, three main steps for fingerprint recognition using minutiae extraction technique which are:

1. Image Enhancement
2. Minutiae Feature Extraction
3. Comparison and Matching

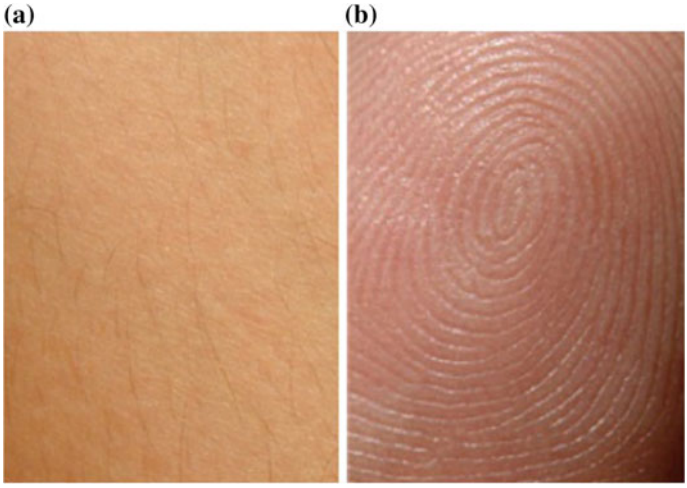

Fig. 5 Two types of skin on the human body: **a** smooth skin and **b** friction ridge skin [27]

11.4 Image Enhancement

Fingerprint image acquisition sometimes results in noisy data like holes, smudges or creases, and this lead to unsuccessful efforts for recovering real valleys or ridges. There is a need for an enhancement algorithm to enhance the structure clarity of valleys and ridges of the image to mask lost regions.

The enhancement process begins with normalizing the input image so that image mean and variance are identified and estimate the image orientation. The resulted image is used to compute a frequency image from which the region mask is acquired using block classification of normalized image. Finally, Gabor filters applied to valley and ridge pixels of normalized image to output the enhanced image of fingerprint. Figure 6b, c shows the mask region and enhanced images of the fingerprint respectively.

11.5 Feature Extraction

Before extracting the minutiae features, a thinning algorithm is applied to the enhanced fingerprint image after being binarized to decrease the thickness of ridges to a single pixel. Minutiae features are the bifurcations and ridge endpoints that are extracted from the resulted skeleton image. Minutiae points' location and orientation are extracted and stored to create a feature set. The crossing number (CN) method uses eight neighborhood connected pixels to extract minutiae points by extracting bifurcations and ridge endings from the enhanced image by testing the nearest pixels to each ridge pixel using 3×3 window. The crossing number (CN) for a given ridge can be defined as:

$$CN = \frac{1}{2} \sum_{k=1}^{8} |V_k - V_{k+1}| \tag{1}$$

where V_i is the pixel value at index i and V9 = V1. According to CN, the ridge pixels can be classified as a ridge ending, bifurcation, or not minutiae point, when CN equals 1, 3, or otherwise respectively. Figure 6d shows the minutiae points on the skeleton image. The feature vector for each detected minutiae point contains its spatial coordinates, and the ridge segment orientation. The following data is stored for each minutiae point extracted:

- The coordinates x and y,
- Ridge segment orientation, and
- Minutiae type (bifurcation, ridge, or ending)

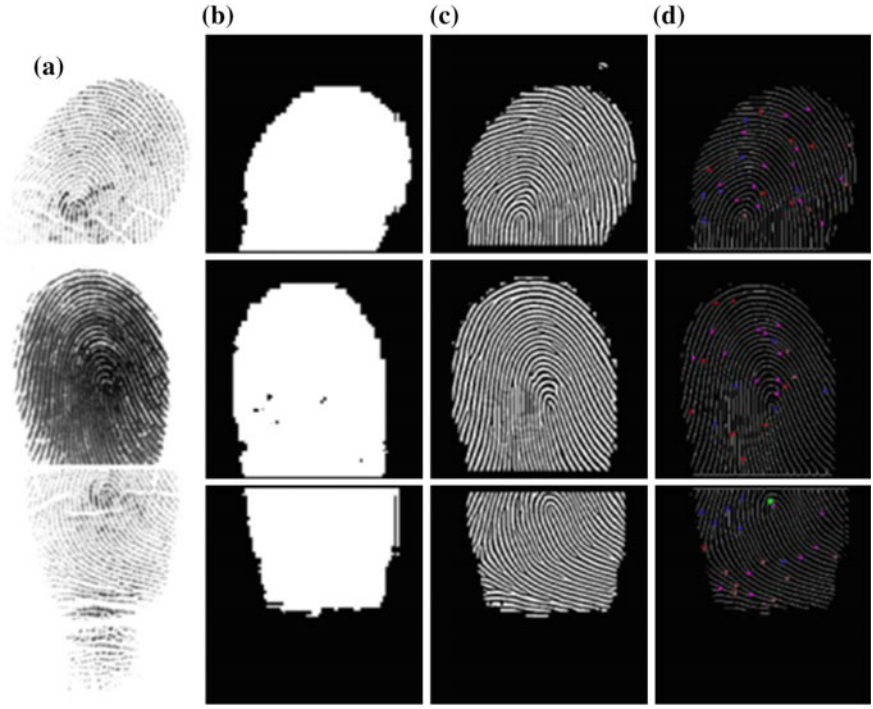

Fig. 6 Fingerprint minutiae feature extraction. **a** original image. **b** mask image. **c** enhanced image. **d** skeleton image with the minutiae points

11.6 Comparison and Matching

Minutiae points extracted from the stored database, and the query fingerprint is presented to the matching algorithm. The matching algorithm finds the association between the input query fingerprint and the stored template that maximizing the number of minutiae pairings. Consider A = $m_{a1}, \ldots m_{am}$ denotes the set of extracted minutiae points from the template in the stored database, and B = $m_{b1}, \ldots ma_{bm}$ be the extracted minutiae points from the input query fingerprint; where mi = $x; y; \theta$, x and y represents the spatial coordinates of a minutiae point and θ is its orientation. The two minutiae sets are paired if both satisfy the following geometric distance D_s and angle difference D_a constraints:

$$D_s(m_{a_i}, m_{b_j}) = \sqrt{(x_{a_i} - x_{b_i})^2 + (y_{a_i} - y_{b_i})^2} < r_d, \tag{2}$$

$$D_a(m_{a_i}, m_{b_j}) = \min\left(|\theta_{a_i} - \theta_{b_i}|, 360 - |\theta_{a_i} - \theta_{b_i}|\right) < r_a, \tag{3}$$

where r_d, and r_a are the allowed difference between the two minutiae pair. The similarity score is computed based on the number of matching minutiae pairs N_m and a total number of minutia points in the database template N_a and the query fingerprint image N_b.

$$S_{finger} = \sqrt{\frac{N_m^2}{N_a N_b}} \tag{4}$$

The generated similarity score S_{finger} between the tested and stored images is passed to the decision level. In the decision level, the S_{finger} is compared to a decision threshold. If the S_{finger} is greater than or equal to the decision threshold then the user is identified/verified and the system ends, otherwise the system moves to the next level (i.e. iris recognition).

12 Level II: IRIS

The Human Iris IRIS is a thin circular velum, lies between lens and cornea of the eye Fig. 7. IRIS consists of many layers, dense pigmentation cells contained in epithelium; the lowest layer. Above the epithelium layer lies the stromal layer which contains two iris muscles, blood vessels and pigment cells. The color of IRIS determined by density of stromal pigmentation. The externally visible surface of the multi-layered iris contains two zones, which often differ in color [16]. An external ciliary zone and an inward pupillary zone, and these two zones are separated by the collaret-which shows up as a crisscross example.

Arrangement of the iris starts by the third month of embryonic life [16]. The one of a kind example on the surface of the iris is formed the first year of life, and pigmentation of the stroma happens for the initial couple of years. Arrangement of the novel examples of the iris is arbitrary and not identified with any hereditary variables [32]. The main trademark that is subject to hereditary qualities is the pigmentation of the iris, which decides its shading. Because of the epigenetic way of iris examples, according to an individual contain totally autonomous iris examples, and

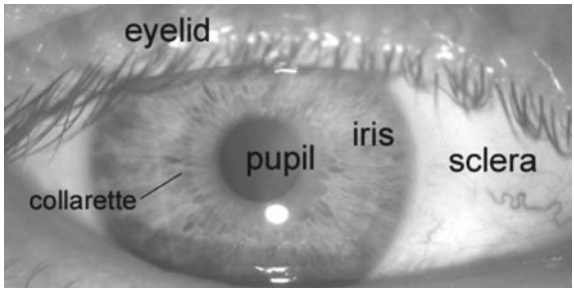

Fig. 7 Human eye view [16]

indistinguishable twins have uncorrelated iris designs. For further points of interest on the life structures of the human eye counsel the book by Wolf [16].

Iris Recognition Each person has a unique iris print which remains stable over his life. Two Circles could estimate The iris region, a circle for the pupil boundary (a central solid black circle of eye) and the other one is for the iris boundary (an annular ring between the pupil boundary and sclera). Pupil size changes according to light; when eye exposed to light the pupil expands, and when dark pupil contracts. Iris is unique for each individual as it contains the unique flowery pattern. The eyelashes and eyelids usually block the lower and upper portions of iris region. Sometimes reflections exist corrupting the iris configuration. A technique is required to locate the circular iris region, and separate and reject these objects. A standard algorithm for detecting Iris boundary is the Hough transform which can be used to derive the radius and center coordinates of the iris and pupil regions. The major steps for iris recognition are:

1. Iris and pupil segmentation
2. Normalization
3. Extracting Features
4. Comparison and Matching

Before applying the four steps mentioned above, iris image need to be captured using a suitable high-quality iris camera because the four steps will depend on image quality.

12.1 Iris and Pupil Segmentation

First; we use Canny edge detector to create an edge map. In order to effectively highlight the iris boundary, the gradients were weighted more in the vertical direction. While for pupil detection, the gradients were equally weighted in both directions. Figure 5.5b, c shows the full edge map and vertical edge map obtained by the Canny edge detector. By using the edge map, the circular Hough transform parameters are chosen. These parameters are: radius r, center coordinates x_c and y_c to define the circle according to this equation:

$$x_c^2 + y_c^2 - r^2 = 0 \tag{5}$$

The best circle radius and center coordinates are the maximum points in the Hough space. Note, the Hough transform for the iris is computed firstly. Once the iris region is detected, the second Hough transform is applied within the iris region to detect the pupil. Figure 8d shows the resulted iris and pupil segmentation. To detect the eyelids, linear Hough transform is used to fit a line on the upper and lower eyelid.

When using all gradient data it is found that the eyelids are aligned horizontally, and the eyelid edge interacts with the circular iris outer boundary. When using vertical gradients only to detect iris outer boundary decrease the impact of the eyelids

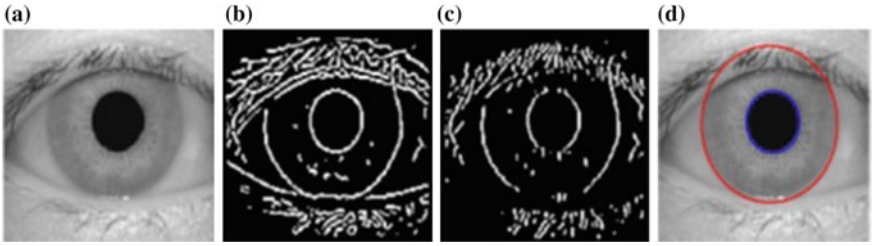

Fig. 8 Iris segmentation. **a** original image. **b** edge map. **c** vertical edge map. **d** segmented iris and pupil boundaries

when performing Hough transform technique, and some edge pixels of the iris circle can be neglected. Using this technique make iris circle localization more accurate and more efficient as it decreases the edge points tested in Hough space.

13 Normalization

The normalization is applied on the segmented iris region to have fixed dimensions of different iris images. The normalization is based on Daugman's rubber sheet model [19]. The iris region I(x; y) is transformed into the strip. The mapping is done by transforming the Cartesian coordinates (x; y) into its polar coordinates $(r; \theta)$ equivalent using

$$I(x(r,\theta), y(r,\theta)) \longrightarrow I(r,\theta) \tag{6}$$

with $x(r;\theta) = (1-r)xp(\theta) + rxi(\theta)$ and $y(r;\theta) = (1-r)yp(\theta) + ryi(\theta)$. Where $x_p; y_p$ and $x_i; y_i$ are the pupil and iris boundaries coordinates along the θ direction. The value of θ and r belongs to $[0; 2\pi]$, and [0; 1] respectively. The center of the coordinate system is at the pupil center. The reflections, eyelashes, and eyelids removed from the normalized image. Here, the polar transformed image has 20×240 dimension represents the radial and angular resolutions as shown in Fig. 9a.

Fig. 9 Iris normalization and feature coding; **a** normalized image. **b** feature codes. **c** mask image

13.1 Extracting Feature

In this stage, the most discriminative characteristics of the iris region are only extracted and encoded in a compact form to improve the accuracy recognition rate. Log-Gabor filter is used to extract iris features. The log-Gabor filter works as a band-pass filter to analysis the texture of the image. The encoding process [33] generates a bitwise template of the iris region by analysis phase information. The filter's phase is categorized into one of four quadrants where each quadrant is represented by two bits.

Here, the total number of bits in the template is 9600. A noise mask is also generated to highlight areas such as eyelids, eyelashes, and reflections identified in the segmentation stage. Figure 9b, c shows the encoding features and the mask region. The result vector is used to make the comparison between the stored iris database and query iris image.

13.2 Comparison and Matching

The matching is accomplished between iris codes Ic generated from iris database images and iris query image using Hamming distance technique. The Hamming distance measures the difference between two bit iris codes using the following equation:

$$S_{Iris} = \frac{\|Ic_A \bigoplus Ic_B \bigcap Im_A \bigcap Im_B\|}{\|Im_A \bigcap Im_B\|} \tag{7}$$

where Ic_A, Ic_B are the iris codes for stored database image and query image, and Im_A, Im_B denotes the noise masks. $\bigoplus, \bigcap$ are the Boolean operators *XOR* and *AND*. This matching score S_{Iris} is used as input to the decision level. so that if the S_{Iris} is smaller than or equal to the decision threshold then the user is identified/verified and the system ends, otherwise the system rejects the user.

14 Experimental Results

MATLAB 7.8.0.347(R2009a) is the programming language used to implement this system. The testing of the performance of the proposed system is applied using the following two databases: 1—CASIA-Iris V1 [34]; It contains 756 images acquired from 108 individuals. 7 images for each eye are captured with an advanced home-made camera for iris. All stored images are formated as BMP with resolution 320 × 280. 2—FVC 2000 ($DB4_B$) and 2002 ($DB1_B, DB2_B, DB3_B$) [35]. Each databases contain 80 fingerprints (80) acquired from ten persons; eight impressions from each person. The FVC database is free downloaded. In this proposed system, the first

Table 1 Confusion matrix

		Predicted template	
Actual		Yes	No
	Yes	TP	FN
Template	No	FP	TN

40 individuals are selected from CASIA Iris V1 and FVC 2000 and 2002 for the experiment; 35 individuals enrolled into system database (4 images for each), and 3 images for each individual is used for testing. Images of individuals from 36 to 40 are not registered in the system but used for testing only. The experiment went through four levels; Fingerprint recognition Level, Iris recognition Level, cascaded multimodal biometric level based on fingerprint and iris recognition, and multimodal biometric level based on Fingerprint and Iris recognition using AND rule at decision level fusion. Biometric applications have a number of performance measures used to characterize the performance of biometric systems. False Acceptance Rate (FAR), False Reject Rate (FRR), system accuracy, and Receiver Operating Characteristics curves (ROC) are the most important performance measures in biometric systems. False Acceptance Rate (FAR) is the percentage of imposters that were incorrectly recognized over the total number of imposters tested. False Reject Rate (FRR) is the percentage of clients that are not recognized falsely to the total number of clients tested. Receiver Operating Characteristics curves (ROC) used for visual comparison of classification models FAR, FRR and Accuracy can be calculated using the confusion matrix shown in Table 1.

True positives (TP): refers to the number of users correctly identified by the system. True negatives (TN): refers to the number of non-users correctly not identified by the system. False positives (FP): refers to the number of non-users were identified by the system. False negatives (FN): the number of users not identified by the system. FAR, FRR, and Accuracy can be calculated according to the following equations using Sensitivity which is true positive rate and specificity which is true negative rate:

$$FAR = \frac{FP}{TN + FP}. \tag{8}$$

$$FRR = \frac{FN}{TP + FN}. \tag{9}$$

$$Acc. = \frac{TP + TN}{TP + TN + FP + FN}. \tag{10}$$

14.1 Lever 1: Fingerprint Recognition Results

In this level, fingerprint Image is captured by a fingerprint scanner device, the captured image is usually corrupted because of some noises like holes, creases, and smudges, so the image needed to be enhanced to improve the quality of fingerprint image using Gabor Filter algorithm and this is the second step. In step 3; the enhanced image is binarized and passed to a thinning algorithm to increase ridge thickness to be one single pixel. The last step is matching in which the input minutiae is compared with stored minutiae templates in database, if matching score is smaller than the given threshold, identification is complete else identification is rejected. In this experiment different thresholds are chosen from 0.25 to 0.7 step 0.05. When using small thresholds the False Accept Rate is increased and False Reject Rate and Accuracy is decreased. With increasing the threshold to 0.6 False Reject Rate is increased slightly, Accuracy also is increased obviously, and False Accept Rate is decreased obviously too. When increasing threshold than 0.6 Accuracy starts to decrease again, and False Reject Rate extremely increased. The experiment results are represented in Table 2.

Figure 10 represents the performance measures; FAR, and FRR curves for the fingerprint recognition system using minutiae extraction, and Fig. 11 represents the accuracy curve.

14.2 Level 2: Iris Recognition Results

In this level Iris Image is captured by a suitable device, then automatic segmentation is applied using Hough transform to generate edge map circles and detect iris

Table 2 Finger print recognition results using minutiae extraction

Finger Threshold	FAR	FRR	Accuracy
0.25	0.8838	0	0.1383
0.3	0.5289	0.0095	0.484
0.35	0.1998	0.0381	0.8043
0.4	0.0488	0.1048	0.9498
0.45	0.012	0.1524	0.9845
0.48	0.0034	0.1714	0.9924
0.5	0.002	0.2095	0.9929
0.55	0	0.2571	0.9936
0.6	0	0.4286	0.9893
0.65	0	0.5143	0.9871
0.7	0	0.6667	0.9833

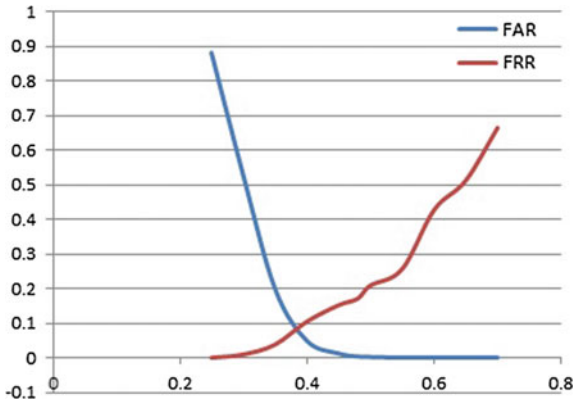

Fig. 10 FAR and FRR curves for fingerprint recognition using minutiae extraction

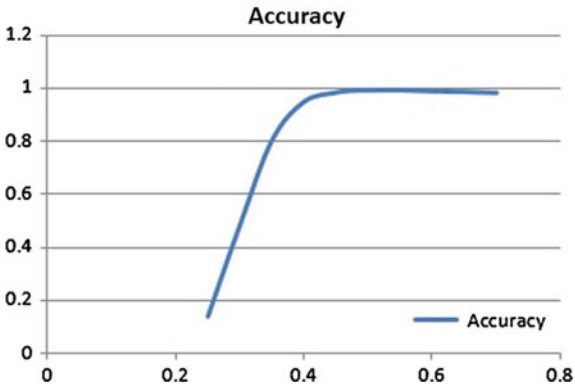

Fig. 11 The accuracy curve for fingerprint recognition using minutiae extraction

boundaries and eyelids, this step is preprocessing. Next step is normalization; in which Iris image is transformed into a strip which involves of points acquired from the outer boundary of iris to the outer boundary of the pupil and normalized to make the strip size constant for different iris images. Features are extracted using Haar wavelet in which Iris image is fragmented into four factors i.e., diagonal, vertical, horizontal, and approximation. The approximation factors are fragmented into four factors. The series of steps are reiterated for five levels and the last level arguments are collected to create a vector. The collected vector is binarized to compare easily between the query image and iris codes stored in the database. The last step is matching in which comparison between query images and iris codes from the stored database is done using hamming distance algorithm. The experiment results are represented in Table 3.

Figure 12 represents the performance measures; FAR, and FRR curves for the Iris recognition system using minutiae extraction, and Fig. 13 represents the accuracy curve.

Table 3 Iris recognition results using Hamming distance

IRIS threshold	FAR	FRR	acc
0.1500	0.000000	1.000000	0.975000
0.1600	0.000000	0.990500	0.975200
0.1700	0.000000	0.990500	0.975200
0.1800	0.000000	0.981000	0.975500
0.1900	0.000000	0.981000	0.975500
0.2000	0.000000	0.961900	0.976000
0.2100	0.000000	0.952400	0.976200
0.2200	0.000000	0.895200	0.977600
0.2300	0.000000	0.847600	0.978800
0.2400	0.000000	0.742900	0.981400
0.2500	0.000000	0.628600	0.984300
0.2600	0.000000	0.466700	0.988300
0.2700	0.000000	0.381000	0.990500
0.2800	0.000000	0.314300	0.992100

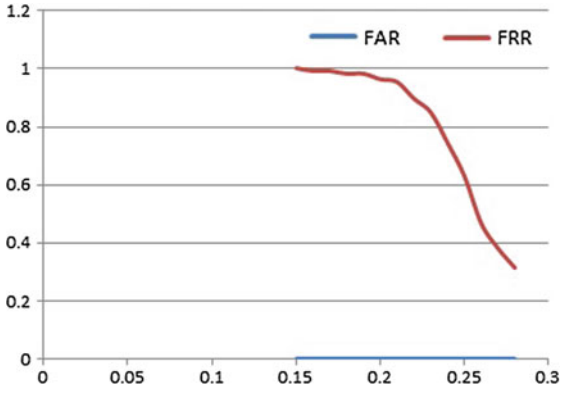

Fig. 12 FAR and FRR curves for Iris recognition using Hamming Distance

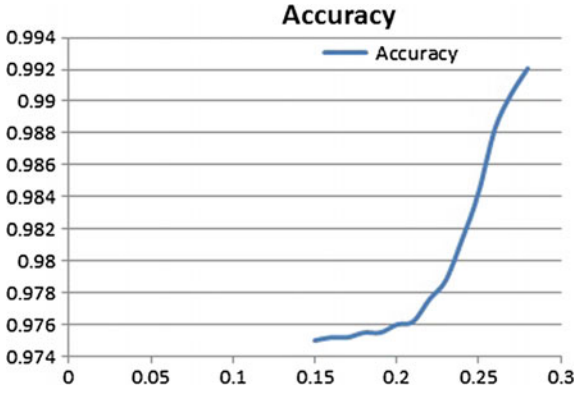

Fig. 13 the accuracy curve for Iris recognition using Hamming Distance

14.3 Level 3: Multimodal Biometric System Results Using Fingerprint and Iris

In this level, the fingerprint image is captured for an individual, enhanced using Gabor Filter algorithm, binarized and passed to thinning algorithm, extract minutiae points, matching with stored templates. If the matching score between the input pattern and the stored template is greater than the given finger threshold then identification/verification is complete else Iris Image is captured for the same individual, automatic segmentation is applied using Hough transform, preprocessing, normalization, features extraction using Haar wavelet, binariztion, matching using hamming distance algorithm.

If the matching score is smaller than the given iris threshold the identification/verification is complete else system stops with no identification/verification. In this experiment different thresholds are chosen from 0.25 to 0.7 step 0.05 for fingerprint and one threshold for Iris 0.28; this threshold is chosen as it is the smallest one achieving the highest accuracy of the tested thresholds with fingerprint thresholds and to reduce the computational complexity. When using small thresholds for fingerprint the False Accept Rate is increased and False Reject Rate and Accuracy are decreased. With increasing the threshold to 0.5 False Reject Rate is increased slightly, Accuracy also is increased obviously, and False Accept Rate is decreased obviously too. When increasing threshold than 0.6 Accuracy starts to decrease again, and False Reject Rate extremely increased. The experiment results are represented in Table 4.

Figure 14 represents the performance measures; FAR, and FRR curves for the Cascaded multimodal biometric system using finger print recognition and Iris recognition, and Fig. 15 represents the accuracy curve.

Table 4 Cascaded multimodal biometric system results using finger print recognition and Iris recognition

Finger threshold	FAR	FRR	Accuracy
0.3	0.5289	0.0095	0.484
0.35	0.1998	0.019	0.8048
0.4	0.0488	0.0286	0.9517
0.45	0.012	0.0381	0.9874
0.48	0.0034	0.0381	0.9957
0.5	0.002	0.0571	0.9967
0.55	0	0.0571	0.9986
0.6	0	0.1619	0.996
0.65	0	0.181	0.9955
0.7	0	0.219	0.9945

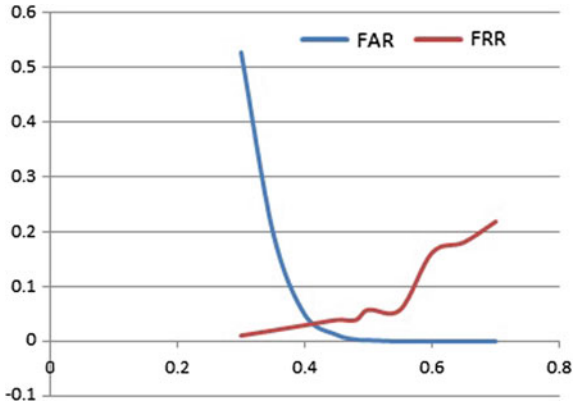

Fig. 14 FAR and FRR curves for the cascaded multimodal biometric system

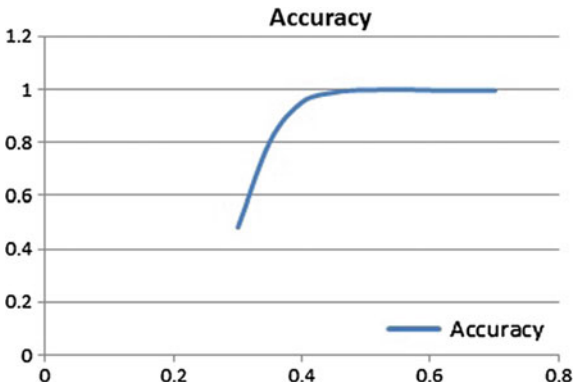

Fig. 15 The accuracy curve for the cascaded multimodal biometric system

The next curve Fig. 16 represents the Receiver Operating Characteristics (ROC) to compare the results of single biometric system using fingerprint and the cascaded multimodal biometric system using fingerprint and Iris recognition. In this curve, the sensitivity (true positive rate) of the multimodal system is farther from the diagonal than the sensitivity of single modal. This means that the multimodal biometric system is more accurate than the single biometric system.

14.4 Level 4: Multimodal Biometric System Results Using Fingerprint and Iris at Decision Level Fusion Using and Rule

In this level, fingerprint and iris images are captured in parallel for the same individual. Each image is processed using the same steps in the previous level. As for fingerprint, the image is enhanced using Gabor Filter algorithm, binarized and passed

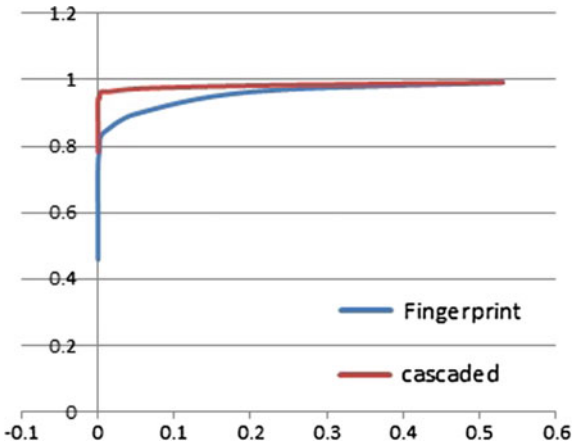

Fig. 16 The ROC curve for fingerprint recognition and cascaded multimodal biometric system using fingerprint and iris

to thinning algorithm, minutiae points extracted, and finally matched with the stored templates. For the iris image, automatic segmentation is applied using Hough transform, preprocessing normalization, Features extraction using Haar wavelet, binarization, finally using hamming distance algorithm for matching.

If the matching score for both fingerprint and iris are greater than or equal to the pre-specified threshold for both finger and iris the individual is accepted to access the system otherwise the individual is not accepted and have no wright to access the system. In this experiment the system increase the overall security and false accept rate is totally decreased; however, the accuracy is decreased and false reject rate is increased. Also, in this experiment, the time needed for identification or verification is increased as it requires to work on both fingerprint and iris for each user even if one of them is sufficient for identification or verification.

In this experiment, different thresholds are chosen from 0.3 to 0.7 step 0.05 for fingerprint and one threshold for Iris 0.28; this threshold is chosen as it is the one achieving the highest accuracy of the tested thresholds and to reduce the computational complexity.

The experiment results are represented in Table 5.

Figure 17 represents the performance measures; FRR curve for the multimodal biometric system using fingerprint and iris recognition at decision level fusion using the AND rule, and Fig. 18 represents the accuracy curve.

However, using AND rule increase system security as it requires the user to enrol both fingerprint and iris together to the system, but the cascaded system achieved more accuracy than using the AND rule.

Table 5 Multimodal biometric system results using AND rule

Finger Threshold	FAR	FRR	Accuracy
0.3	0	0.314286	0.992143
0.35	0	0.333333	0.991667
0.4	0	0.390476	0.990238
0.45	0	0.428571	0.989286
0.48	0	0.447619	0.98881
0.5	0	0.466667	0.988333
0.55	0	0.514286	0.987143
0.6	0	0.590476	0.985238
0.65	0	0.67619	0.983095
0.7	0	0.790476	0.980238

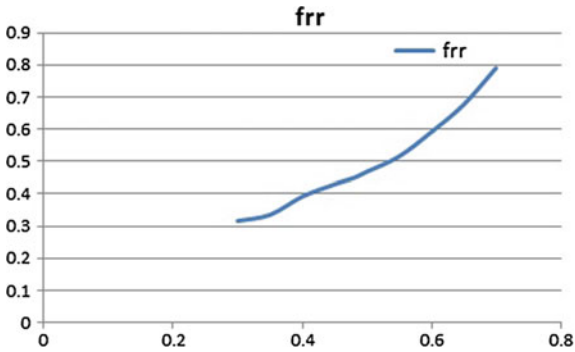

Fig. 17 FAR and FRR curves for the multimodal biometric system using fingerprint and iris at decision level fusion using AND rule

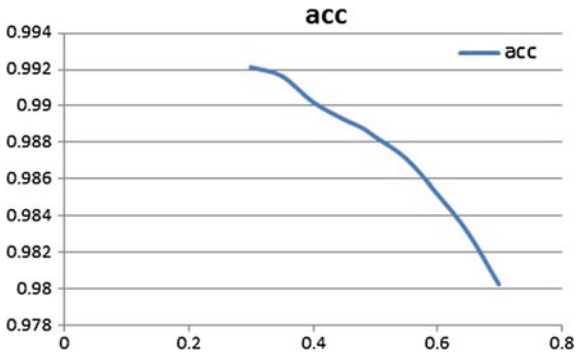

Fig. 18 The accuracy curve for the multimodal biometric system using fingerprint and iris at decision level fusion using AND rule

14.5 Conclusion

Most Security systems can be considered as one of these three types; knowledge based; "What you know" like PIN, passwords, or ID however it may be guessed, forgotten, or shared. Another type is token "What you have" like cards, or key; it may be lost or duplicated and it can be stolen. Last type is the use of biometrics; "What you are" like fingerprint, IRIS, face …, etc.

Biometric identification systems have the ability to recognize individuals by measuring and analyzing physiological or behavioral characteristics and comparing them against template set stored in the database. Unimodal biometric systems suffer from some problems like noise in sensed data, non-universality, spoof attacks, intra-class variations, and inter-class similarities.

Multimodal biometric system is the use of a combination of two or more biometric types to increase the security of a system (like: Fingerprint and Iris) to increase security for user identification or verification.

Five levels of fusion in multimodal biometric systems: sensor level; in which raw data captured by the sensor are combined, feature level; in this level, features created from each user biometric process are combined to make a single feature set, score level; in which match scores provided by different matchers representing degree of similarity between the input and stored templates, are fused to reach the final decision, rank level; each biometric subsystem assigns a rank to each enrolled identity and the ranks from the subsystems are combined to obtain a new rank for each identity, and decision level; the final result for every biometric subsystem are combined to obtain final recognition decision.

Multibiometric systems categorized into six different types: multi sensor; uses more than one sensor to capture biometric trait to extract various data, multi algorithm; in which more than one algorithm applied to the same biometric data, multi instance; use more than one instance of the same biometric (for example, left and right index fingers or left and right irises), multi sample; more than one sample of the same biometric are captured using the same sensor to acquire a more complete representation of the underlying biometric, multimodal; combine evidence of two or more biometric traits, and hybrid; refers to systems using two or more of the other five mentioned categories.

In this chapter a proposed system using Fingerprint and Iris recognition is presented based on minutiae extraction for fingerprint recognition and hamming distance for IRIS Recognition. The proposed system is implemented with MATLAB 7.8.0.347(R2009a) using dataset from CASIA Iris V1 for Iris recognition and FVC 2000 and 2002 DB1 A for fingerprint recognition.

The experiment results carried on datasets from CASIA Iris V1 for Iris recognition and FVC 2000 and 2002 DB1 A for fingerprint recognition. It compares FAR, FRR, and accuracy metrics for Fingerprint standalone recognition system and the multimodal biometric system based on Fingerprint and Iris and shows that the multimodal system results of FAR and FRR are decreased and accuracy is increased compared to the fingerprint standalone system.

References

1. Ross, A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics. Springer- Science + Business Media, LLC (2006)
2. ISO/IEC TR 24722:2007, Information technology biometrics: multimodal and other multibiometric fusion, July 2007
3. Ross A., Govindarajan, R.: Feature level fusion using hand and face biometrics. In: Proceedings of the SPIE Conference Biometric Technology for Human Identification *II*, pp. 196–204, Mar. 2005
4. Singh, S., Gyaourova, A., Bebis, G., Pavlidis, I.: Infrared and visible image fusion for face recognition. In: SPIE Defense and Security Symposium, pp. 585–596 (2004)
5. Heo, J., Kong, S.G., Abidi, B.R., Abidi, M.A.: Fusion of visual and thermal signatures with eyeglass removal for robust face recognition. In: Proceedings of the Joint IEEE Workshop Object Tracking and Classification beyond the Visible Spectrum, June 2004
6. Son, B., Lee, Y.: Biometric authentication system using reduced Joint feature vector of iris and face. In: Lecture Notes in Computer Science vol. 3546, pp. 261–273 (2005)
7. Ross, A., Jain, A.K.: Fusion techniques in multibiometric systems. In: Hammound, R., Abidi, B., Abidi, M. (eds.) Face Biometrics for Personal Identification. Springer, Berlin, Germany (2007)
8. Lanckriet, G.R.G., Ghaoui, L.EI., Bhattacharyya, C., Jordan, M.I.: J. Machine Learning Res. 3, 552 (2002)
9. Verlinde, P., Cholet, G.: Comparing decision fusion paradigms using k-NN based classifiers, decision trees and logistic regression in a multi-modal identity verification application. In: Proceedings of the International Conference Audio and Video-Based Biometric Person Authentication (AVBPA), pp. 188–193, Washington, DC, Mar. 1999
10. Ross, A., Jain, A.K.: Information fusion in biometrics. Pattern Recogn. Lett. **24**(13), 2115–2125 (2003)
11. Jain, A., Hong, L., Kulkarni, Y.: A multimodal biometric system using fingerprint, face and speech. In: Second International Conference on AVBPA, pp. 182–187, Washington, DC, USA (1999)
12. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial gummy fingers on fingerprint systems. In: Proceedings of the SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275–289, Jan. 2002
13. Kittler, J., Hatef, M., Duin, R.P.W., Mates, J.: On combining classifiers. IEEE Trans. Pattern Anal. Mach. Intell. **20**(3), 226–239 (1998)
14. Wang, F., Yao, X., Han, J.: Improving iris recognition performance via multi-instance fusion at the score level. Chin. Opt. Lett. **6**(11), 824–826 (2008)
15. Jain, A.K., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems. Pattern Recogn. **38**(12), 2270–2285 (2005)
16. Bowyer, K.W., Chang, K.I., Flynn, P.J., Chen, X.: Face recognition using 2-D, 3-D, and infrared: is multimodal better than multisample. Proc. IEEE **94**(11), 2000–2012 (2006)
17. Jain, A.K., Ross, A.: Fingerprint mosaicking. In: Proceedings of the International Conference Acoustic Speech and Signal Processing, vol. 4, pp. 4064–4067 (2002)
18. Yao, Y.-F., Jing, X.-Y., Wong, H.-S.: Face and palmprint feature level fusion for single sample biometrics recognitionion. Neurocomputing **70**, 1582–1586 (2007)
19. Benaliouche, H., Touahria, M.: Comparative study of multimodal biometric recognition by fusion of iris and fingerprint. Sci. World J. **2014**, 113 (2014)
20. Chen, X., Flynn, P.J., Bowyer, K.W.: IR and visible light face recognition. Comput. Vis. Image Underst. **99**(3), 332–358 (2005)
21. Han, J., Bhanu, B.: Gait recognition by combining classifiers based on environmental contexts. In: Lecture Notes in Computer Science, vol. 3546/2005, pp. 113–124 (2005)
22. Ratha, N.K., Connell, J.H., Bolle, R.M.: Image mosaicing for rolled fingerprint construction. In: Proceedings of the International Conference Pattern Recognition, vol. 2, pp. 1651–1653 (1998)

23. Chellappa, R., Wilson, C.L., Sirohey, S.: Human and machine recognition of faces: a survey. Proc. IEEE **83**(5), 705–740 (1995)
24. Metawa, N., Elhoseny, M., Kabir Hassan, M., Hassanien, A.: Loan portfolio optimization using genetic algorithm: a case of credit constraints. In: 12th International Computer Engineering Conference (ICENCO), pp. 59–64. IEEE (2016). doi:10.1109/ICENCO.2016.7856446
25. Metawa, N., Hassan, M.K., Elhoseny, M.: Genetic algorithm based model for optimizing bank lending decisions. Expert Syst. Appl. **80**, 75–82 (2017). ISSN 0957-4174. doi:10.1016/j.eswa.2017.03.021
26. Proenca, H., Alexandre, L.A.: UBIRIS iris image database, Dec. 2006. http://iris.di.ubi.pt
27. Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE, Biometrics, Vol. 14, No. 1, January 2004
28. Elhoseny, M., Elminir, H., Riad, A., Yuan, X.: A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. J. King Saud Univ.-Comput. Inf. Sci. (2015)
29. Elhoseny, M., Yuan, X., El-Minir, H.K., Riad, A.M.: An energy efficient encryption method for secure dynamic WSN. Secur. Comm. Netw. **9**, 2024–2031 (2016)
30. Poh, N., Bengio, S., Korczak, J.: A multi-sample multi-source model for biometric authentication. In: Proceedings of the IEEE Workshop Neural Networks for, Signal Processing, pp. 375–384 (2002)
31. Uludag, U., Ross, A., Jain, A.K.: Biometric template selection and update: a case study in fingerprints. Pattern Recogn. **37**(7), 1533–1542 (2004)
32. Bromba, M.U.A.: Bioidentification frequently asked questions. http://www.bromba.com/faq/biofaqe.htm
33. Daugman, J.: Recognizing persons by their Iris patterns. In: Jain, A.K., Bolle, R., Pankanti, S. (eds.) Biometrics: Personal Identification in a Networked Society, pp. 103–121. Kluwer, Norwell, MA (1999)
34. Chinese Academy of Sciences: Institute of Automation. http://biometrics.idealtest.org
35. Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L., Jain, A.K.: FVC2000: Fingerprint Verification Competition, Das, R., Signature Recognition. Keesing J. Doc. Identity, **24** (2007)