Chapter 12
Multimodal Biometric Invariant Fusion Techniques

P. Viswanatham, P. Venkata Krishna, V. Saritha, and Mohammad S. Obaidat

1 Introduction

Recent advancements in technology have given scope for more threats to personal data and national security due to large amount of stored data. The information transmitted through online can be easily hacked and override the authorized user by the hackers. There are many traditional methods such as password-, watermarking-, and cryptography-based systems to protect the data from the hackers. But these methods are not sufficient to handle new generation applications [1–4].

The biometric based authentication was introduced to avoid the brute force attack. Here, the authentication process is performed by the unique physical features of humans like fingerprint [5], iris, retina, hand geometry, etc. They provide high-secured systems than the traditional methods. Initially, the mono-biometric [6] authentication systems were used to authenticate users and secure systems. Fingerprint verification system is the one of the biometric authentication systems that is highly reliable and is being extensively used by forensic experts. Fingerprint applications include entrance control, door-lock applications, fingerprint identification

P. Viswanatham
School of Information Technology and Engineering, VIT University, Vellore, India

P. Venkata Krishna (✉)
Department of Computer Science, Sri Padmavati Mahila Visvavidyalayam, Tirupati, India
e-mail: dr.krishna@ieee.org

V. Saritha
Department of Computer Science and Engineering, Sri Padmavati Mahila Visvavidyalayam, Tirupati, India

M. S. Obaidat
Department of Computer and Information Science, Fordham University, New York, NY, USA
e-mail: m.s.obaidat@ieee.org

M. S. Obaidat et al. (eds.), *Biometric-Based Physical and Cybersecurity Systems*,
https://doi.org/10.1007/978-3-319-98734-7_12

mouse, and fingerprint mobile phones, among others. The biometric fingerprint means allow authorized users access to multiple clinical, financial, and other systems. It also avoids forgery of certificates, conveying of false information, threats, and crimes.

There are three stages in the fingerprint verification system. These are the enhancement, feature extraction, and comparison. Image enhancement is the preprocessing stage where the quality of the edges is improved and contrast level is increased. The poor-quality images will have low-contrast edges and also the boundaries are not well defined which reduce the ratio of FAR and FRR to about 10% [7].

In case of biometrics, the huge number of images needs to be maintained irrespective of the features, as the population is typically high. Hence, an effective compression technique is required in order to utilize the storage space efficiently. But the disadvantage of using the compression technique is loss of data, which leads to inaccurate matching. In this chapter, the Morlet wavelet algorithm is discussed for fingerprint enhancement and compression during the preprocessing stage of fingerprint verification system [8].

Minutiae-based methods [9, 10] and image-based methods [11–13] are the two variations in fingerprint verification systems. Minutiae is defined as the points of interest in the fingerprint. Minutiae are used as features in minutiae-based methods, and the position of the minutiae, their orientation, and type are stored as sets. The disadvantage is that they may not utilize rich discriminatory information and may have high computation complexity, whereas the image-based methods utilize ridge pattern as feature. Tico et al. [14] proposed transform-based method using digital wavelet transform (DWT) features, while Amornraksa et al. [15] proposed using digital cosine transform (DCT) features. These transform methods show a high matching accuracy for inputs which are identical to the one in its own database. However, these methods have not considered the invariance to an affine transform to deal with different input conditions.

To satisfy the variability condition, integrated wavelet and Fourier-Mellin transform (WFMT) [16] using multiple WFMT features is used. However, this scheme is not suitable for all types of fingerprint images since it chooses core point as a reference point.

To overcome these methods, the simple binaries method is introduced to extract the core reference point. The Zernike and invariant moments are calculated from the reference point invariant to translate, rotate, and scale. The feature is evaluated by the range of correlation between the moments, which reduces the number of features required for comparison during authentication. In this, the authentication is performed by single biometric system [11], which results in high error rates when many similar features exist in the database.

In order to overcome the high error rates, the multimodal biometric system has been developed. It means that more than one biometric [17] is used simultaneously in order to authenticate and validate the user as well as to maintain more information for security purpose. The multimodal biometric system leads to having more information for authentication so it takes more time for authentication and consumes

more storage. It results in high complexity, storage, and execution time. The new fused biometric systems have been introduced to solve the above constraints where the features of the multiple biometrics are combined into a single feature and the authentication is performed using predefined threshold value.

The multimodal biometric fusion system leads in an increase in the error rate for authentication due to the more similar features. There are many fusion methods based on decision, score, and feature level that are used in biometric authentication system. These techniques differ upon what biometric information is going to be fused and how the fusing is done. In decision-level fusion techniques [18], the biometric image was divided into equal small squares from which the local binary patterns are fused to single global features pattern. The performance of these techniques leads to 95% of accuracy. The score level fusion technique [19] is fusing the PCA analysis of the face and fingerprint into single identification system, and in this case the error rate reaches more than 11%. The feature level fusion techniques [20] fuse the feature points of the fingerprint and the face and provide 97% efficiency, but none of the previous fusion techniques provide zero error rates.

In this chapter, a new simple and robust fusion technique called the multimodal biometric invariant moment fusion authentication system has been introduced, and it provides better adaptation of genuine and imposter among various test data sets. The fused algorithm gives a single identification decision (data sets) using coefficients which solve the problem of timely constraints and storage space [21]. This approach provides better results than score, feature, and decision-level fusion technique.

2 Multimodal Biometric Invariant Moment Fusion Authentication System

In multimodal biometric system, more than single biometric is used for authentication purpose. Usually, both mono- and multimodal systems perform the two major operations, namely, enrolment and authentication. During enrolment, the distinct information of the biometric is stored in the database which is used for verification. After enrolment, the authentication is performed by comparing the information with the stored information. Depending upon the ratio of similar or non-similar data, the genuine or imposter must be identified.

2.1 Invariant Moment Fusion System

The binaries method extracts the core reference point in which the Zernike and invariant moments are calculated. Translation, rotation, and scaling are performed on invariants. The final features for authentication are evaluated by the range of correlation between the moments to reduce the amount of storage.

2.2 Fingerprint

2.2.1 Morlet Enhancement and Compression

The Morlet fingerprint image enhancement and compression [8] consists of two-stages in processing. They are wavelet analysis and smoothening. In wavelet analysis, the Fourier transforms are applied on the 2D Morlet wavelet and the original image separately. The transformed images are then obtained from these transformed functions. The corrected two-dimensional continuous wavelet transform (2D CWT) is obtained by applying the inverse Fourier transform in the transformed image. During the smoothing process, the orientation and the frequency image [22] of the 2D CWT image are estimated and applied in the Gabor filter in order to remove noise.

The steps involved in the algorithm are as follows:

1. The image is decomposed using Morlet wavelet.
2. Ridge segmentation is done to identify the broken ridges.
3. The ridge orientation is estimated.
4. The frequency is estimated using orientation image.
5. The final image is reconstructed based on adjoining chosen filtered blocks.

2.2.2 Morlet Wavelet

2.2.2.1 2D Continuous Wavelet Transforms

2D CWT is performed by convolving a wavelet function and image. For $f(x, y) \in L_2R$, 2D CWT in time domain is given as:

$$cwt(s, a, b) = \frac{1}{\sqrt{s}} \int\int f(x, y)\psi\left(\frac{x-a}{s}, \frac{y-b}{s}\right) dxdy \tag{12.1}$$

where s is the "dilation" parameter used to change the scale and a, b are the translation parameters used to slide in time. The factor of $s^{1/2}$ is a normalization factor to keep the total energy of the scaled wavelet constant.

The 2D CWT in frequency domain is given as:

$$cwt(s, w_1, w_2) = \sqrt{s}F(w_1, w_2)\Phi(sw_1, sw_2) \tag{12.2}$$

where w_1 and w_2 refer to the frequency of the image, $F(w_1,w_2)$ is the low-frequency spectrum, and $\phi(w_1,w_2)$ is the phase modulation, which defines the spectrum of deformed image. The Fourier transform in Morlet wavelet is applied to the image, which calculates the discrete points depending on the scale and displays the real part of the inverse Fourier transform.

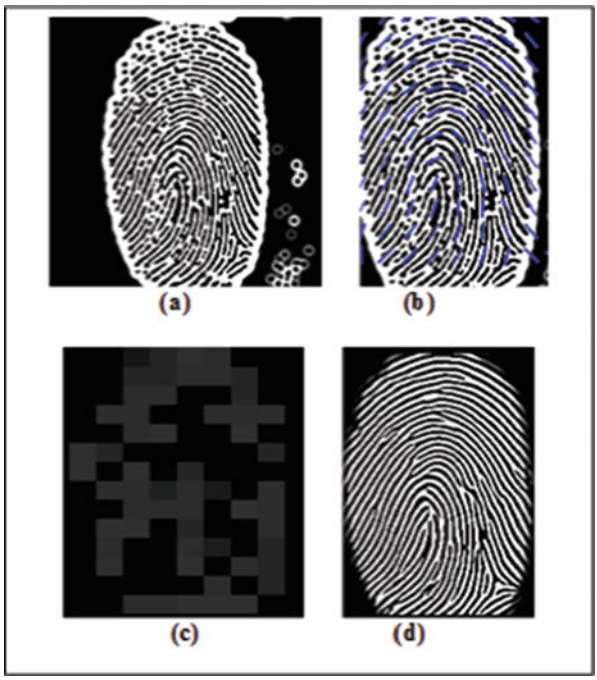

Fig. 12.1 The resultant phases of the enhancement: (**a**) Morlet image, (**b**) orientation image, (**c**) frequency image, and (**d**) enhanced image

$$\psi(kx, ky) = \sqrt{2\pi}\left(e^{-\frac{1}{2}(2\pi kx-k)+(2\pi ky)^2} - e^{-\frac{1}{2}k^2\psi}\right)e^{-\frac{1}{2}\left(2\pi kx^2+2\pi ky^2\right)} \tag{12.3}$$

The decomposition of the fingerprint image by 2D Morlet wavelet is shown in Fig. 12.1a. The resultant transformed image has good contrast and enhanced ridges with compression.

2.2.3 Ridge Orientation

The orientation image represents an intrinsic property of the fingerprint image and defines invariant coordinates for ridges and furrows in a local neighborhood as shown in Fig. 12.1b. A ridge center maps itself as a peak in the projection. The projection waveform facilitates the detection of ridge pixels. The ridges in the fingerprint image are identified with the help of eight different masks. The ridges are separated from the fingerprint image by the following equations:

$$I(x, y) = I(x, y) - \text{mean} \tag{12.4}$$

$$S(x, y) = I(x, y)/\sigma \tag{12.5}$$

where σ is the standard deviation and $I(x, y)$ is an integrated image.

By viewing ridges as an oriented texture, a number of methods have been proposed to estimate the orientation field of fingerprint images [22]. Given a transformed image, N, the main steps for calculating dominant directions are as follows:

1. Divide N into blocks of size w × w.
2. Compute the gradients and apply Gaussian filter G_{xy}. The gradient operators are simple Sobel operators and Gaussian filter is applied as follows:

$$G_{xy} = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{12.6}$$

3. Estimate the local orientation of each block centered at pixel *(i, j)*

$$O(x,y) = \frac{\pi}{2} \times \tan\left(\left(\frac{G_{xy} - G_{yy}}{G_{xy}}\right)/2\right) \tag{12.7}$$

where the degree of smoothening is governed by the variance σ^2.

2.2.4 Frequency Image

The frequency of the fingerprint image is estimated using the orientation image $O(x, y)$ by Eq. 12.7, and it is shown in Fig. 12.1c. The block is rotated and cropped based on the orientation. The median filtering is then applied for smoothening.

$$F(x,y) = \frac{F(u,v)W(u,v)I(u,v)}{W(u,v)I(u,v)} \tag{12.8}$$

where $W(u,v) = \frac{u}{\sqrt{2}}, \frac{v-\frac{u}{\sqrt{2}}}{2}$

$F(u, v)$ is the wavelet transformed image and $I(u, v)$ ensures that the valid ridge frequency is non-zero. The ridge of 3–25 pixels is the valid range.

2.2.5 Enhanced Image

The Gabor filter optimally captures both local orientation and frequency information to smoothen the fingerprint image. By tuning a Gabor filter to specific frequency and direction, the local frequency and orientation information can be obtained, which will be used for extracting texture information from images, which gives smoothing as a part of enhancement by removing the noise shown in Fig. 12.1d.

$$E(x,y) = \frac{1}{2\pi\sigma_x\sigma_y} e^{\left[-\frac{1}{2}\left(\left(\frac{x^2+y^2}{\sigma_{x,y}^2}\right)/2\right)\cos 2\pi fx\right]} \tag{12.9}$$

where σ_x and σ_y determine the shape of the filter envelop and f represents the frequency of the image.

2.2.6 Determination of Reference Point and Regions of Interest (ROI)

The reference point is determined in order to evaluate the ROI of the fingerprint image, which are used to extract the Zϕ moments. This process simplifies the process of the extraction by reducing its complexity.

The Otsu method is used to define the threshold to the binaries of the image. Intra-class variance is defined as a weighted sum of variances of the two classes:

$$\sigma_\omega^2(t) = \omega_1(t)\sigma_1^2(t) + \omega_2(t)\sigma_2^2(t) \tag{12.10}$$

Weights ω_1 and ω_2 are the probabilities of the two classes separated by the threshold of variance and ${\sigma_1}^2 and\ {\sigma_2}^2$ variances of these classes, respectively. Minimizing the intra-class variance is the same as maximizing interclass variance:

$$\sigma_b^2(t) = \sigma^2 - \sigma_\omega^2(t) = \omega_1(t)\omega_2(t)[\mu_1(t) - \mu_2(t)]^2 \tag{12.11}$$

which is expressed in terms of class probabilities ω_I and class means μ_i. The class probability ω_i(t) is computed from the histogram t:

$$\omega_i(t) = \sum_{i=0}^{t} p(i) \tag{12.12}$$

while the class mean $\mu_i(t)$ is:

$$\mu_i(t) = \left[\sum_{i=0}^{t} p(i)x(i)\right] / \omega_i \tag{12.13}$$

where $x(i)$ is the value at the center of the i^{th} histogram. Similarly, we can compute $\omega_2(t)$ and $\mu_2(t)$ on the right-hand side of the histogram.

The algorithm to binaries detects and crops the ROI of fingerprint:

1. Compute histogram(t) and probabilities of each intensity level
2. Set up initial$\omega_i(0)$ and $\mu_i(0)$.
3. For $t = 1$ to maximum intensity, do:

3.1 Update ω_i and μ_i
3.2 Compute ${\sigma_b}^2(t)$ using Eq. 12.11
3.3 Thresholds ${\sigma_{b1}}^2(t)$ greater and ${\sigma_{b2}}^2(t)$ equal or minimum is defined

$$\text{Threshold } T = \frac{\sigma_{b1}^2(t) + \sigma_{b2}^2(t)}{2} \tag{12.14}$$

$$\text{Binaries image } E_b(x,y) = \begin{matrix} 1 \text{ if } E(x,y)>T \\ 0 \text{ if } E(x,y)>T \end{matrix} \tag{12.15}$$

4. The region labeled with four connected components is chosen which determines the high curvature region used to determine ROI.
5. The median of the region is taken as reference point, and image is cropped into size of 120 × 120. It is shown in Fig. 12.2.

2.2.7 Invariant and Zernike Moment Analysis

The algebraic invariants and Zernike moment are calculated from the reference point of the fingerprint and are invariant to scale, position, and rotation. Algebraic invariants are applied to the moment generating function under a rotation transformation. Nonlinear centralized moment and absolute orthogonal moment invariants are calculated with reference. Fingerprint ZΦ invariants [18] are shown in Table 12.1.

Fig. 12.2 The resultant phases of the fingerprint enhancement with singular point detection

Table 12.1 Fingerprint Zϕ invariants

Data sets	Train image database						
Fing1	6.6739	24.1707	30.6781	30.3368	66.175	42.5687	60.8585
Fing2	6.6439	21.8419	26.9747	30.2023	60.5443	41.5152	58.8209
Fing3	6.6444	14.9212	28.2185	28.0322	57.1951	35.5803	58.8439
Fing4	6.5548	14.7008	29.5278	28.9722	59.2708	37.7285	58.6214
Fing5	6.6496	23.3503	30.7699	31.9627	64.0907	48.2492	63.8234
Fing6	6.6524	23.6642	30.9556	30.0366	62.4862	43.1547	60.855

Invariant Moments

Central moments of order 3 or less are for translational invariance. For a 2D continuous function $f(x, y)$, the moment of order $(p + q)$ is defined as:

$$m_{0,0} = \sum_{i,j=1}^{n} f \quad \bar{x} = \frac{m_{1,0}}{m_{0,0}} \bar{y} = \frac{m_{0,1}}{m_{0,0}} m_{1,0} = \sum_{i=1}^{n} x \cdot f$$

$$m_{0,1} = \sum_{j=1}^{n} y \cdot f m_{1,1} = \sum_{i,j=1}^{n} x \cdot y \cdot f$$

$$m_{2,0} = \sum_{i=1}^{n} x^2 \cdot f m_{0,2} = \sum_{j=1}^{n} y^2 \cdot f m_{1,2} = \sum_{i,j=1}^{n} x \cdot y^2 \cdot f m_{3,0} = \sum_{i=1}^{n} x^3 \cdot f m_{0,3}$$
$$= \sum_{j=1}^{n} y^3 \cdot f m_{2,1} = \sum_{i,j=1}^{n} x^2 \cdot y \cdot f$$

Second-order central moment for image orientation for scaling invariant:

$$\xi_{1,1} = \frac{\left(m_{1,1} - \bar{y} \cdot m_{1,0}\right)}{m_{0,0}^2} \xi_{2,0} = \frac{\left(m_{2,0} - \bar{x} \cdot m_{1,0}\right)}{m_{0,0}^2} \quad \xi_{0,2} = \frac{\left(m_{0,2} - \bar{y} \cdot m_{0,1}\right)}{m_{0,0}^2}$$

$$\xi_{3,0} = \frac{\left(m_{3,0} - 3\bar{x} \cdot m_{2,0} + 2 \cdot \bar{x}^2 \cdot m_{1,0}\right)}{m_{0,0}^{2.5}} \quad \xi_{0,3} = \frac{\left(m_{3,0} - 3\bar{y} \cdot m_{0,2} + 2 \cdot \bar{y}^2 \cdot m_{0,1}\right)}{m_{0,0}^{2.5}}$$

$$\xi_{2,1} = \frac{\left(m_{2,1} - 2\bar{x} \cdot m_{1,1} + \bar{y} \cdot m_{2,0} + 2\bar{x}^2 \cdot m_{0,1}\right)}{m_{0,0}^{2.5}}$$

$$\xi_{2,1} = \frac{\left(m_{1,2} - 2\bar{y} \cdot m_{1,1} - \bar{x} \cdot m_{0,2} + 2\bar{y}^2 \cdot m_{1,0}\right)}{m_{0,0}^{2.5}}$$

A set of seven invariant moments derived from the second and third moments is a set of absolute orthogonal moment invariants proposed by Hu [23].

Rotational invariant moments: $\varphi(1) = \xi_{2,0} + \xi_{0,2}$.

Moment of inertia (pixel intensity to physical density for rotation invariant).

$$\varphi(2) = \left(\xi_{2,0} + \xi_{0,2}\right)^2 + \left(4\xi_{1,1}^2\right) \varphi(3) = \left(\xi_{3,0} - 3\xi_{1,2}\right)^2 + \left(3\xi_{2,1} - \xi_{0,3}\right)^2 \varphi(4)$$
$$= \left(\xi_{3,0} - \xi_{1,2}\right)^2 + \left(\xi_{2,1} + \xi_{0,3}\right)^2$$

$$\varphi(5) = (\xi_{3,0} - 3\xi_{1,2})(\xi_{3,0} + \xi_{1,2})\left((\xi_{3,0} + \xi_{1,2})^2 - 3(\xi_{2,1} + \xi_{0,3})^2 + (3\xi_{2,1} - \xi_{0,3})(\xi_{2,1} + \xi_{0,3})\left(3(\xi_{3,0} + \xi_{1,2})^2 - (\xi_{2,1} + \xi_{0,3})^2\right)\right)$$

$$\varphi(6) = (\xi_{2,0} - \xi_{0,2})\left((\xi_{3,0} + \xi_{1,2})^2 - (\xi_{2,1} + \xi_{0,3})^2 + 4\xi_{1,1}(\xi_{3,0} + \xi_{1,2})(\xi_{2,1} + \xi_{0,3})\right)$$

$$\varphi(7) = (3\xi_{2,1} - 3\xi_{0,3})(\xi_{3,0} + \xi_{1,2}) \times \left((\xi_{3,0} + \xi_{1,2})^2 - 3(\xi_{2,1} + \xi_{0,3})^2\right) + (3\xi_{1,2} - \xi_{3,0})(\xi_{2,1} + \xi_{0,3})\left(3(\xi_{3,0} + \xi_{1,2})^2 - (\xi_{2,1} + \xi_{0,3})^2\right)$$

Skew invariants distinguish between mirror and identical images.

Zernike Moments

The Zernike moment is a set of complex polynomials $\{V_{\mathrm{nm}}(x,y)\}$, which form a complete orthogonal set over the unit disk of $x^2 + y^2 \leq 1$ from the polynomial in polar coordinates, where n is the +ve integer or 0, n-$|m|$ is even, $|m| \leq n$ and $\theta = \tan(y/x)$.

The radial polynomial:

$$R_{nm}(r) = \sum_{s=0}^{(n-|m|)/2} \frac{(-1)^s (n-s)!}{s!\left[\frac{n+|m|}{2} - s\right]!\left[\frac{n-|m|}{2} - s\right]!} r^{n-2s} \tag{12.16}$$

The Zernike moment is:

$$Z_{\mathrm{nm}}(x,y) = \frac{n+1}{\pi} \sum_{x=0}^{N} \sum_{y=0}^{M} f(x,y) V_{n,-m}(x,y) \tag{12.17}$$

2.3 Face Fusion System

The architecture of the face fusion system is shown in Fig. 12.3. The eigen faces are extracted from the face and used for authentication [17]. Initially, the mean and difference of each image in the training set is computed by using Eqs. 12.18 and 12.19. Then the entire centralized image T is merged using mean to obtain the result A. The merged value is used for computing the surrogate covariance matrix L using

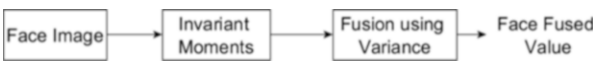

Fig. 12.3 Block diagram of face fusion

Table 12.2 Face Zϕ invariants

Data sets	Train image database					
Face 1	−0.0861	0.0292	0.2199	0.0595	−0.1391	−0.0263
Face 2	0.1025	−0.0871	0.0046	0.0363	−0.1580	0.0161
Face 3	−0.0021	−0.2707	0.0512	−0.0392	0.0847	0.2199
Face 4	0.3195	−0.0552	0.1880	−0.3034	−0.1184	−0.1025
Face 5	−0.3618	−0.0130	0.3020	−0.2350	0.4339	−0.2700
Face 6	−0.4902	0.8825	−0.2266	−1.0756	−0.1895	1.0297

Eq. 12.20. The diagonal elements of covariance matrix are taken as eigen faces using Eq. 12.21. Eigen elements are sorted and are eliminated if their values are greater than 1. Finally, the six invariant features are extracted from the faces using Eq. 12.22.

The high dimensionality makes a good face recognition algorithm. The sample tested face features fusion is shown in Table 12.2.

$$\text{mean} = \frac{1}{n}\sum_{i=1}^{n} X_i \tag{12.18}$$

$$A_i = T_i - \text{mean} \tag{12.19}$$

$$L = A' \times A(X_i - \text{mean}) \tag{12.20}$$

$$[V \times D] = \text{Eig}(L) \tag{12.21}$$

$$\text{Variant} = L \times A \tag{12.22}$$

2.3.1 Fusion

The data sets are independently computed by the described variants of face and fingerprint [18]. The variation distance of the moments is calculated using Eqs. 12.23 and 12.24. It is used for enrolment and comparison during authentication.

$$d_1 = \mu(\varphi_i), \mu(\sigma(\varphi_i)), \mu\left(\sigma^2(\varphi_i)\right), \frac{\mu(\varphi_i)}{\mu(\sigma(\varphi_i))} \tag{12.23}$$

$$d_2 = \mu(Z_i\varphi_i), \mu(\sigma(Z_i\varphi_i)), \mu\left(\sigma^2(Z_i\varphi_i)\right), \frac{\mu(Z_i\varphi_i)}{\mu(\sigma(Z_i\varphi_i))} \tag{12.24}$$

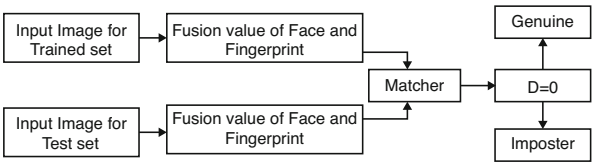

Fig. 12.4 Block diagram of the face and fingerprint fusion authentication

2.3.2 Authentication

The multimodal biometric authentication is one of the new breeds of authentication system performed by means of more than one biometric in order to validate/authenticate the user. The overall architecture of our authentication system is shown in Fig. 12.4. The trained set of inputs in which invariant moment is extracted is fused and enrolled in the database. Now during authentication, the test data input image of fingerprint and face scanned by the user is fused and compared with the fused value in the database. Then matching is performed by calculating the correlation r between the distance d_i of enrolled moments α and verification moments β by Eq. 12.25. The correlation between the fused values computed using Eq. 12.25 and variation using Eq. 12.26 determine whether the user is legitimate or not.

The resultant difference value is compared with the threshold value to validate the user using Eq. 12.22. The threshold value is based upon the sensitivity of the system. If the difference is low, then the similarity will be higher and it crosses the threshold limit to authenticate the user. Otherwise, the user is not authenticated. This multimodal biometric authentication system performed well and provides more than 99% accuracy.

$$r = \frac{2C_{rf}}{C_r + C_f} \text{ where } C_r = \sum_{i=0}^{N} \alpha(i)^2$$

$$C_f = \sum_{i=0}^{N} \beta(i)^2 \text{ and } C_{rf} = \sum_{i=0}^{N} \alpha(i)^2 \beta(i)^2 \tag{12.25}$$

$$D = Fused_{scanned} - Fused_{Enrolled} \tag{12.26}$$

$$A = \begin{cases} \dfrac{100 - D}{100} \times 100 < \text{Th} = \text{Notauthehticated} \\ \dfrac{100 - D}{100} \times 100 > \text{Th} = \text{Authenticated} \end{cases} \tag{12.27}$$

3 Experimental Results

The fingerprint image database used in this experiment is the FVC2002 database, which contains four distinct data set DB1, DB2, DB3, and DB4.

The performance is evaluated in terms of false acceptance rate (FAR) and false reject rate (FRR).

$$FAR = \frac{\text{Number of accepted imposter}}{\text{Total number of imposter}} \times 100 \tag{12.28}$$

$$FRR = \frac{\text{Number of rejected genuine}}{\text{Total number of genuine}} \times 100 \tag{12.29}$$

The FAR means imposter accepted as a genuine user, and FRR means the genuine user is rejected as imposter. They are calculated using the Eqs. 12.28 and 12.29, respectively.

The equal error rate (EER) is used as a performance indicator, which indicates the point where FRR and FAR are equal and for evaluating the performance in terms of recognition rate.

The receiver operating characteristic is used as another performance indicator (ROC). It plots the genuine acceptance rate (GAR = 1-FRR) against FAR. The missing probability and alarm probability are evaluated.

Finally, EER is evaluated and results are shown in Figs. 12.5, 12.6, and 12.7, where it is shown that the performance of the proposed system works well in comparison with other image-based approaches.

The DCT coefficient used by Amorniska in [15] and Jimin [16] used WFMT features; Sha [13] with Gabor filter and Ju [24] with invariants using BPNN are compared, and results shown in Table 12.3 with the proposed method provided more accuracy.

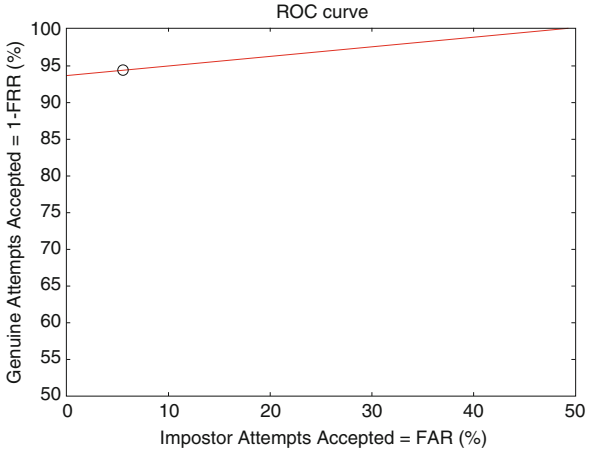

Fig. 12.5 The performance evaluation of the proposed method shows the ROC determines the GAR against FAR

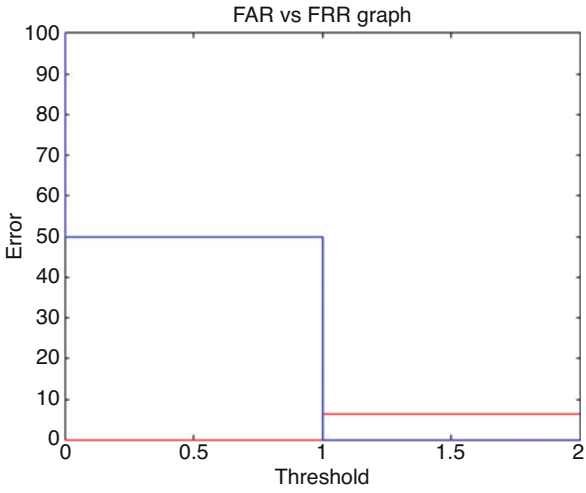

Fig. 12.6 Probability of missing and alarm

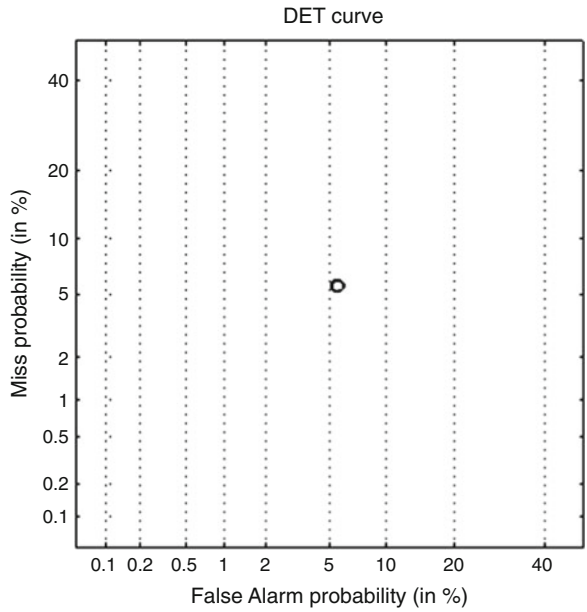

Fig. 12.7 Threshold and the equal error rate (ERR) between FAR vs FRR

Table 12.3 The GAR% against FAR% of the proposed method compared with other methods

Methods	DB1	DB2	DB3	DB4
Amorniska [13]	91.4	85.7	82.1	92.6
Sha [15]	92.7	88.9	85.3	93.2
Jin [14]	94.3	92.4	90.6	94.9
Ju [25]	96.4	95.8	94.2	97.3
Multimodal fusion	98.7	97.2	95	98.2

4 Conclusion

The combined Morlet enhancement with fusion of Zernike and invariant moment features of fingerprint and face is fused by evaluating the distance, mean, and correlation. The combined Morlet enhancement with fusion of Zernike and invariant moment features reduces the storage of features and error rate. The binaries approach using high curvature region accurately determines the reference point used to extract the moments. It is invariant to affine transformations on various input condition. The combined feature maintained for authentication into single identification data reduces the amount of biometric features. The analysis on multimodal biometric using $Z\varphi$ moment's invariant improves the verification accuracy up to 97% as compared to other approaches. The maximum FAR and FRR were maintained at less than 1%. This system demonstrates high reliability, robustness, and good performance in personnel authentication systems.

References

1. M.S. Obaidat, N. Boudriga, *Security of e-Systems and Computer Networks* (Cambridge University Press, Cambridge, UK, 2007)
2. M.S. Obaidat, B. Sadoun, Verification of computer users using keystroke dynamics. IEEE Trans. Syst. Man Cybern. B **27**(2), 261–269 (1997)
3. M.S. Obaidat, B. Sadoun, Keystroke dynamics based identification, in *Biometrics: Personal Identification in Networked Society*, ed. by A. Jain et al. (Springer, Kluwer, 1999), pp. 213–229
4. W. Stallings, *Cryptography and Network Security- Principles and Practices* (Prentice-Hall, Upper Saddle River, 2003)
5. T. Jea, V. Govindaraju, A minutia-based partial fingerprint recognition system. Pattern Recogn. **38**(10), 1672–1684 (2005)
6. T. Jea, V.K. Chavan, V. Govindaraju, J.K. Schneider, Security and matching of partial fingerprint recognition systems. Proc. SPIE **5404**, 39–50 (2004)
7. D. Maio, D. Maltoni, A.K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition* (Springer, Berlin, 2003)
8. P. Viswanathan, P. Venkata Krishna, Fingerprint enhancement and compression method using Morletwavelet. Int. J. Signal Imaging Syst. Eng. **3**(4), 261–268 (2010)
9. S. Prabhakar, J. Wang, A. K. Jain, S. Pankanti, R. Bolle. Minutiae verification and classification for fingerprint matching. In *Proc. 15th International Conference Pattern Recognition*, Vol. 1, Barcelona, September 3–8, 2000, pp. 25–29
10. J. Liu, Z. Huang, K. Chan, Direct minutiae extraction from gray-level fingerprint image by relationship examination. Proc. Int. Conf. Image Process. **2**, 427–430 (2000)
11. P. Viswanathan, P. Venkata Krishna, Morlet Wavelet fingerprint invariant automated authentication system. Int. J. Recent Trends Eng. **4**(1), 1–5 (2010)
12. C. Chen, Decision level fusion of hybrid local features for face recognition. In Neural networks and signal Processing, 2008 International Conference on (pp. 199–204). IEEE (2008).
13. L.F. Sha, F. Zhao, X.O. Tang, Improved finger code for filter bank-based fingerprint matching. Proc. Int. Conf. Image Process. **2**, 895–898 (2003)
14. M. Tico, E. Immonen, P. Ramo, P. Kuosmanen, J. Saarinen, Fingerprint recognition using wavelet features. Proc. IEEE Int. Symp. Circuits Syst. **2**, 21–24 (2001)

15. T. Amornraksa, S. Achaphetpiboon, Fingerprint recognition using DCT features. Electron. Lett. **42**(9), 522–523 (2006)
16. A.T.B. Jin, D.N.C. Ling, O.T. Song, An efficient fingerprint verification system using integrated wavelet and Fourier-Mellin invariant transform. Image Vis. Comput. **22**(6), 503–513 (2004)
17. D. Maio, D. Maltoni, Direct gray scale minutia detection in fingerprints. Trans. PAMI **19**(1), 27–40 (1997)
18. P. Viswanathan, P. VenkataKrishna, Multimodal biometric invariant moment fusion authentication system. Information Management Processing, BAIP 2010, Springer CCIS, vol 70, 2010, pp. 136–144
19. G.L. Marcialis, F. Roli, Score-level fusion of fingerprint and face matchers for personal verification under "stress" conditions. In *14th International Conference on Image Analysis and Processing (ICIAP 2007)* 0-7695-2877-5/07 $25.00 © 2007 IEEE
20. A. Rattani, D.R. Kisku, M. Bicego, M. Tistarelli, Feature level fusion of face and fingerprint biometrics 978-1-4244-1597-7/07/$25.00 ©2007 IEEE
21. T.-Y. Jea, V. Govindaraju, A minutia-based partial fingerprint recognition system. Pattern Recogn. **38**(10), 1672–1684 (2005)
22. C.I. Watson, G.T. Candela, P.J. Grother, Comparison of FFT fingerprint filtering methods for neural network classification. NISTIR **5493** (1994) Available: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=900727
23. M.K. Hu, Visual pattern recognition by moment invariants. IRE Trans. Info. Theory **IT-8**, 179–187 (1962)
24. J.C. Yang, D.S. Park, Fingerprint verification based on invariant moment features and nonlinear BPNN. Int. J. Control. Autom. Syst. **6**(6), 800–808 (2008)
25. L. O'Gormann, J.V. Nickerson, An approach to fingerprint filter design. Pattern Recogn. **22**(1), 29–38 (1989)