Applied Intelligence (2020) 50:1086–1099
https://doi.org/10.1007/s10489-019-01579-1

Quality based adaptive score fusion approach for multimodal biometric system

Keshav Gupta[1] · Gurjit Singh Walia[2] · Kapil Sharma[3]

Published online: 17 December 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract
Multimodal Biometric Systems are extensively employed over unimodal counterparts for user authentication in the digital world. However, the application of multimodal systems to security-critical applications is limited mainly due to non-adaptiveness of these systems to the dynamic environment and inability to distinguish between spoofing attack and the noisy input image. In order to address these issues, a multimodal biometric system, which adaptively combines the scores from individual classifiers is proposed. For this, three modalities viz. face, finger, and iris are used to extract individual classifier scores. These classifier scores are adaptively fused considering that concurrent modalities are boosted and discordant modalities are suppressed. The conflicting belief among classifiers is resolved not only to achieve optimum fusion of classifier scores but also to cater dynamic environment. The proposed quality based score fusion also distinguish between spoofing attacks and noisy inputs as well. The performance of the proposed multimodal biometric system is experimentally validated using three chimeric multimodal databases. On an average, the proposed system achieves an accuracy of 99.5%, an EER of 0.5% and also outperforms state-of-the-art methods.

Keywords Image quality · Adaptive score fusion · Multimodal biometric

1 Introduction

Identity confirmation is very critical in today's digital world. Traditional pin and password methods are becoming obsolete day by day as it is easier to break them with an increase in technology. To address this, biometric systems which use people′s traits like face, fingerprints are considered a more appropriate solution in terms of robustness, reliability, and accuracy. Biometric systems using only a single modality like a fingerprint, face, etc. are known as unimodal systems. Unimodal systems possess different issues such as non-universality, intra-class variations, noise in input data, spoof attacks, and distinctiveness.[1]. These issues are limitedly handled by multimodal systems which combines information from multiple biometric modalities [1, 2]. However, with an increase in the number of identity frauds, a robust and reliable authentication system is required which can cater to security and privacy concerns.

In multimodal biometric systems, information obtained from multiple biometric traits is fused together using various techniques such as score level fusion, feature level fusion, and decision level fusion. [1, 2]. Fusion can be performed in serial and parallel modes. Researchers have worked on multimodal biometric systems at different fusion levels to show their efficiency over other traditional methods. For instance, Hossain et al. [3] proposed a serial fusion approach over face and iris modality. Here, multiple classifiers were arranged in a serial mode using 'best to worst' approach. On the other hand, Yang et al. fused the features of finger vein and fingerprint modalities to generate a more discriminative feature [4]. Although the feature set contains the highest amount of information, incompatibility

✉ Kapil Sharma
kapil@ieee.org

Keshav Gupta
keshavgupta101@gmail.com

Gurjit Singh Walia
gurjit.walia@gmail.com

1 Department of Computer Science, Delhi Technological University, New Delhi 110042, India

2 Defence Research and Development Organization, Ministry of Defence, New Delhi 110054, India

3 Department of Information Technology, Delhi Technological University, New Delhi 110042, India

in type and dimension of features extracted from different modalities limits the application of feature level fusion. Generally, score level fusion is used to overcome the issues of feature level fusion. For example, Peng et al. proposed a t-norm based score level fusion method which combined various classifier scores to generate a final score [5]. The score fusion provided a trade-off between ease of use and efficiency. Fusion can also be performed at the decision level. For instance, Prabhakar and Jain worked in combining the results of four different fingerprint matching algorithms [6]. Fusion at the decision level is quite inflexible because of low information available and choice of the classifier. The most commonly used approach is fusion at score level due to low computation complexity and sufficient information content to discriminate [1, 2]. Biometric systems generally face challenges from spoof attacks where a fake biometric sample is used for illegitimate access. Apart from this, the computed match score highly depends on the quality of the input probe image.[7] Degraded environmental conditions or faulty devices used to capture the biometric feature may result in a poor match score for a genuine individual. This may result in poor performance of the biometric system.

To address the issue of spoofing attacks, Singh et al. [8] proposed an antispoofing technique for face recognition. The method presented identified face liveliness with morphological operations. For fingerprint spoof detection, Kho et al. [9] presented an incremental method based on SVMs and dynamic weight update procedure. Similarly, in order to address iris spoof attacks, Kaur et al. [10] presented an antispoofing method based on orthogonal features. Mostly, anti-spoof methods used feature specific properties of biometric traits to handle spoof attacks and may not be suitable for multimodal systems as it requires a more generic approach to handle spoof attacks.

While capturing input image, dynamic environmental conditions and other faulty feature-capture mechanisms introduce noise. This results in degradation of overall image quality. Poor quality images will generate a low match score and the biometric system's performance is degraded. Harin et al. [7] proposed a face recognition system to handle varying lighting conditions. Nathan et al. [11] proposed a unimodal biometric system using iris modality to deal with environmental issues as well as faulty device issues. Similarly, Pisani et al. [12] proposed an adaptive biometric system that deals with changing biometric feature over time, but a comprehensive solution which addresses all these issues simultaneously was not investigated. In order to resolve these issues, an adaptive multimodal system is required which not only handle poor environmental conditions like improper lighting or sweating fingers but also robust to spoofing attacks.

This paper presents an adaptive multimodal biometric system incorporating reliability factors for each modality. The reliability factor is estimated using image quality which can be a decisive factor in identifying fake biometric. The proposed technique addresses various issues simultaneously and works efficiently for multimodal systems. Few key points of the proposed method are summarised below.

- An adaptive multimodal biometric system using score fusion technique is proposed having three complimentary modalities namely fingerprint, iris and face. Multimodal systems highly decrease the chances of a successful spoof attack.
- Boosting of concurrent classifier scores and suppression of discordant classifier scores is performed simultaneously. This approach creates a clear and distinguished decision-boundary between an imposter and a genuine class.
- The reliability factor is calculated using no-reference quality measurement techniques for each modality. This not only adds to its adaptive nature but also makes it more robust under a dynamic environment and against spoof attacks.
- The proposed method is experimentally validated over three multimodal chimeric datasets generated using benchmarked images. The results depict high performance, low error rate and better detection of fake biometrics as compared to state of the art techniques.

The paper organization is as follows:

Related work in the field of the multimodal biometric system with a focus on the state-of-the-art score fusion methods are discussed in Section 2. The overview of the architecture of the proposed biometric system and details about the proposed score level fusion technique is discussed in Section 3. Section 4 contains the details of datasets used, qualitative and quantitative performance assessment of the proposed technique and exhaustive result analysis for the proposed biometric system. Section 5 draws the final conclusion and future directions.

2 Related work

Recently, multimodal biometric systems are extensively investigated for achieving robust and reliable solutions. In this section, we explicitly reviewed recent literature which is closely related to our work. Generally, biometric features can be combined at various levels such as feature level, score level and at the decision level. Combining similarity scores evaluated from different biometric traits is considered a suitable approach as it not only increases the reliability of the results but also reduces the overall complexity. There are various score fusion techniques proposed by researchers. For example, in [5], T-norms were used to fuse matching scores evaluated from multiple hand modalities like finger knuckle print, palm print, finger vein, and fingerprint. Evaluated scores were also normalized and score fusion was performed using different T-norms. Similarly, Nanni et al. [13] used statistical and machine learning approaches for a combination of various fingerprint matchers on 4 FVC2006 databases. Authors investigated various score level fusion algorithms to check the best approach for score fusion and correlation among multiple fingerprint classifiers. In [14], authors proposed a multiple-instance score fusion using a finger-knuckle print of 4 different fingers. Match scores were first normalized and then fused together to reach a final decision. Also, Tao and Veldhuis [15] presented a score level fusion method using likelihood ratio under the assumption of Naïve Bayes. The likelihood ratio was estimated via operation points on ROC. Results were evaluated over the Face Recognition Grand Challenge (FRGC) 2D-3D face database. However, the traits used to distinguish between various users were limited to a single body part, these methods mostly suffered from universality problem.

To resolve the issue of universality, traits belonging to multiple regions were adopted. For instance, in [16], iris and facial features were fused at score level. In this, weights were assigned to individual scores from classifiers and a weighted score level fusion was performed. The fused score is used to take the final decision. Similarly, Sim et al. [17] presented a score fusion technique to combine similarity scores from the face and iris biometric traits. The experiments were performed on self-made "Universiti Teknologi Malaysia Iris and Face Multimodal Datasets" (UTMIFM) dataset along with the ORL face database and UBIRIS version 2.0 database. Also, Mukherjee et al. [18] proposed a novel fusion technique where different similarity scores were mapped to a single amalgamated match score for decision making. Parameters were tuned using differential evolution (DE) to reduce the overlapping of genuine and imposter score distribution area in a frequency distribution plot. Results were evaluated over two databases each having four different modalities viz. iris, fingerprint, left and right ear. Further, Liang et al. [19] presented a probabilistic score fusion algorithm which cast the fusion into an optimization problem having a natural order-preserving constraint. The effectiveness of the algorithm was demonstrated on two databases viz NIST-BSSR1 and XM2VTS-benchmark respectively. In [20], a hybrid approach using both score and decision level fusion was followed. Scores from individual classifiers were fused using Mean-closure weighting (MCW) and a decision was made based on DS theory over 3 virtual multimodal databases. In [21], a score fusion technique which combined scores from iris and face modalities was proposed. The authors deployed a fuzzy C-means clustering with level set (FCMLS) method to effectively localize iris images improving the overall results. Also, Liau and Isa [22] used support vector machines(SVM) to perform weighted score level fusion of optimized face and iris feature scores. However, the issue of conflicting match scores and the optimal combination was limitedly addressed among the techniques.

Nandakumar et al. [23] proposed an optimal match score fusion technique on the basis of a likelihood ratio test. A finite Gaussian mixture model was created using genuine and impostor score distribution. Experiments were conducted on 3 publicly available datasets NIST-BSSR1, XM2VTS-benchmark and WVU database. To resolve the conflict among classifier scores, Walia et al. [24] proposed a score fusion technique using PCR-6 with Backtracking Search Optimization. Similarly, Mezai et al. [25] presented a score fusion technique incorporating belief functions for iris and face modality. Authors used Denoeux and Appriou models to convert matching scores into belief assignments and PSO was used to compute the confidence factor. DS theory was then used to combine the masses and PCR-5 to predict the user's class. In [26] authors used graph diffusion technique to secure the biometric template and optimally fuse the individual classifier scores. Also, Kumar and Kumar [27] explored the ability of multimodal systems to adapt to the required security level. An Ant Colony Optimization (ACO) based parameter manipulates various other parameters like threshold, fusion technique, weights, etc. depending upon the given security level. However, the performance of these systems degraded in the presence of noisy input data.

Poh et al. [28] incorporated quality measures in multimodal biometric fusion which determined the reliability of the results given by fusion methods. In this, the quality information was used by Bayesian framework working with discriminative and generative classifiers to improve system's performance. Similarly, in [29], authors proposed a quality-dependent technique for score normalization in order to minimize the performance degradation which arises due to cross-device matching. Further, Shekhar et al. [30] investigated a joint sparse representation including a quality measure for each modality which optimized individual classifier scores. However, the performance for these methods was compromised under a dynamic environment and vulnerable against spoofing attacks.

Generally, multimodal biometric systems provide desired accuracy using fixed rules for combination and security level. But under dynamic conditions and ever-changing environment, the same rules may not be applicable or equally efficient. Keeping this issue in mind, an adaptive multimodal biometric system with score level fusion technique is proposed, which maps the matching scores into different domain by boosting or suppressing their values based on the threshold and security requirements to reach a final decision. The proposed method can effectively distinguish between low-quality images and spoofing attacks. The next section presents a detailed overview of the proposed method.

3 Proposed multimodal biometric system

The architecture of the proposed multimodal biometric system is presented in Fig. 1. In this, three biometric features viz. Iris (i), Face (f), and Fingerprint (p) are fused using the proposed adaptive score level fusion.

Three biometric features are taken as input and corresponding features are extracted. For iris feature extraction, segmentation is done using an improvised hough transform method followed by normalization into rectangular blocks with fixed dimensions using Daugman's model. Finally, phase data extracted from 1-D log Gabor filter is quantized to encode unique pattern into a bit-wise biometric template. For extracting facial feature, Gabor filters are used which explore various visual properties like orientation selectivity, spatial localization, and spatial frequency characteristics. The feature vector is created by convolving the image with Gabor filters. For fingerprint trait, the input image is first enhanced using binarisation and thinning operations. Further, minutiae-based features are extracted from the corresponding image.

Comparison of the query image is performed with the templates stored in database and similarity match scores are obtained as S^i, S^f and S^p for iris, face and fingerprint respectively. These scores are processed and optimally combined using the proposed fusion model. Fusion model comprises of 3 stages: In the first stage, adaptive scores are calculated from the match scores for each modality. In the next stage, confidence and optimization factors are computed and finally score fusion is performed followed by normalization step. Finally, the fused score is compared with a threshold value to reach a decision. The proposed system is adaptive in nature as an adaptive score is calculated depending upon the distance of match score from a threshold value. Also, each modality is assigned with a reliability factor (α) using input image quality which provides unequal priors depending upon the reliability of input features. The following sub-section presents the details of the proposed Multimodal Biometric System.

3.1 Feature extraction and classifier score estimation

Multimodal modalities viz. iris, face, and fingerprint are processed for generic feature extraction and individual classifier scores are determined. For facial feature extraction, we adopted the Gabor filter approach for edge detection [31] due to low complexity, robustness against noise and other photometric disturbances [32]. This method recognizes a particular region of interest by capturing relevant frequency spectrum at specified orientations to extract features [31]. A Gaussian kernel function $\Upsilon_{\nu,\Theta}(x, y)$ is used to modulate

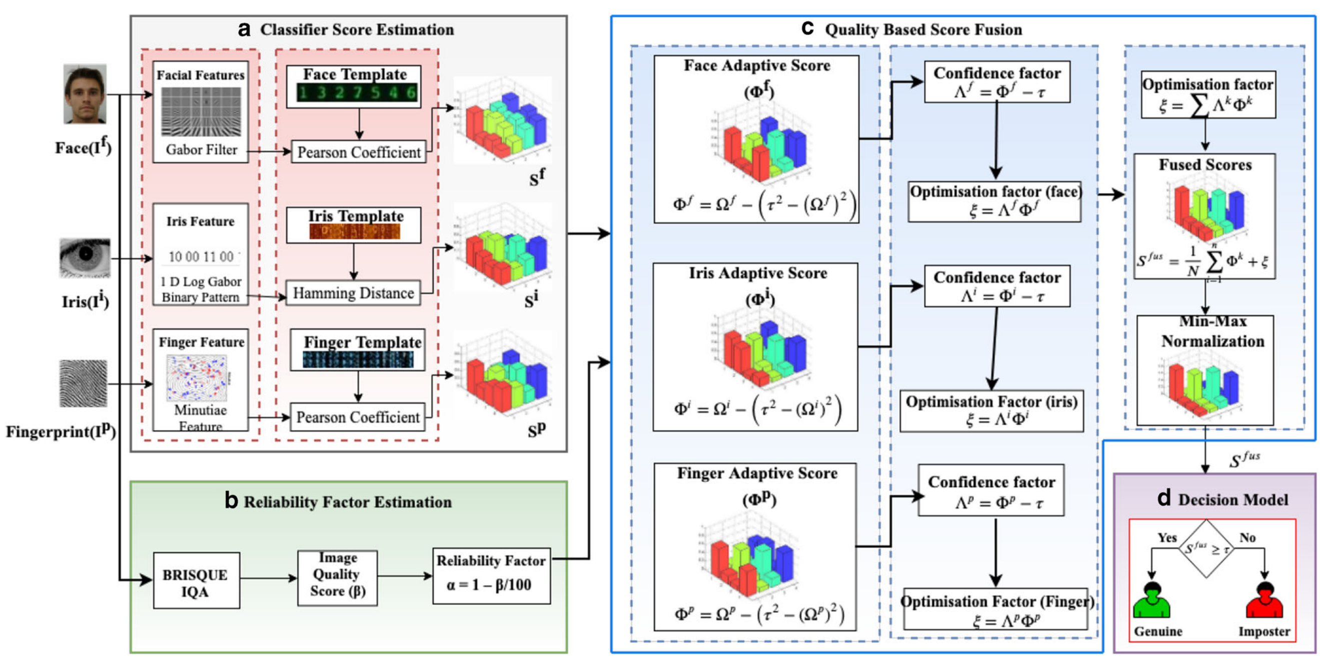


Fig. 1 Overview of the Proposed Multimodal Biometric System. Features from query image are extracted and compared with stored templates to generate individual classifier scores. Combined with reliability factor, scores are fused based on the proposed score fusion method to reach a final decision

the 2-D Gabor filter in form of a complex sinusoidal wave as in (1):

$$\Upsilon_{\nu,\Theta}(x,y)=\exp\left[-\frac{1}{2}\left\{\frac{x_{\Theta_n}^2}{\sigma_x^2}+\frac{y_{\Theta_n}^2}{\sigma_y^2}\right\}\right]\exp\left(2\pi\nu x_{\Theta_n}\right) \tag{1}$$

Where,

$$\begin{bmatrix} x_{\Theta n} \\ y_{\Theta n}\end{bmatrix}=\begin{bmatrix} sin\Theta_n & cos\Theta_n \\ -cos\Theta_n & sin\Theta_n\end{bmatrix}\begin{bmatrix} x \\ y\end{bmatrix} \tag{2}$$

Here, ν is sinusoidal frequency, σ_x , σ_y are standard deviation along x and y direction of Gaussian envelop and Θ_n is the orientation defined in (3):

$$\Theta_n=\frac{\pi}{m}(n-1) \tag{3}$$

For n=1, 2… m where m represents the orientation count. Here, forty Gabor filters are used to convolve input grey facial image I^f in five scales and eight orientations followed by down-sampling by a factor of four to reduce redundancy before concatenating to form a feature vector, η^f which is stored in the database. Similarly, input facial probe image is convolved with Gabor filter bank to extract feature vector, ψ^f. The similarity match score between store template η^f and input probe image ψ^f is computed using Pearson's correlation coefficient using (4):

$$S^f=\frac{cov\left(\eta^f,\ \psi^f\right)}{\sigma_{\eta^f}\sigma_{\psi^f}} \tag{4}$$

where cov calculates the covariance between two vectors and σ represents their standard deviation.

For fingerprint feature extraction, a minutiae-based technique is employed. This technique is widely used by researchers [33, 34] for its high performance, low complexity and its analogy with methods used by forensic experts for fingerprint recognition. In this, input finger image I^p is first pre-processed through binarization and thinning. Binarization increases the contrast between ridges and valleys using (5):

$$B(m,n)=\left\{\begin{matrix} 1, & if\ I(m,n)\geq\ t \\ 0, & otherwise\end{matrix}\right\} \tag{5}$$

Where $I(m,n)$ represents the intensity value at pixel position (m,n) and t is threshold value. Thinning reduces ridges to unit-pixel thickness also known as skeletons and is performed using inbuilt morphological functions on binary images at Matlab platform. Minutiae are located over the thinned image using a 3x3 sliding window in a circular anti-clockwise manner to produce rutovitz crossing number (CN) [34] which defines the type of minutia and can be computed using (6):

$$CN=\frac{1}{2}\sum_{j=1}^{8}|q_j-q_{j-1}| \tag{6}$$

Where q_j represents pixel values of eight neighbors of any pixel q. Depending upon the value of CN, ridge pixel may be classified as isolated, ending, continuing, bifurcation and crossing point. Each minutia is then represented as a vector M=[m,n,CN,θ]. Where, (m,n) represents the coordinates of pixel p and θ is minutia orientation. For input finger image I^p, a feature template, η^p is generated by combining n minutiae using (7):

$$\eta^p=[M_1,M_2,\ldots M_n] \tag{7}$$

Similarly, a feature template, ψ^p for input probe image is generated. For computing the similarity match scores, minutiae are matched based on spatial distance and directional difference and a total number of matching minutiae are computed. Score S^p is computed between the acquired probe image and stored template using (8) as:

$$S^p=\frac{n_{match}^2}{n_\eta n_\psi} \tag{8}$$

Here, n_{match} represents the number of matching minutiae between two templates and n_η, n_ψ represents the total number of minutiae extracted.

For extracting the iris features, binary templates are generated using Khalil and Chadi [35] method as it improves the speed and accuracy of the iris segmentation process by accepting high quality images which also reduce the recognition error and produce a discriminating feature vector so as to improve the recognition accuracy and computational efficiency. In this, iris segmentation from input image I^i is performed using circular Hough transform [36] which provides center and radius of the iris. Further, the iris segment is normalized into a rectangular block with fixed dimensions using Daugman's rubber sheet model [37]. Additionally, localized iris texture is transformed from Cartesian to polar coordinates and iris texture is mapped in the radial direction using polar coordinates. The normalized iris is convolved with 1D Log-Gabor filter [38] whose frequency response is defined using (9):

$$G(\rho)=\exp\left\{-0.5\times\frac{log\left(\frac{\rho}{\rho_0}\right)^2}{log\left(\frac{\sigma}{\rho_0}\right)^2}\right\} \tag{9}$$

Where ρ_0 represents central frequency and σ provides filter bandwidth. The extracted phase data from this convolution is quantized to four levels corresponding to four different phases. This results in a unique binary pattern, generating iris feature binary template η^i. Similarly, a feature template,

ψ^i for iris probe image is also generated. The similarity between the input query image and the stored template is calculated using hamming distance in (10).

$$HD\left(\eta^i,\ \psi^i\right) = \frac{1}{N}\sum_{j=1}^{n}\eta^i \bigotimes \psi^i \tag{10}$$

The hamming distance calculated between two templates is then converted into matching scores using the radial basis function (RBF) kernel in the range of [0, 1]. Using the RBF kernel, the match score between the input query image and the stored templates is computed as per (11):

$$S^i = exp\left(-\frac{HD\left(\eta^i, \psi^i\right)}{2\sigma^2}\right) \tag{11}$$

The calculated match scores from three modalities S^i, S^f, S^p are passed to the proposed fusion model to generate a fused score. The design of the proposed fusion model is discussed in the next section.

3.2 Quaity based adaptive score fusion

The fusion process is very important in a multimodal biometric system for making a decision. Here, we have proposed an adaptive score level fusion method with reliability factor (α) corresponding to each modality giving unequal priors depending upon the quality of input features. The proposed method performs boosting and suppression of individual classifier scores, which makes it adaptive under dynamic environment and robust against spoofing attacks.

Biometric image samples acquired under a dynamic environment may contain extra added noise. A reliability factor (α) based on image quality is calculated which provides a measure of reliability for each modality. Reliability factor (α) is estimated based on the No-reference quality assessment of input images. For this purpose, Blind/Referenceless image Spatial Quality Evaluator (BRISQUE) is adopted [39] which is used as an image quality metric. Here, Mean subtracted Contrast Normalized (MSCN) image is generated from the intensity image (I) using (12).

$$I_k'(x, y) = \frac{I_k(x, y) - \mu_k(x, y)}{\sigma_k(x, y) + 1} \tag{12}$$

where $k \in \{f, p, i\}$, (x,y) are spatial indices, μ and σ represents the mean and standard deviation respectively. Further, a Generalized Gaussian Distribution (GDD) is applied to obtain changes in coefficients distribution in the noisy image using (13).

$$f_k(x; p, \sigma^2) = \frac{p}{2q_k\Gamma(1/p)}\exp\left(-\left(\frac{|x|}{q}\right)^p\right) \tag{13}$$

where

$$q_k = \sigma\sqrt{\frac{\Gamma(1/p)}{\Gamma(3/p)}} \tag{14}$$

for $k \in \{f, p, i\}$, Γ is the gamma function, p is a shape parameter and σ^2 controls variance. Further, a brisque score is calculated using support vector regression (SVR) model trained on image database having similar distortions. The input image is compared to the SVR model with an RBF kernel providing a score value (β) in a range of 1-100. A low score value indicates a high quality of input image. Poor quality of the input query image suggests a high probability of the input image being fake or synthetic/reconstructed. In such cases, input biometric feature cannot be trusted and the reliability of biometric input image is reduced accordingly as per (15).

$$\alpha_k = 1 - \beta_k/100 \tag{15}$$

for $k \in \{f, p, i\}$, moreover, high quality input biometric feature results in high reliability. Thus, an overall reliability factor (α) is calculated for each biometric trait which denotes the reliability of each subject. This reliability factor (α) is incorporated with individual classifiers match scores (S^k) to generate optimized match scores with unequal priors using (16).

$$\Omega^k = \alpha_k * S^k \tag{16}$$

for $k \in \{f, p, i\}$ representing face, finger and iris modality. Thus, the reliability factor helps to tackle fake biometric features but also various dynamic environmental conditions where one modality is more reliable than any other modality by providing unequal priors. Individual classifier scores are optimized by calculating the adaptive scores (Φ^k) for each modality using (17) as:

$$\Phi^k = \Omega^k - \left(\tau^2 - \Omega^{k^2}\right) \tag{17}$$

where, τ is an optimal threshold value and Ω^k denotes the match scores of individual classifiers for $k \in \{f, p, i\}$ representing the face, finger and iris modality. Further, a confidence factor (Λ) for each modality is calculated from the threshold value using (18) which indicates the score difference from the threshold value. Higher the difference, value of confidence factor will be high for both genuine and imposter scores.

$$\Lambda^k = \Phi^k - \tau \tag{18}$$

Using adaptive score, Φ_i and Confidence factor Λ_i, an Optimisation factor, ξ is computed for each modality as per (19)

$$\xi = \sum_{j=1}^{n}\Lambda^k\Phi^k \tag{19}$$

where n denotes the number of modalities. Optimization factor, ξ helps in determining the level of boosting or suppression to be done for individual match scores. The final fused score is estimated using (20) and is passed to a decision model for classification into genuine or imposter class.

$$S^{fus} = \frac{1}{N}\sum_{i=1}^{n}\Phi^{k} + \xi \tag{20}$$

The proposed score fusion is adaptive in nature as it performs boosting and suppression of individual classifier scores using (17) which helps in creating distinguished decision boundary for genuine and imposter class and robust against spoofing attacks as it incorporates quality based reliability factor using (16).

3.3 Decision model

The fused score is normalized using min-max approach and a final decision is performed using an optimal threshold value (τ) if the normalized fused score is greater than τ, then it is considered as Genuine else imposter. For validation of the proposed method, experiments are performed on three chimeric multimodal datasets generated using benchmark images. The next section provides the details of datasets used and its overall analysis.

4 Experimental validation

The performance of the proposed multimodal biometric system is evaluated over three multimodal databases in both qualitative and quantitative manner. In qualitative analysis, face, fingerprint and iris modalities are combined to generate a final score and are compared with individual classifier match scores. On the other hand, during quantitative analysis, various performance metrics like Decidability Index (DI), Equal Error Rate (EER), and Recognition Index (RI) are determined. In addition, the performance of the proposed score level fusion method is compared with other state-of-the-art methods.

4.1 Database & experimental design

We have obtained our Multimodal datasets from various benchmark datasets to validate our proposed algorithm. These Chimeric datasets are obtained by uniquely combining benchmark datasets namely CAS-PEAL Large-Scale Chinese Face Database [40], Casia-Face version 5.0 (Casia-FaceV5, http://biometrics.idealtest. org/), MCYT Bimodal Database [41], FVC2006 DB1-A fingerprint database [42], Casia iris database (Casia-IrisV1, http://biometrics.idealtest. org/), IITD PolyU iris database [43] and MMU2 iris database [44]. Few Sample images of the mentioned datasets are available in Fig. 2.

CAS-PEAL-R1 face database accommodates a total of 30,863 facial images from 1040 individuals out of which 595 are males and 445 females. The database is captured using 9 cameras to capture facial images with different poses, facial expressions, six accessories, and various lighting and background changes. Casia Face version 5.0 consists of 2500 16 bit color facial images having resolution 640*480 in BMP format of 500 distinct subjects. MCYT fingerprint database is obtained using two different sensors. These sensors namely CMOS-based capacitive capture device, and an optical capture device have a resolution of 500 dpi. Twelve samples with each sensor were captured

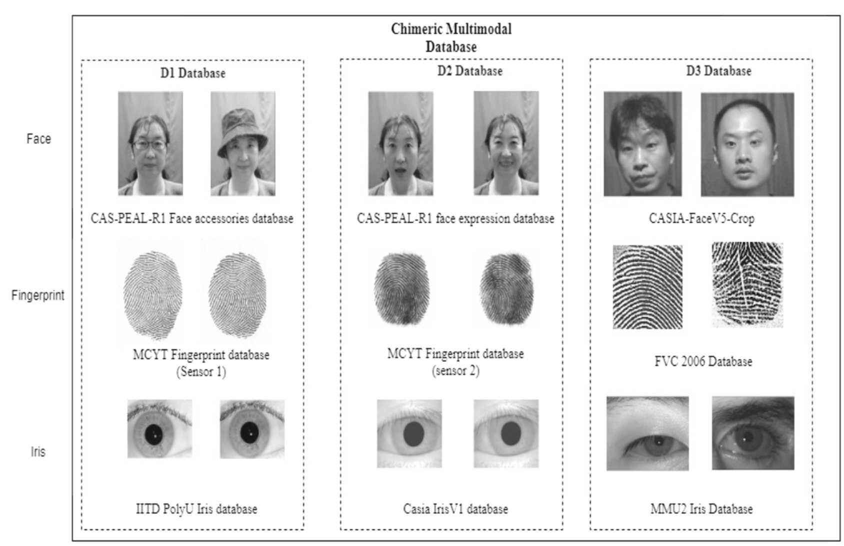


Fig. 2 Sample multimodal database images from the benchmark datasets

for each fingerprint from 330 subjects. Image resolution for captured images is 300x300 for sensor 1 and 256x400 for sensor 2 respectively. FVC2006 DB1-A contains 1680 uncompressed, 256 gray-levels fingerprint images from 140 subjects in BMP format. The images are acquired using an electric Field sensor with image size 96x96 having a resolution of 250 dpi. IITD PolyU iris database images are captured using a digital CMOS camera containing 5 samples from each eye of 224 subjects having a size of 320x 240 pixels. Casia IrisV1 database contains 756 iris images from 108 subjects in two different sessions. All captured images are in BMP format having a resolution of 320*280. MMU2 Iris database consists of 995 iris images in BMP format having resolution 320x238 pixels from 100 volunteers.

Three chimeric datasets are created namely D1, D2 and D3 to validate the proposed multimodal biometric system. D1 contains samples from N distinct subjects from CAS-PEAL-R1 accessories face database, MCYT fingerprint database from sensor 1 and IITD iris PolyU database. A virtual multimodal dataset containing N subjects is created by combining distinct subjects from each of the above-mentioned datasets. Similarly, D2 dataset is created from distinct subjects each from CAS-PEAL-R1 expression face database, MCYT fingerprint database from sensor 2 and Casia IrisV1 iris database and D3 dataset is created from distinct subjects each from Casia V5 face database, FVC2006 DB1-A fingerprint database, and MMU2 iris database. Also, all the subjects are different in D1, D2 and D3 database. In addition, a consolidated multimodal dataset, D4 of 3N subjects is also created by merging all subjects from D1, D2, and D3 databases. Five-fold cross-validation is performed with five different samples considering each sample as input subject once. We have implemented the proposed system on MATLAB 2018a platform with the hardware configuration of 4GB RAM and Intel i3 processor. The next section presents a qualitative analysis of the proposed system.

4.2 Performance metrics

The proposed system's performance is quantitatively analyzed by means of Decidability Index (DI), Equal Error Rate (EER), and Recognition Index(RI). Further, the results are compared with other state-of-the-art fusion methods. During this process, feature extraction and score calculation techniques are kept the same for evaluation of all the methods. Decidability Index (DI) is a performance metric used to quantify the distance between genuine and imposter score distributions and is calculated using (21):

$$DI = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 - \sigma_i^2)/2}} \tag{21}$$

Here, μ_g , μ_i denotes the mean values, andσ_g and σ_i denotes the standard deviation values of genuine and imposter scores distributions, respectively. A high decidability index value suggests a higher ability of the classifier to separate genuine from imposters. Values of decidability index are shown in Table 1 for individual and proposed classifier over chimeric datasets D1, D2, and D3. Equal Error Rate (EER) is calculated by plotting ROC curves where the false acceptance rate (FAR) is plotted against the genuine acceptance rate (GAR). It provides the measure of the accuracy of the proposed biometric system. Recognition Index (RI) provides the recognition rate at rank-1 and can be used for performance evaluation. Cumulative Matching Characteristics (CMC) curves show the relationship between rank and the recognition rate.

4.3 Performance validation

The proposed adaptive multimodal biometric system is validated in a qualitative and quantitative manner. A qualitative analysis of the proposed system is presented in the next section.

4.3.1 Qualitative validation

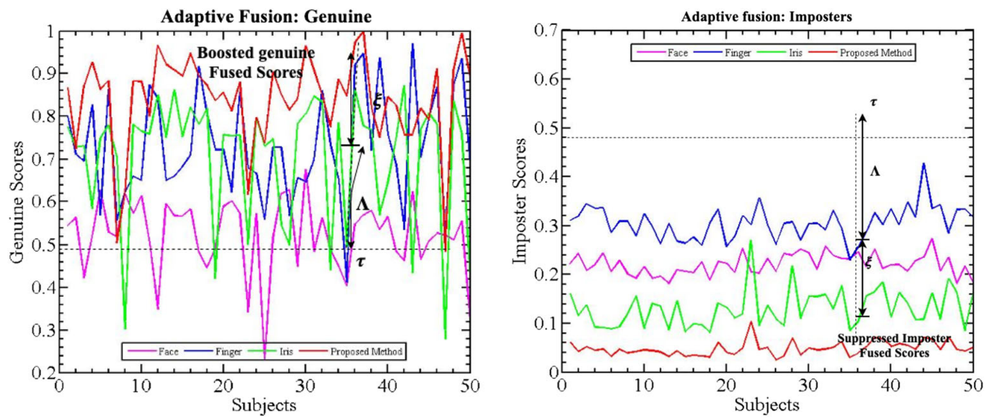
The performance of the proposed adaptive multimodal biometric system is validated over three multimodal databases and scores from individual classifiers are combined together using the proposed fusion method by boosting and suppression of the individual classifier match scores based on optimal threshold τ. For this, an adaptive score is calculated where scores above the optimal threshold are boosted to high values while scores below the threshold are suppressed to lower values. In the next step, a confidence factor (Λ^k) is calculated corresponding to adaptive match scores using (18) such that higher the value of score from the threshold, higher will be the corresponding confidence factor. Similarly, lower score values yield a low confidence factor corresponding to adaptive match scores. Further, an optimization factor is calculated using the confidence factor from individual classifiers. Boosting or suppression is carried out based on the value of the optimization factor which is decided on the basis of combined consensus from individual classifiers. The value of the optimization factor will be high if all three individual classifiers consider the subject to be genuine resulting in a boosted fused score. Similarly, if all individual classifiers consider a subject to be an imposter, a more suppressed fused score is generated as shown in Fig. 3.

Hence, score values change adaptively depending upon their distance from the threshold value. These two steps largely contribute to the boosting and suppression of individual classifier match scores and add to the adaptive

Table 1 Comparison of EER, DI, and RI values for D1, D2 and D3 databases

Method / DB	D3 database			D4 database								
	EER	DI	RI	EER	DI	RI	EER	DI	RI	EER	DI	RI
Face	3.98±0.23	3.88±0.35	95±0.75	2.99±0.19	4.58±0.37	95±0.75	5.01±0.21	4.11 ±0.19	93±0.50	3.33±0.28	4.50 ±0.26	95±0.50
Finger	2.97±0.20	2.77±0.42	89±0.50	3.04±0.24	2.78±0.28	90±0.45	6.02±0.17	2.33±0.31	88±1.00	3.60±0.12	2.19±0.42	90±0.75
Iris	3.47±0.32	4.96±0.42	88±1.11	2.88±0.24	7.51±0.46	88±1.11	4.01±0.25	5.79±0.18	92 ±0.80	3.34 ±0.13	5.61±0.27	91±1.00
Frank t-norm	0.95±0.12	5.46±0.11	98±0.11	0.11±0.08	4.52±0.18	98±0.11	0.92±0.29	4.59±0.22	99±0.20	1.02±0.21	4.18±0.29	98±0.10
PCR5	0.79 ±0.26	5.13±0.16	98±0.31	0.20±0.15	7.98±0.21	99±0.15	0.22±0.17	7.67±0.14	98±0.40	0.69±0.16	6.83±0.15	98±0.20
PCR6 with BSA	0.99±0.22	5.78±0.28	98±0.51	0.78±0.22	7.82±0.18	98±0.35	0.87±0.16	7.56±0.17	99±0.10	0.91±0.23	5.80±0.25	98±0.25
PSO wtd. sum	1.99±0.27	5.17±0.29	97±0.51	0.89±0.27	6.88±0.19	98±0.55	1.06±0.19	6.23±0.12	98±0.45	1.47±0.29	5.61±0.29	98±0.50
Symmetric sum	2.00±0.31	4.93±0.35	95±0.47	1.00±0.23	7.20±0.18	98±0.55	1.14±0.19	4.17±0.13	96±0.75	1.64±0.17	5.12±0.25	96±0.60
Yager t-norm	4.0±0.36	2.62±0.21	90±0.41	4.50±0.31	2.23±0.33	90±0.50	3.50±0.38	2.64±0.25	91±0.60	4.21±0.27	2.57±0.43	90±1.00
Weighted Score Fusion	1.01±0.26	5.11±0.11	97 ±0.45	0.74±0.21	6.36±0.23	97 ±0.50	0.76±0.28	6.16±0.26	97 ±0.50	0.87±0.25	5.39±0.29	97±0.50
Fuzzy Score Fusion	1.08±0.21	4.92±0.24	99±0.50	0.88±0.31	4.18±0.23	95±0.40	2.99±0.27	3.52±0.14	96±0.50	1.65±0.18	2.95±0.34	97±0.45
Proposed Method	0.87±0.14	5.14±0.34	98±0.64	0.11±0.05	7.95±0.43	98±0.64	0.16±0.10	6.71±0.22	99±0.50	0.61±0.16	5.96±0.39	99±0.45

Fig. 3 Comparision of Individual Classifier Scores with fused scores after boosting and suppression of (**a**) Genuine Scores and (**b**) Imposter scores



(a) Genuine Score values

(b) Imposter Score values

nature of the proposed biometric system. Boosting factor calculated from these two steps determines the amount of boosting and suppression to be performed and is used during the final score fusion process. This also leads to a higher separation between the peaks of genuine and imposter score distribution. The score distributions for individual classifiers as well as fusion model are presented in Fig. 4 Reliability factor (α) is also introduced corresponding to every individual input probe image depicting its reliability depending upon the environmental conditions, equipment used, etc. This reliability factor is computed using no-reference image quality scores provided by BRISQUE. If the input probe image possesses high noise, its quality will be low and vice-versa which helps in addressing various environmental challenges.

The frequency distribution of genuine and imposter scores of all 3 individual classifiers shows the smaller distance between peak values. This is generally due to irregularities in captured images, noise, and other environmental conditions. It basically represents a high rate of false acceptance and false rejection with smaller distance resulting in the decreased overall efficiency of the individual classifiers. On the other hand frequency distribution of scores for the proposed biometric system clearly shows the larger distance between Genuine and imposter classes and is also depicted in the quantitative analysis of results obtained.

4.3.2 Quantitative validation

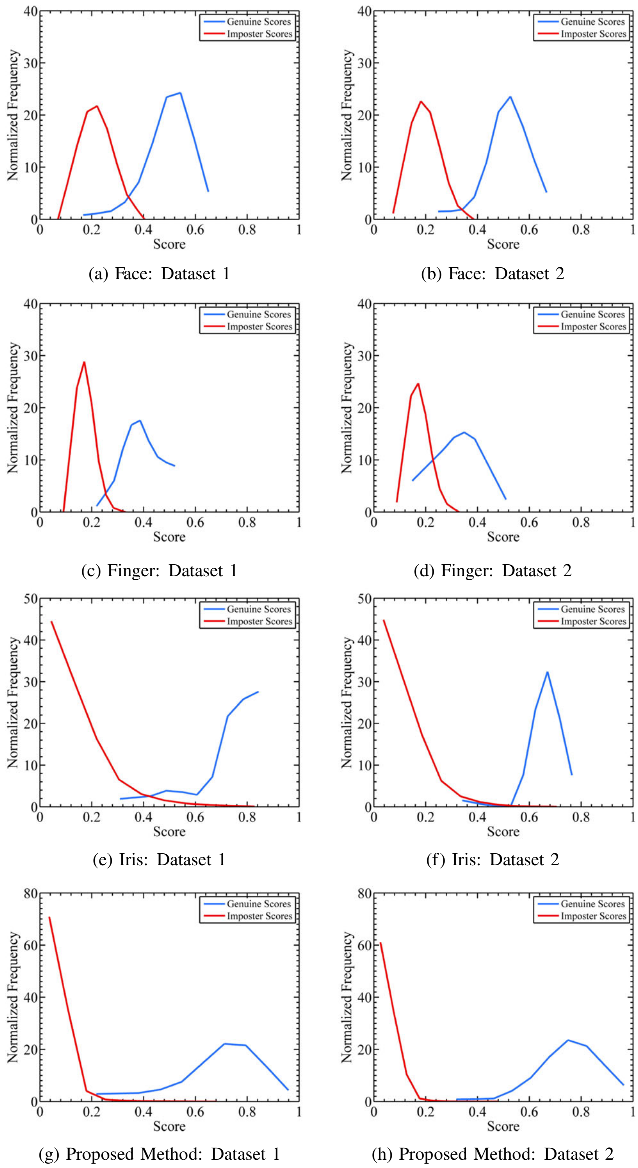
Quantitative analysis of the proposed system is performed on the basis of accuracy analysis, adaptivity analysis, and time-complexity analysis.

Accuracy Analysis The accuracy of the proposed system is analyzed using performance metrics namely EER, DI, and RI. The performance of the proposed method is compared with state-of-the-art techniques using these metrics as well. EER, DI, and RI values for various methods viz. T-norms (2011)[45], score fusion using PCR5 (2018) [46], score fusion using PCR6 with BSA (2019) [24], PSO weighted sum (2009) [47], Symmetric Sum (2018) [48], weighted score fusion (2014) [49] and fuzzy approach based score fusion (2016) [50] are compared with the proposed fusion method in Table 1

The EER value for proposed score level fusion method is 0.87 for D1 database, 0.11 for D2 database, 0.16 for D3 database and 0.61 for consolidated D4 database which is lowest in comparison with other state-of-the-art methods. The efficiency of the proposed system is also depicted by high decidability value of 5.14 for D1 database, 7.95 for D2 database, 6.71 for D3 database and 5.96 for D4 database and supported by ROC and CMC curves in Figs. 5 and 6 respectively. It is due to boosting and suppression of match scores which effectively distinguishes between Genuine and Imposter classes by creating a clear decision boundary. The variation among EER values is due to the use of different datasets and five-fold cross validation.

Quantitative analysis reveals that limitations of individual classifiers were effectively addressed by the proposed fusion method providing higher accuracy and more reliable results. The complimentary traits are fused together making system adaptive to dynamic environmental conditions and robust against spoofing attacks. The Roc curves in Fig. 5 and CMC curves in Fig. 6 shows the proposed fusion method performs better in comparison to single modality as well as other fusion methods.

Adaptivity Analysis To prove the adaptive nature of the proposed system, a new database was created by introducing extra noise to the original database which imitates acquired samples in a dynamic environment and spoofing attacks.



(a) Face: Dataset 1 (b) Face: Dataset 2 (c) Finger: Dataset 1 (d) Finger: Dataset 2 (e) Iris: Dataset 1 (f) Iris: Dataset 2 (g) Proposed Method: Dataset 1 (h) Proposed Method: Dataset 2

Fig. 4 Frequency Distribution Curves for D1 and D2 databases for (**a**) Face images over D1 (**b**) face images over D2 (**c**) Fingerprint images over D1(**d**) Fingerprint images over D2 (**e**) Iris images over D1 (**f**) Iris images over D2 (**g**) Proposed Method over D2 database (**h**) Proposed Method over D2 database

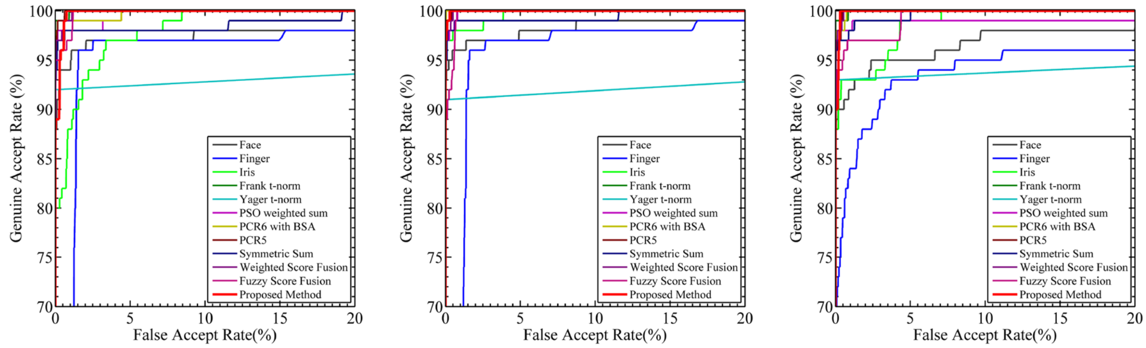
For this purpose, Gaussian noise with $\sigma = 0.05$ and offset $\delta = 0.01$ was introduced in iris and face images while for fingerprint images a Gaussian filter with a standard deviation of 0.4 is used. Sample images from the noise-induced database are shown in Fig. 7

Matching scores were calculated using noisy images as input probe images and the performance of the proposed biometric system was evaluated. During the fusion process, firstly, the noise was introduced in a single modality followed by noise introduction in two modalities and in the end noise was introduced in all three modalities and system's performance was measured in form of EER as tabulated in Table 2.

where $\bar{f}$, $\bar{p}$, $\bar{i}$ represents noisy modality for face, finger, and iris respectively. Low EER values indicate that the proposed system is able to give optimal performance when noise is introduced in one or two modalities. This represents dynamic environmental conditions where the acquired input probe image contains noise. The performance of system exponentially decreases when the input probe images from all three modalities were noisy. This represents a spoofing attack situation where synthetic/reconstructed samples with poor image quality are used. Thus the proposed multimodal biometric system is adaptive in nature withstanding dynamic environmental conditions and robust against spoofing attacks.

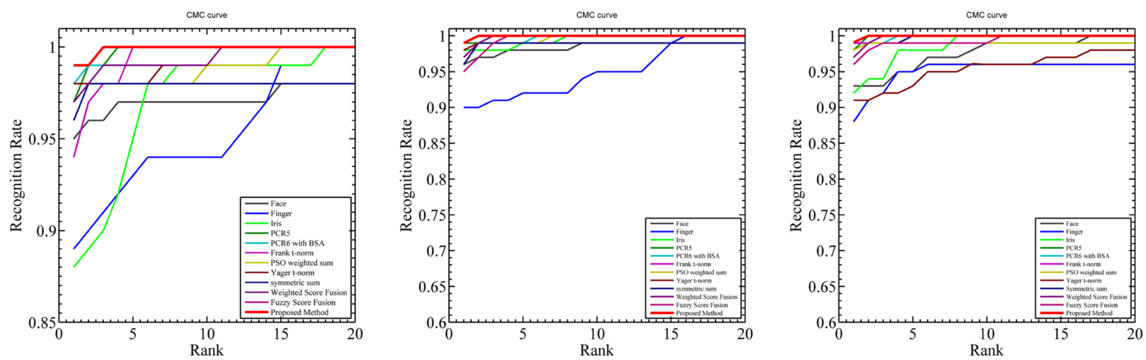
Time Complexity Analysis The computational efficiency of the proposed system is analyzed though time-complexity analysis of score fusion process of various methods. The time taken per subject by the proposed system is compared with other state-of-the-art methods in Table 3. It is evident from the results that the performance of the proposed method is comparable to other methods and better than its unimodal counterparts. The proposed method not only shows high performance but also provided added advantages after incorporating reliability factor.

In sum, the proposed fusion model optimally fuses complementary features making it adaptive to the dynamic environment and robust against spoofing attacks. Various facial distortion, iris off-angle blur, and insufficient boundary information in fingerprints limits the performance of individual classifiers and is also revealed in quantitative analysis. On the other hand, the proposed fusion method not only overcome these limitations by adaptively combining individual classifiers but also makes the system robust against spoofing attacks. An adaptive fusion is performed by boosting and suppression of match scores. Image quality is incorporated which boosts the adaptive nature of the proposed system under dynamic environment and robustness against spoofing attacks as compared with other state-of-the-art methods. The performance of the proposed method is validated with high decidability index, recognition index and low EER value are compared with other state-of-the-art methods. Moreover, lower time complexity makes the proposed system suitable for various real-time industry and security application. Hence, the proposed system shows improved performance along with adaptivity under dynamic environment and robust against spoofing attacks.



(a) D1 Database (b) D2 Database (c) D3 Database

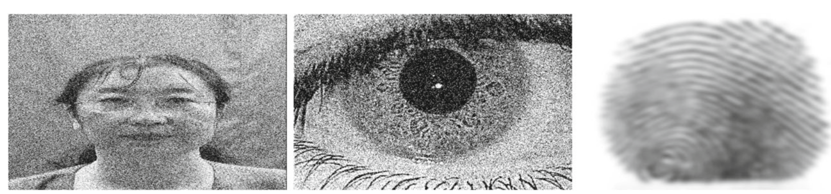
Fig. 5 Performance comparision of evaluated methods: ROC curves for D1, D2 and D3 database (**a**) ROC curves for various fusion techniques over Database D1 (**b**) ROC curves for various fusion techniques over Database D2 (**c**) ROC curves for various fusion techniques over Database D3



(a) D1 Database (b) D2 Database (c) D3 Database

Fig. 6 CMC curves for D1, D2 and D3 databases (**a**) comparison of CMC curves of various fusion techniques over Database D1 (**b**) comparison of CMC curves of various fusion techniques over Database D2 (**c**) comparison of CMC curves of various fusion techniques over Database D3

Fig. 7 Sample images from Noisy database



(a) Gaussian Noise (b) Gaussian Noise (c) Blurred

Table 2 Comparision of EER values for D1, D2 and D3 databases after adding Noise

Noise in modality	D1 database	D2 database	D3 database
$\bar{f}pi$	2.01±0.23	1.00±0.32	2.43±0.28
$f\bar{p}i$	1.80±0.17	0.15±0.21	0.91±0.15
$fp\bar{i}$	2.08±0.32	2.86±0.36	2.01±0.41
$\bar{f}\bar{p}i$	2.95±0.22	1.99±0.38	3.49±0.57
$\bar{f}p\bar{i}$	4.98±0.65	24.27±2.61	16.42±1.95
$f\bar{p}\bar{i}$	4.99±1.23	4.01±1.66	3.45±1.35
$\bar{f}\bar{p}\bar{i}$	39.85±4.72	58.07±5.81	60.78±5.08

Table 3 Comparision of time complexity for various Biometric recognition methods

Method	Time(ms)
Face	29.08
Finger	17.37
Iris	20.81
PCR5 [46]	17.43
PCR6 with BSA [24]	20.44
PSO wtd. Sum [47]	29.16
Symmetric Sum [48]	23.56
Frank t-norm [45]	20.26
Yager t-norm [45]	21.85
Weighted Score Fusion [49]	22.15
Fuzzy Score Fusion [50]	51.85
Proposed Method	20.56

5 Conclusion and future directions

This paper presents a novel adaptive score fusion technique for a multimodal biometric system using three biometric traits viz. fingerprint, face, and iris. The proposed technique performed boosting and suppression of individual scores from each modality. Reliability factor based on image quality is evaluated for each individual modality to resolve the problem of dynamic environment. It provides unequal prior to each classifier based on the quality of input images. The high value of the reliability factor improves the overall impact of the corresponding modality during score fusion. This not only helps in dealing with various problems of the dynamic environment but also very effective against spoofing attacks as well. The proposed system is evaluated on three chimeric multimodal databases generated from benchmark images of fingerprint, face and iris modality. Exhaustive result analysis shows that the proposed fusion technique overpass many state-of-the-art fusion methods under a dynamic environment. Quantitative analysis shows that the proposed adaptive score level fusion technique is computationally efficient for performing a fusion of scores from multiple classifiers. The qualitative analysis shows the distance between genuine and imposter score distribution is large resulting in high reliability and accuracy of the system.

In the future, incorporating user specific traits for estimating Reliability factor may also be used. This will result in an increase in the adaptive nature of the system and a more wide variety of challenges may be addressed. It may be done for each user or on the basis of the system's performance for a specific use. The proposed biometric system can also be customized to work at multiple security levels as per requirements.

References

1. Ross A, Jain A (2003) Information fusion in biometrics. Pattern Recogn Lett 24(13):2115–2125
2. Unar JA, Seng WC, Abbasi A (2014) A review of biometric technology along with trends and prospects. Pattern Recogn 47(8):2673–2688
3. Hossain M, Chen J, Rahman K (2018) On enhancing serial fusion based multi-biometric verification system. Appl Intell 48(12):4824–4833
4. Yang J, Zhang X (2012) Feature-level fusion of fingerprint and finger-vein for personal identification. Pattern Recogn Lett 33(5):623–628
5. Peng J, El-Latif AAA, Li Q, Niu X (2014) Multimodal biometric authentication based on score level fusion of finger biometrics. Optik 125(23):6891–6897
6. Prabhakar S, Jain A (2002) Decision-level fusion in fingerprint verification. Pattern Recogn 35(4):861–874
7. Sellahewa H, Jassim SA (2010) Image-Quality-Based Adaptive face recognition. IEEE Trans Instrum Meas 59(4):805–813
8. ManminderSingh AS (2017) Arora a robust anti-spoofing technique for face liveness detection with morphological operations. Optik 139:347–354
9. Kho JB, Lee W, Choi H, Kim J (2019) An incremental learning method for spoof fingerprint detection. Expert Syst Appl 116:52–64
10. Kaur B, Singh S, Kumar J (2019) Cross-sensor iris spoofing detection using orthogonal features. Comput Electr Eng 73:279–288
11. Kalka ND, Zuo J, Schmid NA, Cukic B (2010) Estimating and fusing quality factors for iris biometric images. IEEE Trans Syst Man Cybern - Part A: Syst Hum 40(3):509–524
12. Pisani PH, Lorena AC, de Carvalho AC (2018) Adaptive Biometric Systems using Ensembles. IEEE Intell Syst 33(2):19–28
13. Nanni L, Lumini A, Ferrara M, Cappelli R (2015) Combining biometric matchers by means of machine learning and statistical approaches. Neurocomputing 149:526–535
14. Shariatmadar ZS, Faez K (2014) Finger-knuckle-print recognition performance improvement via multi-instance fusion at the score level. Optik - Int J Light Electron Opt 125(3):908–910
15. Tao Q, Veldhuisl R (2013) Robust biometric score fusion by naive likelihood ratio via receiver operating characteristics. IEEE Trans Inf Forensic Secur 8(2):305–313
16. Sim HM, Asmuni H, Hassan R, Othman RM (2014) Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. Expert Syst Appl 41(11):5390–5404
17. Sim HM, Asmuni H, Hassan R, Othman RM (2014) Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. Expert Syst Appl 41(11):5390–5404
18. Mukherjee S, Pal K, Majumder BP, Saha C, Panigrahi BK, Das S (2014) Differential evolution based score level fusion for multi-modal biometric systems. IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM), pp 1–7
19. Liang Y, Ding X, Liu C, Xue J-H (2016) Combining multiple biometric traits with an order-preserving score fusion algorithm. Neurocomputing 171:252–261
20. Dwivedi R, Dey S (2019) A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. Appl Intell 49(3):1016–1035
21. Roy K, Shelton J, O'Connor B, Kamel MS (2015) Multibiometric system using fuzzy level set, and genetic and evolutionary feature extraction. IET Biom 4(3):151–161

22. Liau HF, Isa D (2011) Feature selection for support vector machine-based face-iris multimodal biometric system. Expert Syst Appl 38(9):11105–11111
23. Nandakumar K, Chen Y, Dass SC, Jain A (2008) Likelihood Ratio-Based biometric score fusion. IEEE Trans Pattern Anal Mach Intell 30(2):342–347
24. Walia GS, Singh T, Singh K, Verma N (2019) Robust Multimodal Biometric System based on Optimal Score Level Fusion Model. Expert Syst Appl 116:364–376
25. Mezai L, Hachouf F (2015) Score-Level Fusion of face and voice using particle swarm optimization and belief functions. IEEE Trans Human-Mach Syst 45(6):761–772
26. Walia GS, Rishi S, Asthana R, Kumar A, Gupta A (2019) Secure multimodal biometric system based on diffused graphs and optimal score fusion. IET Biom 8(4):231–242
27. Kumar A, Kumar A (2016) Adaptive management of multimodal biometrics fusion using ant colony optimization. Inf Fusion 32(Part B):49–63
28. Poh N, Kittler J (2012) A unified framework for biometric expert fusion incorporating quality measures. IEEE Trans Pattern Anal Mach Intell 34(1):3–18
29. Poh N, Kittler J, Bourlai T (2010) Quality-Based Score normalization with device qualitative information for multimodal biometric fusion. IEEE Trans Syst Man Cybern - Part A: Syst Hum 40(3):539–554
30. Shekhar S, Patel VM, Nasrabadi NM, Chellappa R (2014) Joint sparse representation for robust multimodal biometrics recognition. IEEE Trans Pattern Anal Mach Intell 36(1):113–126
31. Liu C, Wechsler H (2002) Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition. IEEE Trans Image Process 11(4):467–476
32. Abhishree TM, Latha J, Manikantan K, Ramachandran S (2015) Face Recognition Using Gabor Filter Based Feature Extraction with Anisotropic Diffusion as a Pre-processing Technique. Procedia Comput Sci 45:312–321
33. Farina A, Kovács-vajna ZM, Leone A (1999) Fingerprint minutiae extraction from skeletonized binary images. Pattern Recogn 32(5):877–889
34. Sudiro SA, Paindavoine M, Kusuma TM (2007) Simple fingerprint minutiae extraction algorithm using crossing number on valley structure. IEEE Workshop on Automatic Identification Advanced Technologies, pp 41–44
35. Kahlil AT, Chadi FEMA (2010) Generation of iris codes using 1D Log-Gabor filter. IEEE International Conference on Computer Engineering & Systems, pp 329–336
36. Ye H, Shang G, Wang L, Zheng M (2015) A new method based on hough transform for quick line and circle detection. IEEE International Conference on Biomedical Engineering and Informatics (BMEI), pp 52–56
37. Daugman J (2004) How iris recognition works. IEEE Trans Circ Syst Video Technol 14(1):21–30
38. Field D (1987) Relations between the statistics of natural images and the response properties of cortical cells. J Opt Soc Amer 4(12):2379–2394
39. Mittal A, Moorthy AK, Bovik AC (2012) No-Reference Image quality assessment in the spatial domain. IEEE Trans Image Process 21(12):4695–4708
40. Gao W, Cao B, Shan S, Chen X, Zhou D, Zhang X, Zhao D (2008) The CAS-PEAL Large-Scale chinese face database and baseline evaluations. IEEE Trans Syst Man Cybern - Part A: Syst Hum 38(1):149–161
41. Ortega-Garcia J, Fierrez-Aguilar J, Simon D, Gonzalez J, Faundez-Zanuy M, Espinosa V, Satue A, Hernaez I, Igarza J-J, Vivaracho C, Escudero D, Moro Q-I (2003) MCYT Baseline corpus: a bimodal biometric database. IEEE Proc - Vis Image Signal Process 150(6):395–401
42. Cappelli R, Ferrara M, Franco A, Maltoni D (2007) Fingerprint verification competition 2006. Biom Technol Today 15:7–9
43. Kumar A, Passi A (2010) Comparison and combination of iris matchers for reliable personal authentication. Pattern Recogn 43(3):1016–1026
44. MMU2 Iris Database[Online], Available: http://pesona.mmu.edu.my/ccteo/, Accessed: June, 2019
45. Hanmandlu M, Grover J, Gureja A, Gupta HM (2011) Score level fusion of multimodal biometrics using triangular norms. Pattern Recogn Lett 32(14):1843–1850
46. Sharma R, Das S, Joshi P (2018) Score-level fusion using generalized extreme value distribution and DSmt for multibiometric systems. IET Biom 7(5):474–481
47. Srinivas N, Veeramachaneni K, Osadciw LA (2009) Fusing correlated data from multiple classifiers for improved biometric verification. 12th International Conference on Information Fusion, Seattle, USA, pp 1504–1511
48. Cheniti M, Boukezzoula N-E, Akhtar Z (2018) Symmetric sum-based biometric score fusion. IET Biom 7(5):391–395
49. Sim HM, Asmuni H, Hassan R, Othman RM (2014) Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images. Expert Syst Appl 41(11):5390–5404
50. Fakhar K, Aroussi ME, Saidi MN, Aboutajdine D (2016) Fuzzy pattern recognition-based approach to biometric score fusion problem. Fuzzy Sets Syst 305:149–159

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.