

A Comprehensive Overview of Quality Enhancement Approach-Based Biometric Fusion System Using Artificial Intelligence Techniques



Gaurav Jindal  and Gaganpreet Kaur

Abstract Biometric authentication has been reported to be one of the most emerging research fields and its attainments are inseparable from the aid of a heterogeneity of single-modal and multi-modal biometric traits (e.g., fingerprint, hand geometry, iris, face, ear, gait, and so on). Normally, biometric traits are used as authentication information for the security system. Sometimes, the characteristics of biometric traits are difficult to acquire in an appropriate means, and it is essential to practice numerous pre-processing and post-processing algorithms to improve the feature of traits on the security system. In this case, this review paper presents a comprehensive overview of the biometric fusion system (BFS) with some pre-processing and post-processing approaches using the concept of artificial intelligence/machine learning techniques. In this regard, the following subject matters are discussed: 1. Biometric traits quality improvement techniques in the BFS. 2. Feature extraction and optimization approaches. 3. Analysis of classifiers to improve biometric fusion accuracy. 4. Existing challenges of BFS. Besides, a review of existing work based on their accuracy of classification is also discussed. The main aim of this survey is to make available a complete overview of BFS with the role of a different biometric trait in biometrics fusion.

Keywords Biometric authentication system · Biometric modalities · Biometric traits · Image quality improvement techniques · Feature extraction approaches · Optimization approaches · Classifiers · Artificial intelligence/machine learning techniques

G. Jindal (✉) · G. Kaur

Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

1 Introduction

Biometric fusion system (BFS) refers to the automated process of recognizing and validating a user based on their behavior as well as physical traits for instance fingerprint, hand geometry, iris, face, ear, signature, gait, voice, etc. The human biological characteristics are inherent characteristics and the chances of changes are less. These types of biological features frequently have high differences of character, which are considered by constancy, assortment, and openness. Biometrics authentication system (BAS) is a well-known advancement that practices human behavior as well as physiological features for mechanical identification (recognition/verification). In this decade, the mainstream biometrics technologies include physiological biometric traits such as the face, iris, ear, lip, and gait. The BAS with different behavioral as well as physiological biometric traits is shown in Fig. 1.

With the progress of science and innovation with the evolution of the times, in view of the neighborliness and comfort of biometrics innovation, this innovation has been broadly utilized in the banking, transportation, internet business, judicial, security, and diverse fields. The different types of physiological as well as behavioral biometric traits are shown in Fig. 2.

With the ever-increasing advancement of computer technology, single-modal BAS is unable to meet the security requirements of users in most cases, so multi-modal BAS has also become a novel research hotspot. The advantage of the multi-modal BAS is that it can fully utilize the information provided by each biometric to complement the defects of the single-modal BAS, thereby improving the rate of recognition and robustness of the BAS with the concept of feature fusion. For BFS to be effectual in real-time applications, researchers need to prevail over certain associated challenges:

- **Distorted and noisy scanned input data:** In BFS, physiological biometric data composed in real-time applications are distorted and noisy due to boisterous

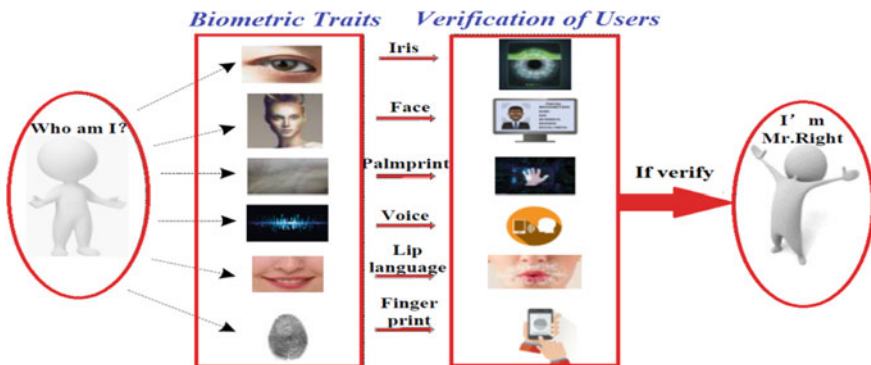


Fig. 1 BAS with different biometric traits

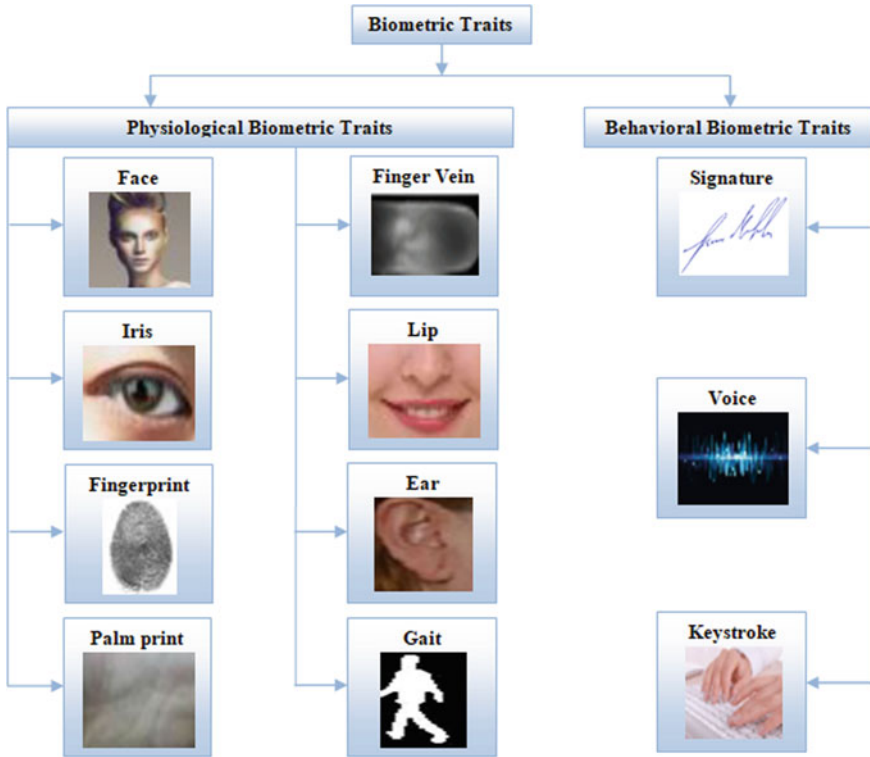


Fig. 2 Types of biometric traits

biometric sensors. The quality of input as a scanned image to be clear when biometric data are captured covertly due to completely unimpeded conditions.

- **Selection of irregular region of interest (ROI):** The selection of proper ROI of scanned input data is the biggest task in any BFS which depends on the pre-processing phases like segmentation, morphological operations, etc.
- **Biometric feature extraction:** Extracting the appropriate biometric features from distorted and noisy input data needs lots of substantial pre-processing techniques, and if extracted features are not unique as per user, then the chances of misclassification are more.
- **Permanence:** Since biological features are based on human factors, they may be unreliable. Physical biometrics vary with time, while biometric behaviors are further discriminated against by socio-ecological factors.
- **Large identities:** BFS includes recognizing possibly a great many people in whom recognizing variables might be unobtrusive. This entails profoundly intricate models to distinguish people at such a scale.
- **Uniqueness:** It is not clear whether a particular biometric model could identify a person differently. In particular, many biometric behavioral features do not apply to human identification and are only used for verification purposes.

- **Attacks on biometric systems:** Biometric systems are often attacked at various levels. Such an attack must be identified as part of the recognition process.

With the current success of machine learning methods, we expect them to be of assistance in addressing the many challenges mentioned above in BFS. Artificial intelligence or machine learning methods learn features from biometric data and, when they are discriminated against, can learn subtle features that can differentiate between a large number of individual users. In addition, if there are satisfactory numbers of feature samples for various biometric features are available, then artificial intelligence or machine learning techniques can train the system to separate such discriminative features based on the users.

Under such scenarios, generative artificial intelligence or machine learning methods might be utilized to synthesize such differences and proved better results. Because of its ability to read biometric data, artificial intelligence or machine learning can also help to differentiate biometric data from a noisy environment. Given these opportunities, we present a comprehensive study to investigate how biometric detection methods have taken advantage of the intrinsic worth of artificial intelligence or machine learning techniques and aspects where artificial intelligence or machine learning can help improve the efficiency of BFS.

This paper presents a survey of the existing trends in BFS with different artificial intelligence or machine learning approaches. Specifically, in Sect. 2, we introduce a literacy study (background survey) of existing work with their advantages and disadvantages. Section 3 of this survey represents a comparative analysis of biometric traits' quality enhancement. The current results-based research is available in Sect. 4 and concludes through discussions on current challenges and future outcomes in Sect. 5.

2 Background Survey

In this segment, we introduce a study of work that is already based on biometric integration with dissimilar techniques. UQi Zhang et al. [1] presented a deep fusion feature network (using the convolution neural network (CNN)) that uses complementary information presented in the iris and periocular regions to improve mobile screening performance. Conventional iris detection systems cannot detect high levels of fragmentation using these low-resolution images and improve the user-identifiable functionality of a cell phone, creating an integrated network of learning features that utilize complementary information proposed in the iris and periocular areas. In this study, the authors are not trying to avoid the problems of distortion of images. Proença et al. [2] presented a model of periocular recognition without iris and sclera with the concept of deep learning frameworks. As a young adult, they describe a series of analysis based on CNN. Talreja et al. [3] proposed a secure biometric system that uses deep neural networks and encrypted error correction codes. The authors introduced a feature-level mixing in the biometric framework to produce a secure biometric

template from multiple biometric for each user. They show that phase performance can be improved in many ways while maintaining good safety and durability. Xu and Lu [4] proposed a model using a flexible set method to set the default settings for all test samples and do not require manual setup. Detailed experiments indicate that the method used exceeds previous contemporary art approaches and they need to improve their results through an in-depth prepared learning approach. Liu et al. [5] introduced a safe and effective framework for producing safe, effectual, and removable biometric templates. The advanced framework uses networks of deep trust and random biometric data predictions using secure keys from user authentication passwords. A great bright spot for the introduced system is that it can store the most significant data of biometric data, even the password used. They did not focus on complex design and experimentation with other recognition algorithms capable of image protection. Muthu Kumar and Kavipriya [6] proposed a biometric system model based on the extraction of the Gabor element with the SVM classifier of Finger-Knuckle-Print (FKP). The authors focused on using FKP recognition through the process of integrating the Gabor and SVM features. Security with FKP and other biometric features should be greatly improved. Srivastava and Srivastava [7] presented a multidisciplinary framework using palm, and fingerprint, a combination of face. The SVM separator produces better results in the approval framework and the ids and accuracy and errors are worse. Leghari et al. [8] proposed a biometric validation development model using a combined learning method as dividers. Researchers systematically explored a variety of biometric recognition classification techniques. The three types of biometric data used include fingerprints, online signature, and offline signature. Class algorithms include nearest neighbors algorithm (k-NN), support vector machine (SVM), and multilayer perceptron (MLP) neural network and ensemble learning algorithms included by extra tree classifier (ETC) and random forest classifier (RFC). They did not use large datasets and did not use an in-depth study of various types of biometric data.

Raja [9] proposed a kernel-based manager support program (ESVM-KM) to improve the recognition of multiple chemical reactions using facials, fingerprints, and iris images. Rane [10] proposed a multidisciplinary biometric recognition system using face and palm print as biometric methods. The author's main goal is to increase the robustness of recognition systems. Both uni-methods and multiple methods are combined using various biometric fusion techniques. Garg et al. [11] proposed a multi-modal biometric system based on the decision-making process. The authors want to present a model with k-NN and a neural classifier that participated in the decision-making process. This research work uses 100 samples of iris and fingerprint from a CASIA database compiled by 50 familiar individuals where each person entered two samples and extracted a feature, counting the texture factors used for the continuation of the identification process. After that, the consolidation of the decision level was done using k-NN and neural classifiers. Many datasets can be used because, in the case of user identification, the data used are insufficient. Gayathri Rajagopal and RamamoorthyPalaniswamy [12] proposed a biometric system with multiple human recognition features using two components, namely, palm print, and iris. The resolution of this study was to evaluate multi-modal integration to attain

better performance. The main objectives of the authors are to increase the accuracy of the detection using fusion-level fusion and to obtain good accuracy but not safety precautions. Cheniti et al. [13] proposed that multi-modal biometric systems, which include data from a wide range of biometric sources, have been revealed to advance the performance of character recognition by overcoming the weaknesses and specific environmental restrictions of illegal systems. An innovative outline for consolidating school standards based on symmetrical statistics (S-sums) has been introduced, and the authors are developing a benchmark of information available on a public bench. Sharma et al. [14] proposed an integrated point-level integration scheme that is a combination of the standard GEV distribution process and fm-based DSMT application. They did not use any encryption algorithm to protect their system. Vishi and Josang [15] introduced a multi-biometric fusion for multi-biometric fusion based on subjective logic, and their results demonstrate that in most phases, subjective logic fusion accomplishes better than classical fusion approaches but they did not test with different modalities for instance the face, finger vein, fingerprint, voice, and iris and with a variety of databases.

The Solution of Existing Challenges in BAS and BFS: From the survey, artificial intelligence or machine learning has outperformed previous state-of-the-art methods in various domains. The following factors which help to solve the current challenges and issues of BAS or BFS:

Biometric Quality Improvement: It is the basic and necessary step to solve the current BFS challenges. If the quality of the biometric image is better, then the chances of higher accuracy are more. A brief description of different biometric quality improvement methods is described in Sect. 3.

Biometric Feature Learning: Artificial intelligence or machine learning methods learn features from biometric data that help to perform other related tasks. A variety of integrated features are analyzed in this paper to the trained system compared to some specific named features. Several feature extraction techniques are available to train the system using feature metrics instead of a particular named feature set. The uniqueness of the named feature is less as compare to the unnamed feature extraction approaches like PCA, SIFT, SURF, etc.

Feature Selection/Optimization: These methods help to learn BFS by selecting a useful feature set of particular biometric data. There are several feature selection/optimization algorithms are available but the selection of an appropriate approach helps to achieve better performance of biometric recognition.

The fusion of Features: The fusion of biometric features is a necessary process to train the system with maximum accuracy. There are several types of methods that are available to fusion the extracted feature which are the following:

- *Sensor-level fusion*
- *Feature-level fusion*
- *Score-level fusion*
- *Rank-level fusion*
- *Decision-level fusion.*

Training with Large-Scale Biometric Datasets: Artificial intelligence or machine learning is the better option for the training of the system but a large-scale biometric dataset helps to achieve a better classification accuracy of the system.

3 Biometric Quality Enhancement

Biometric quality improvement strategies are used to obtain better biometric quality, where ‘quality improvement’ is occasionally defined as neutral and sometimes individual that means making the process of debugging and classification easier by modifying the colors, contrast, or intensities of biometric data. There are a lot of biometric quality improvement techniques are available.

Intensity-based Biometric Quality Improvement (IBQI): Intensity quality-based development is a way to adjust the strength of the biometric image strength values in a series of novels and create a biometric image with better durability. Prior to the improvement of data quality, it is essential to set limits on the maximum and minimum pixel value for which the biometric image will be made. Prior to this, we know that at 8-bit gray-level any images, lower and upper limits, can range from 0 to 255. We look at the lower and upper limits by L_R and H_R , respectively with the iris sample shown in Fig. 3. Then check the biometric image to find the lowest and highest pixel value currently existing in the biometric image that needs enrichment. These pixel values are called L_N and H_N . Thereafter, each pixel (P) of the biometric image is developed by means of the following equation:

$$P_{\text{Enh}} = (P_{\text{Bimg}} - L_N) \left(\frac{H_R - L_R}{H_N - L_N} \right) + L \quad (1)$$

where P_{Enh} is the enhanced biometric image and P_{Bimg} the original biometric image. To illustrate, the third image below shows a low biometric image (iris) with its histogram and enhances its biometric image and its histogram using the IBQI method.

The IBQI method enhances the biometric image strength by transferring each grayscale value to a new pixel series using a collector scatter function from the path of the hardness histogram. Figure 3 represents the IBQI process representing the biometric iris image and the enhanced image after the development process. In this figure, (a) represents the first biometric iris image, (b) signifies an advanced biometric iris image using IBQI, (c) is the histogram of the first biometric iris image, and (d) is the histogram of iris biometric iris image. To improve the image of the biometric iris, below is the IBQI algorithm used.

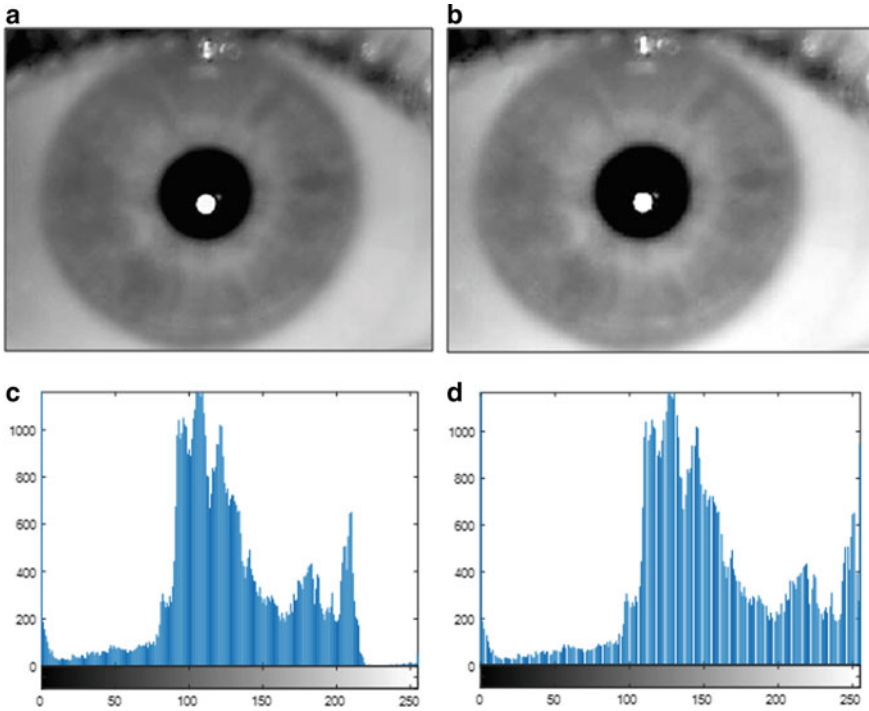


Fig. 3 a Biometric image, b enhanced biometric image, c histogram of biometric image, and d histogram of biometric enhanced image

Algorithm 1: IBQI
Input: Bimg \leftarrow Biometric Image
Output: EBimg \leftarrow Enhanced Biometric Image
1. Calculate the dimension (D) of Bimg
2. If D==3
3. Bimg_R=Red component of Bimg
4. Bimg_G=Green component of Bimg
5. Bimg_B=Blue component of Bimg
6. Using equation (1)
7. Enhanced Rimg= P_E (Bimg_R)
8. EnhancedGimg = P_E (Bimg_G)
9. EnhancedBimg = P_E (Bimg_B)
10. Enhanced Image=cat (3, Enhanced Rimg, EnhancedGimg, EnhancedBimg)
11. Else
12. Enhanced Image= P_E (Bimg)
13. End
14. Return: Enhanced Image as a Enhanced Biometric Image
15. End

Histogram Equalization-based Biometric Quality Improvement (HEBQI): Biometric quality improvement using the histogram equalization approach is a procedure of image intensities adjustment to advance the contrast of a biometric image. It is not indispensable that the contrast of the image will always be a rise in quality improvement using the histogram equalization approach. There may be various cases where quality improvement using the histogram equalization approach to generate an inferior quality image. In that situation, the contrast of a biometric image is reduced.

Consider B_{img} be a given biometric iris image represented as an R by C matrix of integer pixel intensities ranging from 0 to Int , where Int is the number of feasible intensity values of the image. Let N_H denote the normalized histogram of B_{img} with a number of feasible bins intensity. The formula to calculate the normalized histogram of B_{img} is given in Eq. 2.

$$N_H = \frac{\text{No. of pixels with } n \text{ intensity}}{\text{Total Pixels}} \tag{2}$$

$$n = 0, 1, 2, \dots, Int - 1$$

The histogram equalized biometric image $B_{img}H_E$ is well defined by

$$B_{img}H_E(i, j) = R((Int - 1) \sum_{n=0}^{B_{img}(i, j)} H_{Enh}) \tag{3}$$

where $R()$ is the function that is used to rounds down the pixel value to the nearest integer. Let us start biometric quality improvement using a histogram equalization approach by taking an instance of a biometric image below as a simple image.

Figure 4 represents the process of biometric quality improvement using a histogram equalization approach, representing the first biometric image and the enhanced biometric image after development In this figure, (a) represents the first biometric image, (b) signifies the advanced biometric image using the HEBQI process, (c) the histogram of the first biometric image, and (d) is a biometric image enhancement histogram. To make a biometric image, use the HEBQI algorithm mentioned below.

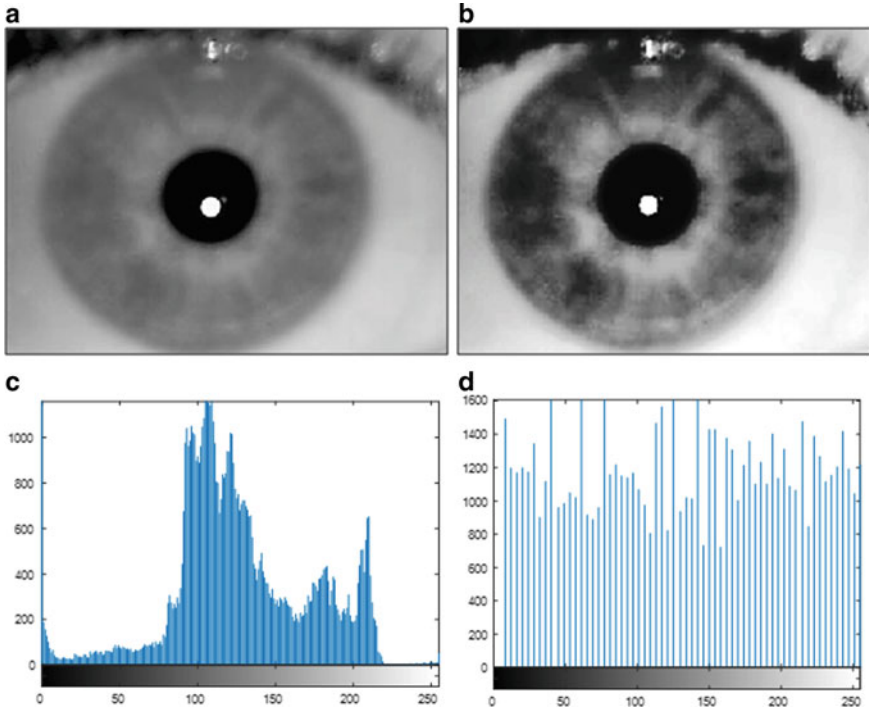


Fig. 4 a Biometric image, b enhanced biometric image, c histogram of biometric image, and d histogram of biometric enhanced image

<p>Algorithm 2: HEBQI</p> <p>Input: Bimg \leftarrow Biometric Image Output: EBimg \leftarrow Enhanced Biometric Image</p> <ol style="list-style-type: none">1. Calculate the dimension (D) of Bimg2. If D==33. Bimg_R=Red component of Bimg4. Bimg_G=Green component of Bimg5. Bimg_B=Blue component of Bimg6. Using equation (3)7. Enhanced Rimg=H_{Enh} (Bimg_R)8. Enhanced Gimg =H_{Enh}(Bimg_G)9. Enhanced Bimg =H_{Enh}(Bimg_B)10. Enhanced Image=cat (3, Enhanced Rimg, Enhanced Gimg, Enhanced Bimg)11. Else12. Enhanced Image=H_{Enh} (Bimg)13. End14. Return: Enhanced Image as an Enhanced Biometric Image15. End

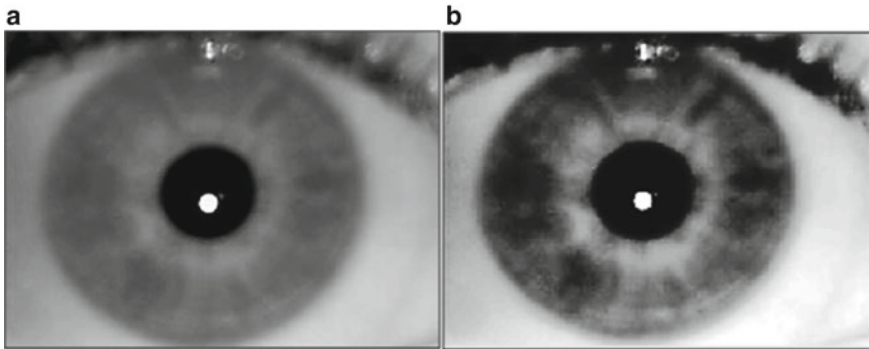


Fig. 5 **a** Before global HEBQI and **b** after HEBQI

Contrast Limited Adaptive Histogram Equalization-based Biometric Quality Improvement (CLAHEBQI): It is the improvisation of HEBQI. In the HEBQI method, we have just considered, it looks at the global difference of biometric image in Eq. (3). In most cases, it is not good for improving the quality of the biometric image. For instance, the below image demonstrates an input biometric iris image and its consequence after global HEBQI.

It is correct that the background contrast of biometric iris image (Fig. 5) has improved after HEBQI but compares the iris part of the eye in both (Fig. 5 a, b) biometric images. We founded that much information is lost due to the problem of overhead. This is because the histogram of the iris image is not limited to a specific region as we have seen in previous cases. The difference does not have to always be an increase in the HEBQI approach. There may be some cases where the HEBQI process may be of poor quality. If so, the biometric image difference is decreasing so we need to use the comparison limit to advance the quality of the biometric image, and this method is known as CLAHEBQI. The CLAHEBQI method is described below:

Phase 1: Firstly provide a biometric image for further process of image quality improvement.

Phase 2: Acquire altogether the input pixel values used in the image quality improvement process such as number of regions in row and column, the total number of drums used in comparison clip limit, histogram conversion function distribution, parameter.

Phase 3: After that, apply to pre-process on the biometric image to split an image into sub-regions.

Phase 4: Process applied over the plane of a biometric image (proper sub-region).

Phase 5: At last, construct gray-level mapping and clipped histogram for the pre-processed part of the image. Unsuitable sub-region, numbers of pixels are divided alike in each gray level so a typical number of pixels for gray level is defined using the given Eq. 4:

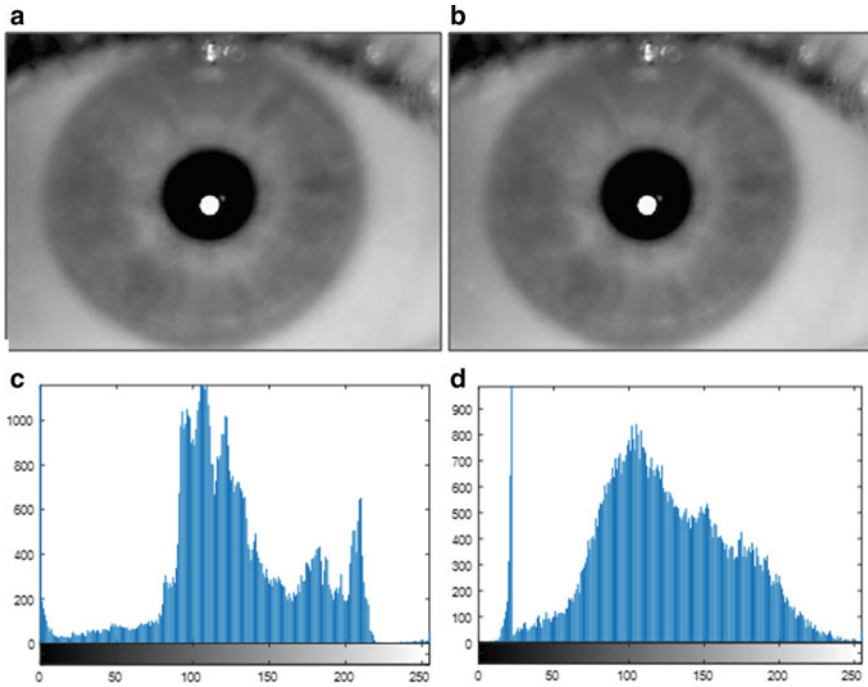


Fig. 6 **a** Biometric image, **b** enhanced biometric image, **c** histogram of biometric image, and **d** histogram of biometric enhanced image

$$Pix_{average} = \frac{Pix_{(CR-XP)} \times Pix_{(CR-YP)}}{Pix_{Gray}} \quad (4)$$

where $Pix_{average}$ is an average number of pixels presents in the biometric image, Pix_{Gray} is the number of gray levels in the appropriate sub-region, P_{CR-XP} is the number of pixels with the x -axis of suitable sub-region, and Pix_{CR-YP} is the number of pixels with the y -axis of the apposite sub-region. After that, compute the genuine clip limit of a biometric image using the given formula:

$$Pix_{CL} = Pix_{clip} - Pix_{average} \quad (5)$$

where Pix_{CL} is the pixel clip limit that is used to set the contrast limitation of a biometric image.

Phase 6: Apply the HEBQI technique with Eq. (3) with a clip limit to advance the quality of the original biometric image.

To exemplify, below-mentioned figure displays the CLAHEBQI process by its histogram and compares it with the original biometric image.

Figure 6 signifies the procedure of the CLAHEBQI method which characterizes the original biometric iris image and enhanced iris image after the quality improvement. In CLAHEBQI technique, quality improvement function is applied over all neighborhood pixels of a biometric image and then the transformation function is derived with limitation. This is differing from the HEBQI method because of its contrast limiting method. In Fig. 6, (a) signifies the first biometric image, (b) signifies the enhanced biometric image using the CLAHEBQI process, (c) is the histogram of the original biometric image, and (d) is the histogram of the enhanced image. The quality of biometric images improved using the CLAHEBQI algorithm.

In this survey, we present a comparative analysis of biometric fusion and the impact of image quality improvement techniques on BFS using different image quality improvement algorithms such as IBQI, HEBQI, and CLAHEBQI.

4 Analysis of Existing Work

From the survey and above observation, we concluded the accurateness in terms of genuine acceptance rate (GAR) for different biometric modalities and techniques is described in the below table.

Figure 7 characterizes the relative analysis of existing work based on the accuracy of classification in terms of GAR. From the figure, we observe that the accuracy attains by using the concept of artificial intelligence/machine learning is better than another author because they present a module by using the concept of CNN using different feature extraction techniques.

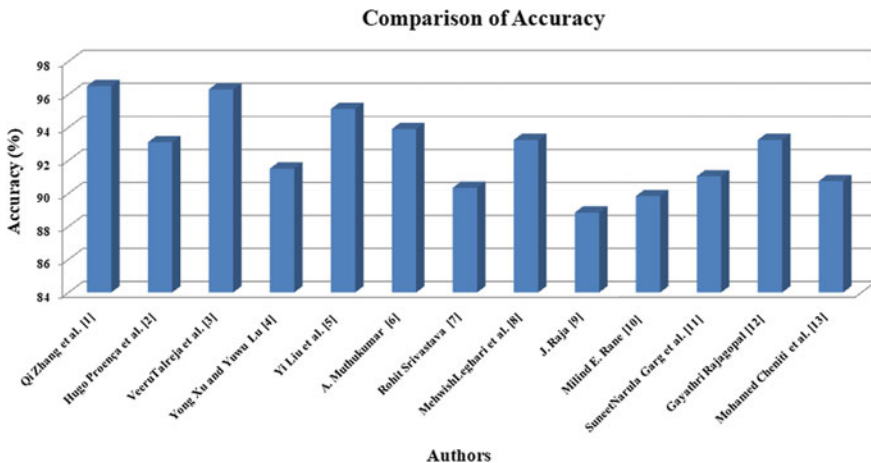


Fig. 7 Comparison of accuracy of proposed work with existing works

5 Conclusion and Future Work

In this paper, a comprehensive overview of the quality enhancement approach-based biometric fusion system via artificial intelligence or machine learning techniques is presented with an analysis of biometric image quality enhancement approaches. It provides a comprehensive view of the various applications and potential challenges of the biometric system which is a tough task in the science and technology field from a security point of view. From the survey, as it provides a large number of different techniques and algorithms, artificial intelligence or machine learning techniques offer numerous advantages over other methods for the biometric pattern recognition system. In this approach, the requirements of capable techniques satisfy a growing need for security and shrewder applications in this world. Also, it could be appreciated that all the given artificial intelligence algorithms congregate the crucial features proposed in Sect. 2 for biometric survey dealing and attained high classification accuracy demonstrates they are appropriate for real-time applications for BAS or BFS. So this survey finds out a better solution to an existing problem in BFS by integrating the concept of artificial intelligence or machine learning techniques with feature extraction and feature optimization approaches with feature fusion in the future trends. In the future, artificial intelligence or machine learning techniques that are utilized as a classifier to train BFS based on hybridization of feature descriptor with soft computing-based feature optimization algorithm could be a better option.

Table 1 Brief summary of traditional BAS

No	Bas with advantages	Adopted approaches disadvantages
1	<p>System</p> <p>Finger print-based BAS</p> <p>Advantages</p> <ol style="list-style-type: none"> 1. Highly mature technique 2. Trouble-free to use and it is a non-intrusive technology 3. Classification accuracy is high 4. Long-term constancy and capability to store and enroll multiple fingerprints 5. A low-cost system with respect to others BAS 	<p>Approach</p> <ol style="list-style-type: none"> 1. Minutiae feature-based methods 2. Image pixel-based approaches <p>Disadvantages</p> <ol style="list-style-type: none"> 1. Failure to enroll some users 2. Affected by human skin circumstance 3. Used sensor need to clean up again and again 4. Association with forensic applications
2	<p>System</p> <p>Face-based BAS</p> <p>Advantages</p> <ol style="list-style-type: none"> 1. Non-intrusive model 2. Designing cost is low 3. Capability to function covertly 4. Potential for isolation abuse 	<p>Approach</p> <ol style="list-style-type: none"> 1. Image pixel-based methods <ol style="list-style-type: none"> i. A model with Eigenfaces ii. A model with Fischer's faces 2. Image feature-based methods <ol style="list-style-type: none"> i. A model with geometric feature ii. A model with features metric iii. Morphological models <p>Disadvantages</p> <ol style="list-style-type: none"> 1. Mat be affected by appearance surroundings 2. High false acceptance rates 3. Twins attacks are applicable

(continued)

Table 1 (continued)

No	Bas with advantages	Adopted approaches disadvantages
3	<p>System</p> <p>Iris-based BAS</p> <p>Advantages</p> <ol style="list-style-type: none"> 1. Potential for high recognition accuracy 2. Confrontation to impostors 3. Long-period constancy 	<p>Approach</p> <ol style="list-style-type: none"> 1. A model with complex-valued 2D Gabor wavelets 2. Gaussian filters for feature extraction from iris 3. A model with zero-crossing wavelet transform as a feature 4. Hough circular transform with filters <p>Disadvantages</p> <ol style="list-style-type: none"> 1. Intrusive and normalization of data is difficult 2. High designing cost 3. Time-consuming
4	<p>System</p> <p>Hand geometry-based BAS</p> <p>Advantages</p> <ol style="list-style-type: none"> 1. Affection rate of the environment is minimum 2. Mature BAS technology 3. The relatively more stable and secure technique of BAS 	<p>Approach</p> <ol style="list-style-type: none"> 1. A feature-based model such as finger length, width, thickness curvatures and relative location of features <p>Disadvantages</p> <ol style="list-style-type: none"> 1. Low accuracy 2. High cost 3. Relatively large readers 4. Difficult to use for some users
5	<p>System</p> <p>Finger vein based BAS</p> <p>Advantages</p> <ol style="list-style-type: none"> 1. Resistance to forgery 2. Commonly secured and accepted 3. Non-intrusive 4. No need to record 	<p>Approach</p> <ol style="list-style-type: none"> 1. Feature-based model <p>Disadvantages</p> <ol style="list-style-type: none"> 1. Pattern inconsistencies 2. Difficult to utilize 3. Required large matching templates 4. Problem with small data

Table 2 Artificial intelligence or machine learning approaches in biometrics

Algorithms	Biometric applications	Analysis
Deep learning	Iris recognition [1] Iris and sclera recognition [2] Face and iris fusion [3] Palm and face [4] Finger vein recognition [5]	Deep learning techniques (CNN, ANN, etc.) are used as a classifier to train and classify the user using their different biometric traits. Using the concept of deep learning techniques, the achieved accuracy is lies between 90 to 96% in different scenarios
SVM	The fusion of Finger-Knuckle-Print [6] The fusion of face, fingerprint, and palm print [7] The fusion of fingerprint, online and offline signature [8] The fusion of face, iris, and fingerprint [9]	SVM (binary classification) is used to train the model based on the different types of features like principal component analysis (PCA), Gabor filter, stroked-based feature, etc. The accuracy of the system is calculated in terms of Genuine acceptance rate and it is near to 90% but needs improvement in the feature selection process
Decision tree, k-NN, random forest, etc.	The fusion of face and palm print [10] The fusion of iris and face [11] The fusion of iris and palm print [12] Face and fingerprint-based fusion model [13]	With the decision tree, k-NN, random forest, etc. as a classifier, they have a limitation of training data and these types of classifiers are applicable for a few amounts of data

Table 3 Analysis of GAR in multi-modal biometric system

Authors	Accuracy (%)
Zhang et al. [1]	96.5
Proença et al. [2]	93.1
Talreja et al. [3]	96.3
Xu and Lu [4]	91.5
Liu et al. [5]	95.11
Muthukumar and Kavipriya [6]	93.9
Srivastava and Srivastava [7]	90.34
Leghari et al. [8]	93.24
Raja [9]	88.84
Rane [10]	89.83
Garg et al. [11]	91.03
Rajagopal [12]	93.24
Cheniti et al. [13]	90.74

References

1. Zhang Qi, Li H, Sun Z, Tan T (2018) Deep feature fusion for iris and periocular biometrics on mobile devices. *IEEE Trans Inf Forensics Secur* 13(11):2897–2912
2. Proença H, Neves JC (2018) Reminiscence of’ mastermind: Iris/periocular biometrics by “In-Set” CNN iterative analysis. In: *IEEE transactions on information forensics and security*
3. Talreja V, Soleymani S, Valenti MC, Nasrabadi NM (2019) Learning to authenticate with deep multibiometric hashing and neural network decoding. *arXiv preprint arXiv: 1902.04149*
4. Xu Y, Yuwu Lu (2015) Adaptive weighted fusion: a novel fusion approach for image classification. *Neurocomputing* 168:566–574
5. Liu Y, Ling J, Liu Z, Shen J, Gao C (2018) Finger vein secure biometric template generation based on deep learning. *Soft Comput* 22(7):2257–2265 (2018)
6. Muthukumar A, Kavipriya A (2019) A biometric system based on Gabor feature extraction with SVM classifier for Finger-Knuckle-Print. *Pattern Recogn Lett* 125:150–156
7. Srivastava R, Srivastava P (2019) A framework design for human authentication based on biometric fusion mechanism. Available at SSRN 3391051
8. Leghari M, Memon S, Sahito F, Chandio AA, Leghari M (2018) Biometric verification enhancement with ensemble learning classifiers. In: *2018 5th international multi-topic ICT conference (IMTIC)*. IEEE, pp 1–6
9. Raja J, Gunasekaran K, Pitchai R (2018) Prognostic evaluation of multimodal biometric traits recognition based human face, fingerprint and iris images using ensembled SVM classifier. *Cluster Comput* 1–14
10. Rane ME, Pande AJ (2018) Multi-modal biometric recognition of face and palm-print using matching score level fusion. In: *2018 fourth international conference on computing communication control and automation (ICCCUBEA)*. IEEE, pp 1–6
11. Garg SN, Vig R, Gupta S (2016) Multimodal biometric system based on decision level fusion. In: *2016 international conference on signal processing, communication, power and embedded system (SCOPE)*. IEEE, pp 753–758
12. Rajagopal G, Palaniswamy R (2015) Performance evaluation of multimodal multi-feature authentication system using KNN classification. *Sci World J* 2015
13. Cheniti M, Boukezzoula N-E, Akhtar Z (2017) Symmetric sum-based biometric score fusion. *IET Biomet* 7(5):391–395
14. Sharma R, Das S, Joshi P (2018) Score-level fusion using generalized extreme value distribution and DSMT, for multi-biometric systems. *IET Biomet* 7(5):474–481
15. Vishi K, Jøsang A (2017) A new approach for multi-biometric fusion based on subjective logic. In: *Proceedings of the 1st international conference on internet of things and machine learning*. ACM, p 68
16. Abdullah-Al-Wadud M, Kabir MH, Dewan MAA, Chae O (2007) Dynamic histogram equalization for image contrast enhancement. *IEEE Trans Cons Electron* 53(2)
17. Yadav G, Maheshwari S, Agarwal A (2014) Contrast limited adaptive histogram equalization based enhancement for real time video system. In: *Advances in computing, communications and informatics (ICACCI, 2014 International Conference on)*. IEEE, pp 2392–2397
18. Gillespie AR (1992) Enhancement of multispectral thermal infrared images: Decorrelation contrast stretching. *Remote Sens Environ* 42(2):147–155
19. Mustapha A, Hussain A, Samad SA (2011) A new approach for noise reduction in spine radiograph images using a non-linear contrast adjustment scheme based adaptive factor. *Sci Res Essays* 6(20):4246–4258
20. Restaino R, Vivone G, Dalla Mura M, Chanussot J (2016) Fusion of multispectral and panchromatic images based on morphological operators. *IEEE Trans Image Process* 25(6):2882–2895
21. Sarhan S, Alhassan S, Elmougy S (2017) Multimodal biometric systems: a comparative study. *Arab J Sci Eng* 42(2):443–457