Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 09 September-2024, Page No.-5140-5147

DOI: 10.47191/etj/v9i09.16, I.F. – 8.227

© 2024, ETJ

Multimodal Biometric System Fusion Using Fingerprint and Iris with Convolutional Neural Network

Ghadeer Ibrahim Maki[1], Sarah Basim Abed[2]

[1]Department Of Nursing –Al Diwaniya Institute .AL-furat Al-Awsat Technical University. Kufa Al-Najaf.Iraq.

[2]Department accounting – Al Diwaniya Institute Al-furat Al-Awsat Technical University . kufa Al-Njaf.Iraq.

ABSTRACT: Biometric sensing technology became everyday life frequent component as a result of world requirement for info security and safety legislation. A strong and efficient individual authentication has appeared because of new developments in multimodal biometrics. Multimodal biometrics integrates different biological traits in trying for creating considerable effect on identification performance. Latent fingerprint biometrics refer to effective human identification system for criminals given the accessible crime evidence shreds. Although, biometric trait restrictions like intra-class variation, sensed data noise, lack of individuality caused low matching score that possesses a negative effect on recognition and investigation process. This paper uses two unimodal biometrics—the fingerprint and the iris—applied as multi-biometrics to show that using these biometrics can produce excellent results with high accuracy. Every biometric result is weighted for involvement in the final decision, and the decision level is utilized for fusion. For every biometric result integration effect, a neural network is used. The datasets' experimental findings have demonstrated a notable biometric system identification capability. The accuracy performance of the suggested approach is 100, the FAR is 0.1, and the EER is 0.1. To demonstrate the efficacy of the suggested system, the suggested method is contrasted with a few other approaches currently in use.

KEYWORDS: Convolutional Neural Network, Fingerprint Recognition, Iris Recognition, Minutiae Extraction, Multi-Biometric.

1. INTRODUCTION

The phrase "biometric sensing" refers to the process of defining an individual's identity verification using their physical or behavioral characteristics. for the safe identification of physical and behavioral characteristics, which is now a challenging and crucial problem for the business and scientific domains. Biometric attributes were applied to hands, faces, irises, DNA, teeth, ears, feet, fingers, typing style, signatures, gaits, veins, retinas, voices, and odors [1]. Working as a system of recognition, a biometric system uses various biometric attributes, checking the physiological features like fingerprints, hand measurements, voice patterns, eye retinas and irises, facial features for authentication. Such systems, also known as unimodal biometric systems, are based on single and intrinsic personal biological/behavioral features' natures for their identity determination/verification [2].

This method applied nowadays like Postal Index Number (PIN) code and passwords does not face min security framework by nowadays' standards. For such reasons a strong algorithm for recognition given something which could not be stolen, forgotten, regenerated, copied falsified, known as biometrics, is more than essential. Biometrics is described as a person science recognition given 1/more of their features, such features are uniform for every person and could be grouped from the physical modalities point of view (Fig.1) like iris and palm print, behavioral modalities, fingerprints, like signature, keystroke, speech [3].

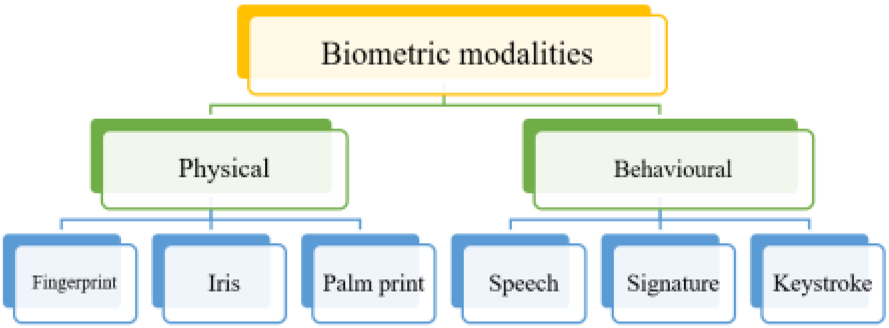

Figure. 1. Biometric modalities [3].

Single biometric systems possess restrictions such as high error rate, non-universality, noise, uniqueness, high spoofing rate. For instance, face recognition is influenced by happiness, position, ambient light amount, sadness. As most investigators have recently realized, approximately 2 percent of the population lacks a readable fingerprint, making it impossible for them to be enrolled in a fingerprint biometrics system. Currently, hybrid biometrics are recommended as a solution to these limitations [4].

Multimodal biometric fusion has some advantages such as raised usability, greater accuracy, developed resilience to spoofing assaults, reduced false acceptance/rejection ratios. This technique could tackle with personal features disadvantages, like lack of distinctiveness, noise, appearance differences, combining different biometric traits. So, way of fusion could propose a more thorough and worthy individual’s recognition assessment, increasing entire authentication system security [5].

Thus, incorporating hybrid biometric modalities for identification is able to tackle with several unimodal biometrics restrictions to later expansion of app plans also develop the precision and trustworthiness of it its. Multimodal biometrics combined hybrid info have shown strong distinguished benefits in comparison with uni-biometrics methods [6]:

(1) More identification precision. Deliberately modelling algorithm of fusion, every modality subscription for identifying identity could be combined efficiently, so considerably developing identification precision in authenticating each person.

(2) Wider practical plans. In real-time plans, a few users might have shortage of particular biometric attributes because of illnesses/ several external agents. For example, an actual modality data may not be achieved because traumatic incidents. Under these positions, multimodal biometrics systems could yet carry out efficiently when no unique modality exists, causing that to be practical to a broader person's scope.

(3) Robust anti-deceptive ability. Integration hybrid biometric traits compensates for restrictions which might present in uni-biometrics systems, causing that to be a concern for attackers to shape hybrid manners at the same time. The difficulty included in modelling hybrid biometrics provide stronger multimodal biometrics systems in contrary to counterfeiting efforts in comparison with depending on a unique biometric modality.

In this paper, decision-level fusion is applied. Such a strategy possesses the benefits of using as a lot of info as feasible from every biometric manner. 2 modes, fingerprint and iris, are applied here. In the first parts, a summary of fingerprint and iris preview needing code is presented, after that the integration technique of 2 modalities and fusion technique are defined.

2. RELATED WORK

Several papers have been performed about the way of increasing biometric recognition systems functionality, specifically multi–biometric systems. The best fusion level as well as the accurate fusion method have always been contentious problems in multi–biometric systems. In a multi–biometric system, fusion attributes could be performed at different levels, such as match score, abstract/decision level fusion, sensor and feature level. The precision level needed from a system, the biometric qualities kind which are considered, data value, the fusion method used in an actual system are several natures which affect optimum fusion level to select. Several investigators have applied different fusion strategies at different fusion levels for increasing multi-biometric systems performance, as discussed in the following.

In [7] concentrates on multimodal biometric modes use for authenticating. Finger vein, face, fingerprint modes are taking into consideration here, extraction of attributes was performed by local binary model also features’ optimization, adjustable PSO was used. A broad learning machine was offered in this paper for classification and great outcomes were created.

Paper [8] applies some suggestions in DL and ML for presenting novel unimodal systems for face, iris, palm. Such modes apply deep wavelet transform networks (WTN) to recognize iris as well as face also deep convolutional neural networks (CNNs) to recognize palmprint. Plus, the writers explain new multimodal biometric system given the unimodal systems.

In [9] the new multi-modal system is presented, integrating 2 biometric traits, retina, fingerprint. Such presented method includes hashing, pre-processing, feature extraction. Pre-processing happens to augment and resize pictures aims. In step of feature extraction, CNN has been applied for spatial info extraction. This doesn’t present the relation among adjacent attributes. To do this, effectively integrate CNN and BiGRU pattern with self-consciousness layer (ConvGRUSA). parameters are adjusted in ConvGRUSA, applying urochord swarm optimization (Tuni-SO) algorithm.

In [10] proposes the new multimodal biometric fusion design which considerably increases accuracy and generalization via AI power. Different techniques of fusion, encompassing feature-level, score-level as well as pixel-level fusion, are seamlessly combined via DNN. At the pixel level, the writers use spatial, intensity fusion approaches, channel for process of fusion optimization. On level of attribute, mode-based splits as well as cooperatively optimized presentation layers launch strong dependencies among modes via backpropagation. At last, smart fusion methods, like class-1 and modality assessment, are saddled to blend complementing outcomes on level of outcome.

In [11] resented novel ERMOTMBA scheme applying SU-NBO mechanism. Firstly, median filtering was used for pre-processing images of iris, finger knuckle, palm print, finger vein, fingerprint. Features extracted for palm print, finger knuckle, finger vein, iris and fingerprint were as: Palm print – Statistical features and line features, Finger vein – Bifurcation point and improved LGBP, Iris- 2D Gabor kernel and polynomial filtering, Finger knuckle- Global feature and local feature, Finger print- Improved Minutiae feature (Binarization and thinning). Next, the developed FLF happens applying correlation. At last, EC (DBN, CNN and Bi-LSTM) were used, which weights were selected by SU-NBO algorithm.

In [12] propose new strategy for safeguarding multimodal biometric patterns applying Cancelable CNN. Our technique uses 2 biometric modes, fingerprint as well as iris. Basically, attributes are separately taken out from such modes as well as integrated in unique attribute vector. Accordingly, a CCNN is used for decreasing this fused vector size. At last, the decreased vector is doubled with a customer-presented issue for the increased ability of removing.

In [13] describe a novel CCNN-based approach for protecting multimodal biometric patterns. The method being offered makes use of the fingerprint and iris as biometric features. In essence, characteristics from these attributes are extracted one at a time and combined into a single feature vector. In light of this, a CCNN is employed to reduce the fused vector size. Finally, a user-presented seed is multiplied by the reduced vector to boost cancelability.

3. FINGERPRINT RECOGNITION

Fingerprint is the most usually applied physiological biometric feature. Fingerprint is the oldest, back to 1893 when that was applied for convicting a murder suspect in Argentina. Fingerprint includes ridges and valleys that shape single models. Minutiae are the main local fingerprint rates that could be applied for assigning fingerprint uniqueness, two of the most essential ones that being ridge endings and ridge bifurcations. Palmprint is the other alternative applied one for authentication aims. Plus, minutiae features, palmprints includes features based on geometry, wrinkles delta points, main lines [14]. As seen in Fig. 2, contactless fingerprint images have comparatively less contrast between the ridges and valleys than contact fingerprint images, such as rolled fingerprints, where the ridges are often black and the valleys are typically white.

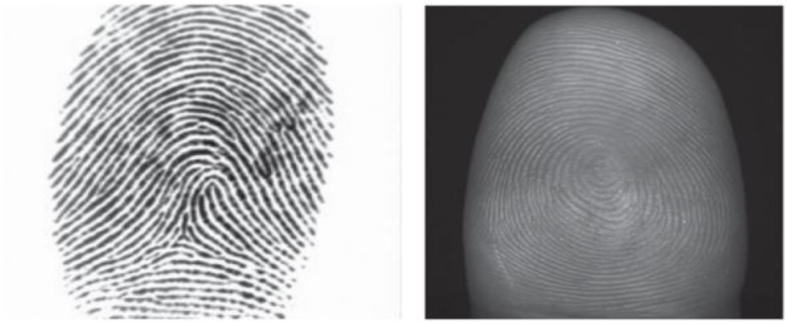

Figure 2. Contact fingerprint and contactless fingerprint comparison: (a) contact fingerprint image from FVC2002-DB1-A with image ID 1_2; (b) contactless fingerprint image from a benchmark set of data with image ID 1_1_1_0 [16].

A fingerprint biometric trait benefit refers to: feature could not be guessable like passwords, could not be dismissed also unsettled. However, the advantage refers to fingerprints which are simply exposed to others in comparison with finger vein and show several great benefits. Spoofing the fingerprint data paths, like: -

- A single person One might easily obtain a fingerprint from a smartphone or any other surface.
- A fake finger could be created by applying an elevated fingerprint picture.
- To assert identity, the dummy finger may be uploaded onto the sensor.

Fingerprint recognition process: in the following there is Figure 3 which illustrates fingerprint recognition process with binary results.

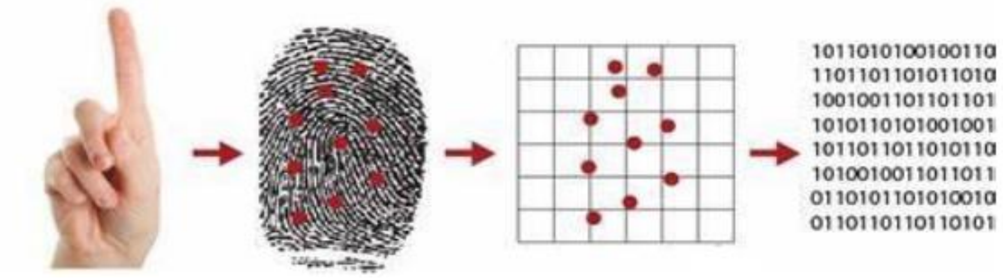

Figure 3. Fingerprint biometric identification system [17]

The three sections of a fingerprint recognition system are the matching, minutia extraction, and image acquisition sections. The portion that acquires images uses optical sensors. Pre-processing, minutia extraction, and post-processing comprise the three sections that make up the fundamental section on minutia extraction. The pre-processing step aims to improve the quality of the produced image by utilizing Fourier transformation and histogram incrementation. It also converts the image to binary format and thinned out the fingerprint ridges. For minutia extraction, the fingerprint picture is currently prepared [18].

4. IRIS RECOGNITION

For recognizing individuals, this technology seeks the features such as rings, freckles, furrows in shaded substance surrounding pupil. It refers to a biometric technology with top accuracy rate. As shown via novel Silicon.com paper, the direction investigation such as single finger sense affirmation, facial and iris acknowledgment, realized that iris affirmation was the best for a validation method, despite the fact of complex enrolment process. The usual camcorder could be used to get an iris image, this could greatly be done from a more considerable space than with pigment outcome. This technology customers require to work together to get an obvious image.Accordingly, gadget is programmed thus while a user puts his head before it and could observe his iris sending back in the gadget, showing that the undeniable image could be taken. For ensuring that the architecture is not tricked by a fake eye, gadget might alarm the light which is sent back to eye and see pupil expansion. Such architecture possesses high validation ratio also fraud defence benefit. Data of iris are similar for the left and right eyes and as you get older it stays stable. Such approach drawback refers to that it is widely invasive; enrolling progress is a bit complex as just a few know this system. John Daugman, a Cambridge College scientist, was in charge of a excellent exploration tackling with an affirmation of iris [19].

The iris, as seen in Fig. 4, can be a focus point that is firmly positioned among the layers. modify the student's focal mass point to the center of the iris while positioning the understudy, and then modify the pursuit gap in the iris edge. Muscle (which causes the student to constrict) and dilator muscles (which cause the understudy to enlarge) are both found in the iris. An outward ciliary zone and an internal papillary zone divide the outer surface of the iris. The "Collarette" is a bending structure that divides the two zones. Liquids are able to enter and exit the iris fast as understudy contracts because to tomb-like, oval-shaped structures surrounding the court. The evolution of an outspread streak led to the graves being enveloped in connective tissue, which corrected itself as a student contracted and ended up being wavy as the understudy grew. Given that students expand, dispensing the iris to overlay, concentrated lines close to the exterior ciliary zone finish up later [20]

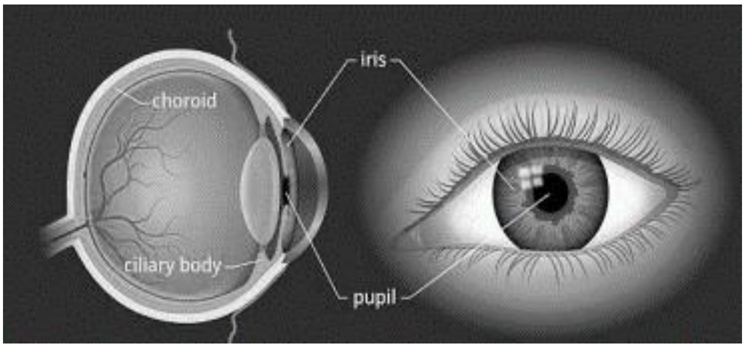

Figure 4. Iris Position in Eyeball Structure [20]

However, the study about iris recognition systems (IRSs) is powerful in limited (ideal) areas, there is a lack of study on iris recognition in unlimited (non-ideal) areas. In unlimited areas of identification, some issues exist like rotational, cropping, off-angle, small-sized iris, scaling, low resolution, occlusion, distortion by blurry image, eyelash, “noise,” interference from the eyeglass frame, reflection from eyeglass lens. Generally, IRS structure in the two traditional and DL strategies include 7 main steps in the following order: iris image acquisition step, preprocessing step, iris image segmentation step, iris normalization step, feature extraction step, feature selection step, and lastly iris classification/matching step [21].

5. MULTI BIOMETRIC

The multibiometric system could tackle with several unibiometric system restrictions through integrating info from various resources in a principled manner. Multiple resources use sometimes developed identification performance and increased system reliability, as integrated info is probably to be more distinctive to a person in comparison with info gained from a unique resource.

biometric systems utilize 5 various techniques to solve unique biometric drawbacks [22]:

Multi-sensor: systems integrate info got by hybrid sensors for similar biometric modality.

Multi- presentation: Multiple sensors detecting similar body parts is known as multi-presentation. (Many fingerprint images from several fingers on a single person). **Multi-instance**: System receives hybrid samples with comparable biometric traits (multi-instance). Regarding iris recognition, the identification module may employ both the left and right irises, resulting in a multi-instance system. A multi-instance fingerprint/palm-print identification system most likely could use information from ten fingers or both palms.

Multiple algorithms: They are used by systems to process different input instances. A unique sensor is used to gather data from a biometric modality; however, some algorithms are used to process the data.

Multi-modal: systems recognize subjects by using information gleaned from several biometric clues. Information gathered from iris, fingerprint, face, speech, face, and voice modalities, as well as face, ear, iris, and periocular modalities, can be utilized by a multi-modal system. There exist multiple tiers within a biometric pipeline where integration of fusion technology may be implemented, including sensor, feature, score, rank, and decision levels. A brief definition of each fusion level is given in [22]:

Sensor-level: In general, fusion and data-level algorithms refer to multi-sensor and multi-sample algorithms where data is swiftly integrated upon acquisition. This indicates that data fusion is done directly on raw data, before feature extraction. The face identification module deals with the direct integration of facial photos captured from a camera at the pixel level.

Feature level: fusion refers to techniques that combine multiple features that have been retrieved from comparable or diverse input data. It can be related to many feature sets for comparable biometric traits, such as a facial image or different textural and structural elements from a hand or palm print image. This has to do with features that are taken from different modalities, such as pictures of hands and faces.

Score-level: Fusion at the score-level refers to algorithms that combine scores produced by different matchers. The max, min, and mean scores of many matchers are taken into consideration as the final score in a number of common fusion algorithms, including mean, max, and score fusion.

Rank-level: Fusion occurs following a comparison of the input probe with the gallery set templates, such as a database. When a recognition function compares an image provided as the probe to a gallery of photos, a matcher may occasionally produce a ranked list of matching identities.

Decision-level: relates to mechanisms that fusion is carried out at level of decision. Majority voting refers to a usual fusion mechanism used at level of decision. Decisions made by n mediators or groupers are integrated given the majority vote, causing to the last decision.

6. PROPOSED METHOD

This study presents a novel approach to personal recognition using a decision-level fusion model that combines fingerprint and iris data. This demonstrates how fingerprint combinations and iris biometrics can perform better than using each individual biometric alone. For fusion, a neural network technique is used, which offers improved accuracy and performance. Neural networks and Hamming distance are used to compare and determine confirmation.This part explains the detail on presented fingerprint identification system applying CNN-Softmax.

Here, our method consists of three fundamental steps: (1) pre-processing the fingerprint image; (2) using CNN model for feature extraction; and (3) using Softmax as a classifier. Following this phase of pre-processing, the CNN framework is used to extract the properties from the pre-processed fingerprint picture. Given the deep supervised learning model, CNN is a CNN. Thus, CNN can be thought of as both a trainable classifier and an automatic feature extractor. The provided fingerprint-CNN framework configuration information are displayed, as seen in Fig. 5.

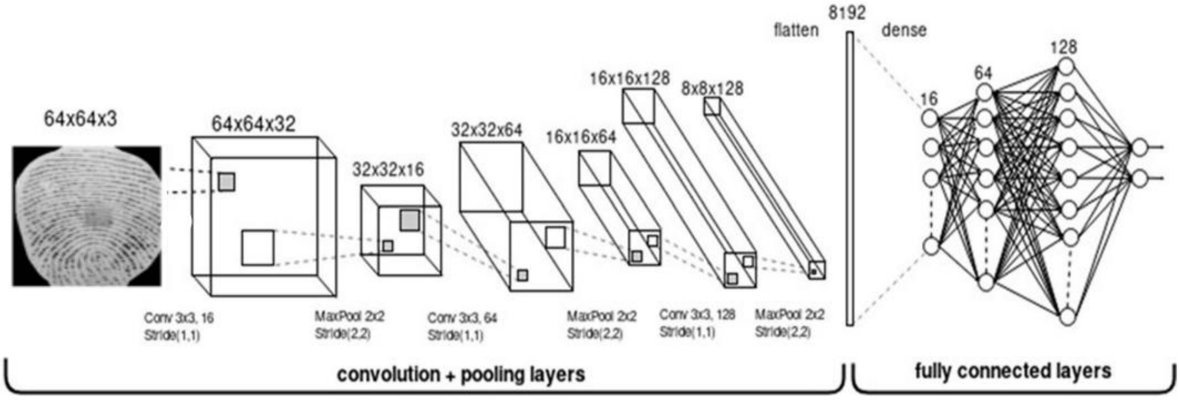

Figure 5. The architecture of the proposed fingerprint-CNN model

CNN uses the size mxmxq picture as its input. For an RGB image, q=3, where m is the image size and q is the channel number. There are k filters (or kernels) of size pxpxq in the convolutional layer. P has to be less than m. Each of the k feature maps produced by the filters has a size of m-p+1. The min of max over pxp contiguous areas is pooled for each map. P values typically fall within this range. The picture portion is selected and the convolution process is performed based on the kernel size. The red matrix is divided into smaller matrices of size 3x3, depending on the kernel size (let's say p=3).

Applying a 4x4 red matrix and a 3x3 kernel, for example, would result in the following for the initial 3x3 red matrix. The product and summation operations would be completed by applying kernels. The red input matrix would provide four size matrices of 3 by 3 depending on the kernel size. Cell-by-cell product operations between the kernel and the obtained matrices would be carried out. The red input matrix would provide four feature matrices as a result of the product function. The values of the total cells would be assigned to each feature matrix. The final matrix, the pink matrix, would have four cells once the sums for each matrix had been obtained. The green and blue matrices would be subjected to the same function. The generated matrices would have dimensions of 2×2×3. ReLU activation is utilized for the nonlinear input signal transformation after such functions. The max (or average) pooling function is then applied to achieve these results. The size of the feature matrix is decreased by using the downsampling function. A 4×4 matrix is divided into smaller 2×2 matrices, as seen in Figure 3. In this case, the maximum function is applied when pooling. This is where the maximum amount is allocated to each split 2x2 image. As seen, the amounts on the matrix are [3, 4, 4, 4]. Four is obtained as the maximum one from such amounts. Four is obtained as the maximum one from such amounts. In order to obtain the input picture feature vector, the pooling layer results would be fattened. The fattened vector in the max pooling figure would be. The feature map is the fully-connected network's input, while the clusters are its output. The input pattern labels are predicted by using the Softmax function.

7. EXPERIMENTAL RESULTS

This part applies a unique biometric fingerprint to obtain results, which are shown in Table 1. Iris recognition is then used, and the desired result is obtained. Better results are now obtained when multi-biometric application is made using iris and fingerprint fusion. Here, simulated outcomes for presented biometric fusion based iris and fingerprint identification applying convolutional neural network are defined. The simulation has been done in MATLAB area.

7.1. Performance metrics

Metrics like accuracy, FAR, and FPR were frequently used to assess classifier performance in machine learning. The confusion matrix was used to calculate the metrics.

Accuracy: One of the most important metrics for evaluating the effectiveness and pace of advancement of a given technique in performance analysis is accuracy. The accuracy from the number of cases checked indicates an accurate solution. Take a look at the following expression to determine accuracy:

$$Acc = \frac{R_{TN} + R_{TP}}{R_{TN} + R_{TP} + R_{FN} + R_{FP}}$$

False acceptance rate (FAR): In a biometric security system, the medium false acceptances amount is calculated using the false acceptance rate (FAR) unit. This calculates the system's accuracy in confirming unregistered or unauthorized users on a given system. The FAR formula is:

$$FAR = \frac{R_{FP}}{R_{TN} + R_{FP}}$$

False Rejection Rate (FRR): it is the probability which a system might inappropriately reject an unregistered /unauthorized user, like:

$$FRR = \frac{R_{FP}}{R_{TP} + R_{FP}}$$

The differences between the two single-biometric and multi-biometric systems are shown in Table 1. After converting the fingerprint image to binary code in the fingerprint section, we could compare it to codes in the database using the hamming distance and select the code in the database with the least amount of difference. Do the same in the Iris section and choose a code from the database with the least amount of variation. Applied CNN is used in the final judgment.

Table 1. Difference between uni-modal and multi-modal

	Accuracy	FAR	FRR
Finger-Iris	100	0.1	0.1
Finger	0.1	0	0.97727
Iris	0.56667	0.1	0.98876

Two bodily components that do not depend on hereditary factors are the fingerprint and the iris. They are twins with different features. The fact that different people have different iris traits is crucial. Each person's fingerprint is unique, even in twins. Therefore, we would undoubtedly get superior results when we applied such two permanent biometrics as multi-biometrics. There are many ways to combine fingerprint and iris biometrics with other biometrics, such face, voice, retina, and so on, but iris and fingerprint biometrics are more reliable.

Table 2 illustrates presented model superiority to the other multimodal biometric systems in [7,11,12,13]. This distinction in presented system outcome was because of the essential agent that was Decision level addition that performed better than fingerprint in case of raising accuracy in recognizing an individual. The other reason for this is that the fusion process in [7,11,12,13] was performed at various feature level abstraction that is various than our fusing technique.

Table 2. Comparison of accuracy and performance values between proposed method already and existing methods.

	Traits	**Level Fusion**	**Accuracy**
Ref [7]	Face, fingerprint, and finger vein	Feature level fusion	97.14
Ref [11]	Palm print, finger vein, finger knuckle, iris, and fingerprint	Feature level fusion	85.16
Ref [12]	Retina and fingerprint	Feature level fusion	99.93
Ref [13]	Facial and dorsal hand	Feature level fusion	99..87
Proposed model	Iris, and fingerprint	Decision level fusion	100

8. CONCLUSION

In this paper a multimodal biometric recognition system utilizing iris and fingerprint pictures, as well as CNN models for human identification, have been defined. The results of the experiments conducted on a multimodal database show that the overall performance of the multimodal system is superior to that of the unimodal and bimodal biometric systems when it comes to different classifiers provided the recognition. The iris code is weighed at 80% and the fingerprint code at 20%. Applying iris and fingerprint as multimodalities yields superior results compared to other modalities.

REFERENCES

1. Priyani J, Nanglia P, Singh P, Shokeen V, Sharma A. HGSSA-bi LSTM: A Secure Multimodal Biometric Sensing Using Optimized Bi-Directional Long Short-Term Memory with Self-Attention. ECS Sensors Plus. 2024;3(1):011401.
2. Shukla PS. Multi-Modal Biometric Authentication System Using Cnn. International Journal of Engineering Research & Technology (IJERT), 2023, 12, 12.
3. HAFS T, ZEHIR H, HAFS A, BRAHMIA H, NAIT-ALI A. Enhancing Recognition in Multimodal Biometric Systems: Score Normalization and Fusion of Online Signatures and Fingerprints. SCIENCE AND TECHNOLOGY. 2024;27(1):37-49.
4. Zolfagharipour L, Kadhim MH, Mandeel TH. Enhance the Security of Access to IoT-based Equipment in Fog. In2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT) 2023 Jul 4 (pp. 142-146). IEEE.
5. Vekariya V, Joshi M, Dikshit S. Multi-biometric fusion for enhanced human authentication in information security. Measurement: Sensors. 2024 Feb 1;31:100973.
6. Li S, Fei L, Zhang B, Ning X, Wu L. Hand-based multimodal biometric fusion: A review. Information Fusion. 2024 Apr 12:102418.
7. Vensila C, Boyed Wesley A. Multimodal biometrics authentication using extreme learning machine with feature reduction by adaptive particle swarm optimization. The Visual Computer. 2024 Mar;40(3):1383-94.
8. Kadhim ON, Abdulameer MH. Biometric Identification Advances: Unimodal to Multimodal Fusion of Face, Palm, and Iris Features. Advances in Electrical & Computer Engineering. 2024 Jan 1;24(1).
9. Sasikala TS. A secure multi-modal biometrics using deep ConvGRU neural networks based hashing. Expert Systems with Applications. 2024 Jan 1;235:121096.
10. Byeon H, Raina V, Sandhu M, Shabaz M, Keshta I, Soni M, Matrouk K, Singh PP, Lakshmi TR. Artificial intelligence-Enabled deep learning model for multimodal biometric fusion. Multimedia Tools and Applications. 2024 Feb 8:1-24.
11. Kumar KP, Prasad PE, Suresh Y, Babu MR, Kumar MJ. Ensemble recognition model with optimal training for multimodal biometric authentication. Multimedia Tools and Applications. 2024 Mar 8:1-25.
12. Vallabhadas DK, Sandhya M, Reddy SD, Satwika D, Prashanth GL. Biometric template protection based on a cancelable convolutional neural network over iris and fingerprint. Biomedical Signal Processing and Control. 2024 May 1;91:106006.
13. Sharma S, Saini A, Chaudhury S. Multimodal biometric user authentication using improved decentralized fuzzy vault scheme based on

Blockchain network. Journal of Information Security and Applications. 2024 May 1;82:103740.

14. Minaee S, Abdolrashidi A, Su H, Bennamoun M, Zhang D. Biometrics recognition using deep learning: A survey. Artificial Intelligence Review. 2023 Aug;56(8):8647-95.
15. Maio D, Maltoni D, Cappelli R, Wayman JL, Jain AK. FVC2002: Second fingerprint verification competition. In2002 International conference on pattern recognition 2002 Aug 11 (Vol. 3, pp. 811-814). IEEE.
16. Zhou W, Hu J, Petersen I, Wang S, Bennamoun M. A benchmark 3D fingerprint database. In2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD) 2014 Aug 19 (pp. 935-940). IEEE.
17. Dargan S, Kumar M. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications. 2020 Apr 1;143:113114.
18. Abdolahi M, Mohamadi M, Jafari M. Multimodal biometric system fusion using fingerprint and iris with fuzzy logic. International Journal of soft computing and engineering. 2013 Jan;2(6):504-10.
19. Samatha J, Madhavi G. SecureSense: Enhancing Person Verification through Multimodal Biometrics for Robust Authentication. Scalable Computing: Practice and Experience. 2024 Feb 24;25(2):1040-54.
20. Nazmdeh V, Mortazavi S, Tajeddin D, Nazmdeh H, Asem MM. Iris recognition; from classic to modern approaches. In2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) 2019 Jan 7 (pp. 0981-0988). IEEE.
21. Malgheet JR, Manshor NB, Affendey LS, Abdul Halin AB. Iris recognition development techniques: a comprehensive review. Complexity. 2021 Aug 21;2021:1-32.
22. Singh M, Singh R, Ross A. A comprehensive overview of biometric fusion. Information Fusion. 2019 Dec 1;52:187-205.