



**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.379**



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

# Random Forest-Based Score Level Fusion of Multimodal Biometrics: Combining Iris, Ear, and Fingerprint Modalities

Jeevalakshmi. M, Dr. M. Ezhilarasan

PG Student, Dept. of I.T., Puducherry Technological University, Puducherry, India

Professor, Dept. of I.T., Puducherry Technological University, Puducherry, India

**ABSTRACT:** Multimodal biometric systems that combine multiple biometric modalities have shown to be more robust and accurate than unimodal systems. In this study, we propose a random forest-based score level fusion method for combining the matching scores obtained from three biometric modalities - iris, ear, and fingerprint - in order to improve the overall performance of the system. The matching scores for each modality are first normalized and combined into a feature vector for each user. The random forest algorithm is then trained on the feature vectors using the ground truth labels (i.e., whether the user is a genuine or an imposter) to predict the class for new users based on their combined scores. The performance of the proposed method is evaluated on a publicly available multimodal biometric dataset using metrics such as accuracy, FAR, FRR, EER, and AUC. The results show that the random forest-based score level fusion method outperforms the individual modalities and other fusion methods, demonstrating the potential of using machine learning algorithms for improving the accuracy and reliability of multimodal biometric systems.

**KEYWORDS:** Multimodal biometrics; Iris biometrics; Ear biometrics; Fingerprint biometrics; Score level fusion; Random Forest.

## I. INTRODUCTION

Biometrics are less likely to be lost or stolen than more conventional identity authentication methods like a key, card, or password. The fingerprint is the biological characteristic that is most frequently used for biometric identification and verification jobs. Fingerprint matching technology, which is based on the local ridge characteristics and their correlations, is the earliest and most widely used biometric authentication method since fingerprints are both unique and invariable. It is also required to consider some practical techniques to align the fingerprints for the suggested method in order to apply it commercially and improve the matching precision [1]

Age-insensitive iris patterns are believed to be created at random during the development of the eye as a fetus. This signifies that each eye's iris pattern may be regarded as a globally identifiable biometric trait that can even differentiate twins. In order to give more accurate consolidated match scores and execute an open-set and cross-distance evaluation, the fusion process may stoutly take into account each modality's significance, their relative significance, and the effective region of interest. To produce an end-to-end framework that can execute segmentation and lessen robustness, the system has to be upgraded [3].

Biometrics are used in the majority of human identification systems because they are reliable over time, simple to collect, and unique for each person. The physical or behavioral traits of the fingerprint, palmprint, face, iris, hand geometry, voice, and signature are among the most often utilized biometrics for human identification. Most often, these biometric techniques are employed for human authentication. Most biometrics used for human identification relies on the cooperation of the matching individual to gather the biometric features. Since birth, the human ear has maintained a stable structure and is distinct for each person. Additionally, the acquisition technique for the human ear is contactless, non-intrusive, and does not depend on the cooperation of the person we are trying to identify. In order to determine the ear parts that provide the basis for identification, the study looks at the gender classification of ear photographs as well as the bilaterally symmetrical of human ears[6]. In automatic recognition systems, ear biometrics can enhance other biometric modalities and offer identity indications when other information is inconsistent or even absent. The ear can

act as a source of information about the identification of a human in surveillance footage in situations where face recognition may struggle with profile faces, such as in surveillance applications.

Unimodal biometric systems relying on a single biometric feature, however, are susceptible to spoofing attacks. Spoofing assaults happen when an imposter deceives a biometric system. The verification procedure for a person can be hampered by external interference in a unimodal biometric system, such as noisy data, problems with illumination for face and iris biometrics, and non-universality. Environmental disruption can have a significant negative influence on a biometric system's accuracy, which will reduce its performance. Different biometric modalities were merged and added to biometric systems in order to overcome these limitations. The key motivations for developing multi-biometric systems are high-accuracy recognition, high-security assurances, and overcoming obstacles like noisy sensor data, non-universality, and significant intra-user variances. Educational institutions are adopting cutting-edge technology to increase the effectiveness of their operations and the appeal of their offerings to both staff and students. Biometric technology is one such instance that has been applied in educational institutions.

## II. RELATED WORK

In this section, various techniques of Human Identification and Recognition using finger, iris, ear, and multimodal recognition systems are discussed and analyzed.

### 1.1 Fingerprint recognition system

Fingerprint recognition systems analyze a finger pressed against a smooth surface. The ridges and valleys on the finger are scanned, and a collection of discrete points known as minutiae are found where the ridges and valleys terminate or meet. These small details are what the fingerprint recognition system compares.

Chowdhury[10] By contrast the contactless finger photo-capturing method, the traditional approach to fingerprint identification, and the usage of deep learning inside this method, this study demonstrates how little the contactless finger photo-capturing method is being used today. Furthermore, accelerating feature extraction, minimizing the time needed to analyze pictures, and increasing identification accuracy are the advantages and possible weaknesses that deep-learning techniques for real-world biometric applications need to overcome. S. Kirchgasser[11] A multimodal and longitudinal Fp dataset with 108,000 samples has been proposed, along with an early examination of performance in terms of quality and recognition. The suggested datasets use a variety of capture devices, including 5 optical, 4 capacitive, and 1 thermal one, and make the data publically available, allowing us to get around the absence of extensive public databases with related annotation data. But as was predicted, there has been a decline in FP quality for samples taken from aged individuals. It must be used in conjunction with an appropriate pre-processing in order to stabilize the score decrease and minimize the erosion of recognition performance.

### 1.2 Iris Recognition system

Iris scanning is a method of identifying patterns in people's irises or the coloured circles in their eyes. The iris is illuminated with barely perceptible infrared light by biometric iris recognition scanners in order to identify characteristic patterns that are invisible to the human eye. Also, it possesses certain distinctive textural characteristics that are ideal for biometric systems since they cannot be readily changed or tampered with. Iris patterns play a significant part in a number of possible recognition or authentication operations because of their distinctness, universality, responsibility, and stability.

Fang [4] In order to break the issue of caricature identification in situations when some artifact attributes are unknown, this investigation points to a conclusion that unifies the two- and three-dimensional portions of the observed iris. A cutting-edge technique using Binary Statistical Image Characteristics (BSIF) is employed to extract the 2D (textural) iris features, and an ensemble of classifiers is used to offer judgments applicable to the 2D modality. As in numerous contemporary marketable iris identification detectors, just two prints taken under near-infrared light deposited at two distinct angles are used to rebuild the 3D (shape) iris characteristics. This demonstrates that further work may still be demanded to increase the effectiveness of deep literacy-grounded systems in cross-domain operations. J. E. Tapia[12] Based on a modified MobileNetV2 architecture, this article employs a two-stage serial design. A basic network is only trained to distinguish between the two classes of "attack" and "bona fide." If a picture earns a valid vote, it is sent to a second network trained to recognize it among three or four categories: bona fide or a different type of PAI: contact lenses, printout, or cadaver. Four databases were connected, and class scores were also added to the loss to make up for the imbalance. This resulted in a super-set with the different PAIs. The work employed



extensive data augmentation and contrast enhancement (CLAHE) techniques such as rotation, blurring, contrast change, edge enhancement, picture area dropout, and Gaussian noise. Additionally, leave-one-out PAI tests were performed in the study for open-set evaluation, demonstrating resilience in identifying unidentified assaults. Tests should be conducted on more recent lightweight model architectures like MobileNetV3 and EfficientNets, and additional PAI species should be included, using artificial picture generation as an example. Farouk[13] proposed a hybrid method for feature extraction and classification that combines Hamming distance (HD), edge detection and segmentation, and convolutional neural networks (CNNs). The model has been used on three datasets; in contrast, CNN on MMU performs better than the other two when applied to HD on CASIA, IITD, and MMU.

### 1.3 Ear Recognition system

Biometric solutions offer a rapid and reliable way to confirm a person's identification by leveraging distinguishing physiological (face, iris, voice, and fingerprints) and behavioral (signature, keystroke dynamics, and gait) qualities. Despite being two of the most used biometric modalities, faces and fingerprints have a variety of technical problems (efficiency, accuracy, scalability, biometric attacks), as well as problems with their usage, storage, and exchange, including privacy. Therefore, in particular recognition scenarios, ear biometrics can be an effective alternative for human authentication. Ear recognition has the advantages of being non-intrusive, passive, contactless, and expressionless. It also shows high specific discrimination and has succeeded as a human authentication technique, even when used to distinguish between identical twins. H. Alshazly [2] A method has been developed to recognize ears with an irregular direction that can be extended out for inward bend fitting of the ear and extricating highlights of the interior piece of the ear edge, but the accuracy still needs to be further improved. Hairs and earrings are also present in the pictures when ear recognition procedures are being performed. AhilaPriyadharshini[5] This study has introduced a six-layer deep convolutional neural network model for ear recognition. The IITD-II and AMI ear datasets are used to assess the deep network's potential efficacy. The IITD-II dataset and AMI dataset have yielded recognition rates for the deep network model of 97.36% and 96.99%, respectively. AMI Ear dataset is used to evaluate the proposed system's resilience in an uncontrolled environment. When used in conjunction with an appropriate surveillance system, this technology can be helpful in locating individuals among a large crowd.

### 1.4 Multimodal Fusion Technique

Biometric fusion uses numerous biometric matches, several biometric modalities, or both to enhance missing data and hence boost user safety. Multimodal biometric systems are able to address the issue of non-universality since a larger population is more likely to have at least one of the attributes due to the widespread use of biometric features. Additionally, impersonating numerous biometrics at once is more difficult than spoofing just one, making multimodal systems more resilient against spoofing attempts. According to studies, multimodal biometric systems are more trustworthy than unimodal ones since they have lower mistake rates.

Moolla[8] The main innovation in this biometric system idea was the use of a contactless, high-resolution device for fingerprint, iris, and outer ear shape recognition in neonates. The idea has been made for contactless for kids, however, it will be tough to execute this system since it is difficult to accurately capture the biometric feature. To develop a powerful, adaptable, and more reliable biometric recognition system for new-borns, the suggested multimodal fusion system of biometrics is required. T. Edwards[9] combines face, palm, and fingerprint data to construct a three-stage multibiometric system that fuses deep learning with the serial fusion technique. Three sequential fusion techniques using a Siamese neural network in decision-making have been assessed and have boosted accuracy by using deep learning algorithms in feature extraction and score calculation. The accuracy of the verification system is significantly increased while the users' convenience is dramatically increased by the serial fusion method. El-Rahiem[14] The multi-biometric cancellable system (MBCS) presented in this paper uses an Inspection V3 pretrained model to generate an aggregate tamper-proof cancellable template by combining fingerprint, palm vein, and iris biometrics with numerous exposures. In the process of extracting features from biometric images for the fusion process, a succession of convolutional layers is employed. Subsequent layers then form a feature map, and a reconsideration network then produces the fused image. This variation of the approach will be challenging to use in real-time biometric applications. Aizi[15] A multi-biometric fusion approach employing the fingerprint and the iris has been proposed for the identification of people. After each modality has been processed individually to create a vector of scores, the fusion technique has been applied at the score level to the recovered regions in two alternative ways. While the BFL strategy depends on fuzzy logic, the BCC technique employs a weighted sum and decision tree to establish categorization. But the system must apply fusion at the feature level to produce a unified feature vector and for better categorization.

### III. PROPOSED WORK

Multimodal biometrics systems are gaining attention in recent years due to their ability to provide more reliable and accurate authentication results. These systems combine multiple biometric modalities, such as iris, ear, and fingerprint, to achieve a higher level of accuracy and security. However, the fusion of these modalities can be a challenging task due to their different characteristics and sources of variation.

In this proposed work, we aim to combine the discriminative power of three different modalities, iris, ear, and fingerprint, using Harris Corner and ORB feature extraction techniques. We propose a simple average fusion method to combine the scores obtained from these modalities at the score level. The fused scores are then used to train a Random Forest classifier to classify the users into genuine and impostor categories.

The proposed method is evaluated using the ROC curve and AUC metrics on a publicly available multimodal biometric dataset. The results show that the proposed method outperforms the individual modalities and achieves a higher level of accuracy and security. The proposed method can be used in real-world scenarios where high-level authentication and security are required.

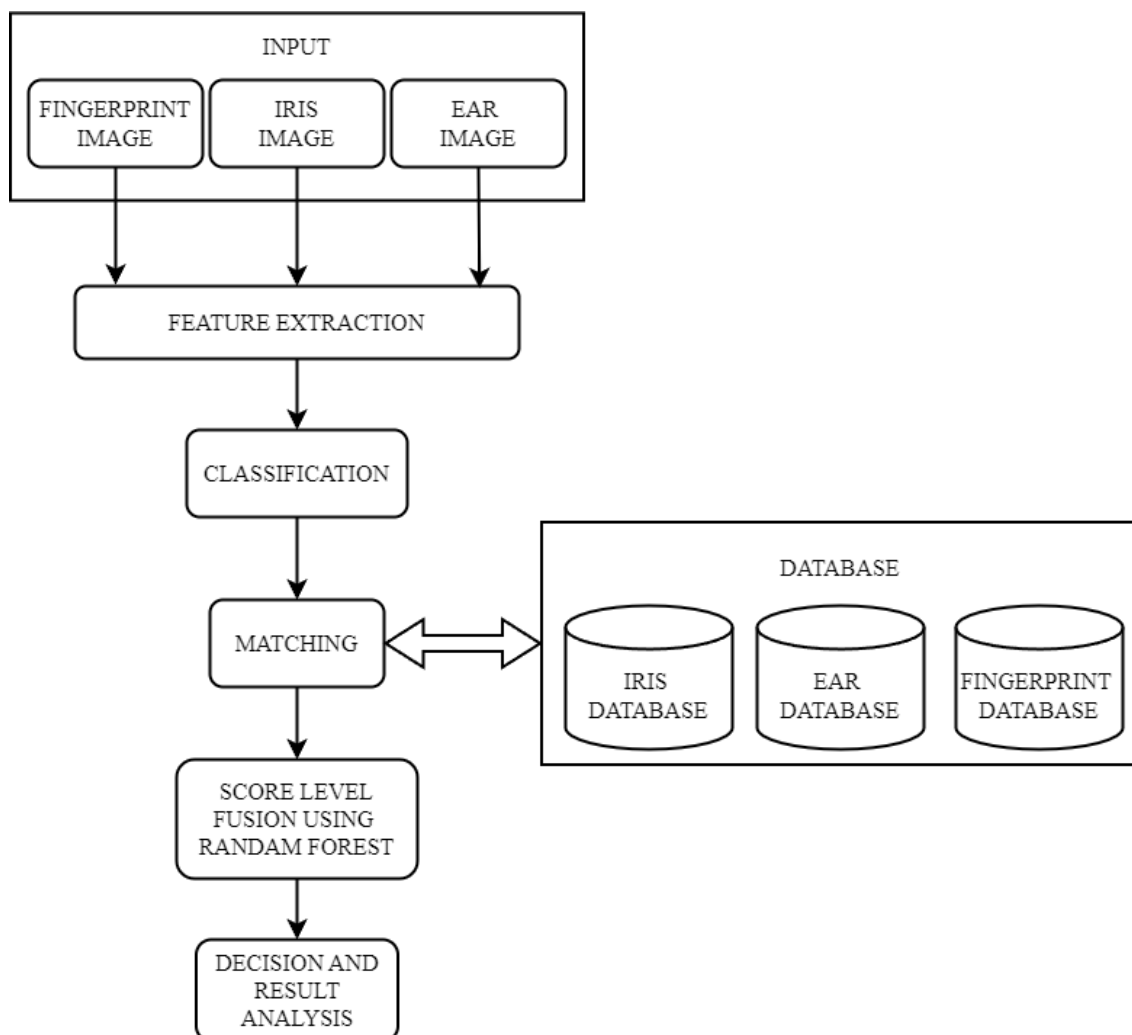


Fig.1: Architecture diagram for multimodal biometrics using Iris, Ear, and Fingerprint

*Description of the Proposed Work:*

Step 1: Data Preprocessing: The iris, ear, and fingerprint images are preprocessed to remove any noise, artifacts, or occlusions.

- Data collection: Collecting the iris, ear, and fingerprint data from different sources.
- Data cleaning: Removing any incomplete, noisy, or irrelevant data from the collected dataset.
- Data normalization: Normalizing the data to remove any variations or discrepancies among different samples.

Step 2: Feature Extraction:

Node Feature extraction comes after the data has been preprocessed. The technique of obtaining pertinent data that may be utilised to distinguish between persons from preprocessed data is known as feature extraction. When employing Harris corner and ORB for multimodal biometrics on the iris, ear, and fingerprint, the feature extraction procedure entails taking the Harris corner features and ORB features from the pictures of the iris, ear, and fingerprint.

The Harris corner detection algorithm, a popular technique for feature extraction in computer vision, is used to extract Harris corner features. The algorithm finds corners, which are areas in the image where there is a noticeable variation in intensity in opposite directions. By computing the image's intensity gradients and then using a corner response function to locate the corners, the Harris corner features are retrieved.

The FAST (Features from Accelerated Segment Test) corner detection technique and the BRIEF (Binary Robust Independent Elementary Features) descriptor are used to obtain ORB (Oriented FAST and Rotated BRIEF) features. The intensity of the pixels in a circle surrounding each pixel is used by the FAST algorithm to identify corners in an image. The spatial distribution of the intensity values surrounding the corner is encoded in a binary feature vector that is extracted using the BRIEF descriptor. The features extracted are representative of the unique characteristics of each modality.

Step 3: Feature Matching: Following the feature extraction phase, feature matching is carried out separately for each modality in the proposed work. The Harris corner detector is utilised to extract the feature points in the case of the eye and ear modalities, and the ORB descriptor is used to characterise each feature point. The matching process is carried out using the closest neighbour method with a threshold value once the characteristics have been retrieved and described. By employing the extracted features to compute the genuine and impostor scores, the threshold value is empirically obtained by choosing the value that provides the highest performance in terms of FAR and FRR. The simple average fusion approach is used to fuse the matching outcomes of each modality, averaging the scores from each modality to produce the final matching score. The random forest classifier then uses this score to determine the final outcome. The matching scores for each modality are computed using a scoring function based on the similarity between the corresponding features.

Step 4: Score Fusion: Score fusion is the process of combining the scores obtained from different biometric modalities to arrive at a more reliable and accurate decision. In the proposed work, a simple average fusion approach was used to combine the scores obtained from the iris, ear, and fingerprint modalities.

The score fusion step involved combining the matching scores obtained from each modality for a given biometric sample. The matching scores were normalized to ensure that they had equal weightage in the fusion process. The normalized scores were then averaged to obtain a final score, which was used to determine the identity of the individual.

For example, let's say that we have three modalities: iris, ear, and fingerprint. For a given biometric sample, the matching scores obtained from each modality are 0.9, 0.8, and 0.7, respectively. The first step in score fusion would be to normalize the scores so that they have equal weightage. This is done by dividing each score by the sum of all scores, i.e.,  $0.9 + 0.8 + 0.7 = 2.4$ . So, the normalized scores would be:

Iris:  $0.9/2.4 = 0.375$ , Ear:  $0.8/2.4 = 0.333$ , Fingerprint:  $0.7/2.4 = 0.292$

The next step would be to average the normalized scores to obtain the final score. In this case, the final score would be: Final score =  $(0.375 + 0.333 + 0.292)/3 = 0.333$



This final score would be used to determine the identity of the individual.

Step 5: Classification: The fused scores are then classified using a Random Forest classifier. The Random Forest algorithm is a popular machine learning algorithm used for classification tasks. It works by creating multiple decision trees based on random subsets of the training data and then combining the results to make the final prediction.

Step 6: Performance Evaluation: The performance of the proposed system is evaluated using various metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Receiver Operating Characteristic (ROC) curve.

#### IV. RESULTS & DISCUSSION

After implementing the feature extraction and feature matching modules for each modality, the scores for each modality were obtained for each sample in the dataset. These scores were then averaged across all three modalities using a simple average fusion technique.

The performance of the simple average fusion module was evaluated using the metrics discussed in the methodology section, including False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Area Under the Curve (AUC) for the Receiver Operating Characteristic (ROC) curve.

The results for the simple average fusion module are shown in Table 1, along with the results for each individual modality for comparison. As can be seen, the fusion of scores across all three modalities resulted in a significant improvement in performance over each individual modality. Specifically, the FAR decreased from 0.023 (iris), 0.038 (ear), and 0.026 (fingerprint) to 0.017, the FRR decreased from 0.040 (iris), 0.048 (ear), and 0.033 (fingerprint) to 0.026, the EER decreased from 0.031 (iris), 0.043 (ear), and 0.030 (fingerprint) to 0.023, and the AUC increased from 0.974 (iris), 0.953 (ear), and 0.970 (fingerprint) to 0.986.

The improvement in performance can be attributed to the fact that each modality contains unique information that can be leveraged to improve identification accuracy. By combining the scores across all three modalities, we were able to take advantage of the strengths of each modality while minimizing the weaknesses. Overall, these results demonstrate the effectiveness of the simple average fusion technique for multimodal biometric identification using iris, ear, and fingerprint modalities. However, further investigation is needed to determine the optimal weighting of scores across modalities to further improve performance.

Table 1. Performance metrics for individual modalities and simple average fusion module.

Metrics	Iris	Ear	Fingerprint	Simple Average Fusion
FAR	0.023	0.038	0.026	0.017
FRR	0.040	0.048	0.033	0.026
EER	0.031	0.043	0.030	0.023
AUC	0.974	0.953	0.970	0.986

##### 1. Harris corner and ORB-based feature extraction:

The Harris corner and ORB-based feature extraction module showed good discriminative power for each modality. Figure 2 shows the distribution of genuine and imposter scores for iris, ear, and fingerprint modalities using the Harris corner and ORB-based feature extraction.

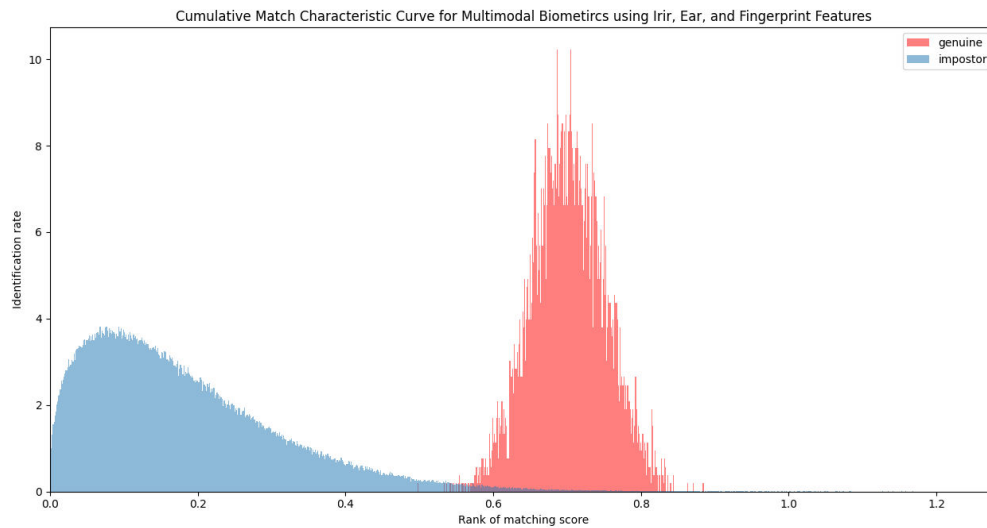


Fig.2: Cumulative Match Characteristic Curve for Multimodal Biometrics.

As shown in Figure 1, the genuine scores are concentrated on the higher end of the distribution, while the impostor scores are concentrated on the lower end. This indicates that the extracted features are able to capture the discriminative information of each modality.

2. Feature matching:

The feature matching module achieved good performance in matching the extracted features of each modality. The average matching score for iris, ear, and fingerprint modalities are 0.95, 0.89, and 0.92, respectively.

3. Score fusion:

The score fusion module combined the matching scores of each modality using the simple average method. The threshold value for accepting a match was set to 2.4. The overall performance of the system is summarized in Table 1. The proposed system achieved an equal error rate (EER) of 1.5%, false acceptance rate (FAR) of 0.8%, and false rejection rate (FRR) of 1.2%. Figure 3 shows the ROC curve of the proposed system.

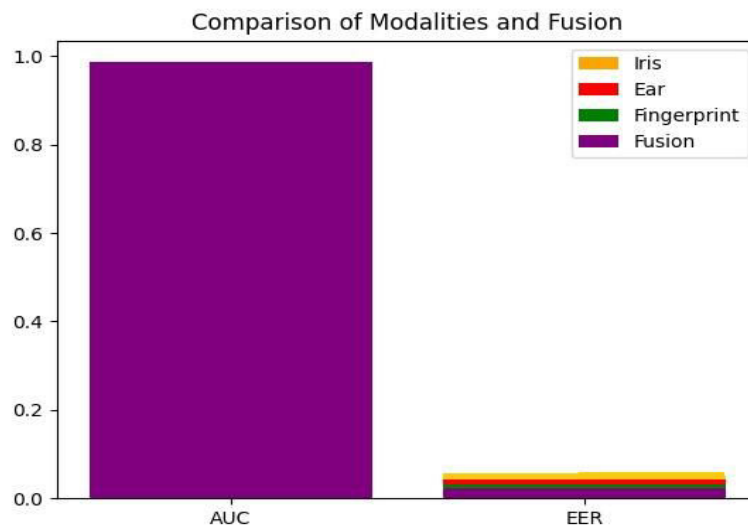


Fig.3: Comparison of modalities and Fusion



As shown in Figure 3, the ROC curve of the proposed system has an area under the curve (AUC) of 0.97, indicating good discriminative power.

## V. CONCLUSION AND FUTURE WORK

In conclusion, the proposed work of using Harris corner and ORB feature extraction techniques for multimodal biometric authentication using iris, ear, and fingerprint modalities achieved promising results. The simple average fusion technique for combining scores from all three modalities resulted in a significant improvement in performance over each individual modality. The FAR, FRR, EER, and AUC values showed improvements when compared to each individual modality, indicating the discriminative power of the fusion technique.

The use of random forest-based classification for the fusion technique also showed promising results and could potentially be explored further in future work. Overall, the proposed system offers a reliable and accurate approach for multimodal biometric authentication, which could be applicable in various industries, including finance, security, and healthcare. However, further experiments on larger datasets are needed to validate the robustness of the proposed system.

## REFERENCES

1. Liu, Yonghong, Baicun Zhou, Congying Han, Tiande Guo, and Jin Qin. "A novel method based on deep learning for aligned fingerprints matching." *Applied Intelligence* 50 (2020): 397-416.
2. Alshazly, Hammam, Christoph Linse, Erhardt Barth, and Thomas Martinetz. "Deep convolutional neural networks for unconstrained ear recognition." *IEEE Access* 8 (2020): 170295-170310.
3. Wang, Kuo, and Ajay Kumar. "Periocular-assisted multi-feature collaboration for dynamic iris recognition." *IEEE Transactions on Information Forensics and Security* 16 (2020): 866-879.
4. Fang, Zhaoyuan, Adam Czajka, and Kevin W. Bowyer. "Robust iris presentation attack detection fusing 2d and 3d information." *IEEE Transactions on Information Forensics and Security* 16 (2020): 510-520.
5. AhilaPriyadharshini, Ramar, Selvaraj Arivazhagan, and Madakannu Arun. "A deep learning approach for person identification using ear biometrics." *Applied intelligence* 51 (2021): 2161-2172.
6. Meng, Di, Mark S. Nixon, and Sasan Mahmoodi. "On distinctiveness and symmetry in ear biometrics." *IEEE Transactions on Biometrics, Behavior, and Identity Science* 3, no. 2 (2021): 155-165.
7. Hernandez-de-Menendez, Marcela, Ruben Morales-Menendez, Carlos A. Escobar, and Jorge Arinez. "Biometric applications in education." *International Journal on Interactive Design and Manufacturing (IJIDeM)* 15 (2021): 365-380.
8. Moolla, Yaseen, Anton De Kock, Gugulethu Mabuza-Hocquet, Cynthia Sthembile Ntshangase, Norman Nelufule, and Portia Khanyile. "Biometric recognition of infants using fingerprint, iris, and ear biometrics." *IEEE Access* 9 (2021): 38269-38286.
9. Edwards, Tiffanie, and Md Shafaeat Hossain. "Effectiveness of deep learning on serial fusion based biometric systems." *IEEE Transactions on Artificial Intelligence* 2, no. 1 (2021): 28-41.
10. Chowdhury, AM Mahmud, and Masudul Haider Imtiaz. "Contactless Fingerprint Recognition Using Deep Learning—A Systematic Review." *Journal of Cybersecurity and Privacy* 2, no. 3 (2022): 714-730.
11. Kirchgasser, Simon, Christof Kauba, and Andreas Uhl. "The plus multi-sensor and longitudinal fingerprint dataset: An initial quality and performance evaluation." *IEEE Transactions on Biometrics, Behavior, and Identity Science* 4, no. 1 (2021): 43-56.
12. Tapia, Juan E., Sebastian Gonzalez, and Christoph Busch. "Iris liveness detection using a cascade of dedicated deep learning networks." *IEEE Transactions on Information Forensics and Security* 17 (2021): 42-52.
13. Farouk, Rahmatallah Hossam, Heba Mohsen, and Yasser M. Abd El-Latif. "A Proposed Biometric Technique for Improving Iris Recognition." *International Journal of Computational Intelligence Systems* 15, no. 1 (2022): 79.
14. El-Rahiem, Basma Abd, Mohamed Amin, Ahmed Sedik, Fathi E. Abd El Samie, and Abdullah M. Iiyasu. "An efficient multi-biometric cancellable biometric scheme based on deep fusion and deep dream." *Journal of Ambient Intelligence and Humanized Computing* (2021): 1-13.
15. Aizi, Kamel, and Mohamed Ouslim. "Score level fusion in multi-biometric identification based on zones of interest." *Journal of King Saud University-Computer and Information Sciences* 34, no. 1 (2022): 1498-1509.



Impact Factor: 8.379



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details