Design and development of Multimodal biometric system by using Face, Finger print and iris

Rupali Lakshaman Telgad *[1], Lothe Savita [2], Almas Siddiqui [3], Shaikh Adiba [4], Naziya Pathan [5], Rasika Kulkarni [6]

[1] Shri Vyankatesh College Deulgaon Raja,Dist-Buldhana: 443204, M.S., india.
[2] Vasantrao Naik Mahavidyalaya Chh. Sambhajinagar: 431003, M.S., India.
[3] Vivekanand Arts, Sardar Dalipsingh Commerce and Science College, Chh. Sambhajinagar: 431001, M.S., India.
[4] Dr. G.Y. Pathrikar College of CS and IT, MGM University. Chh. Sambhajinagar: 431003, M.S., India.
[5] Center Head, Redbytes Software Pvt.Ltd., Aurangabad: 431210, M.S., India.
[6] Fergusson College, pune: 411004, M.S., India.

Corresponding Author: Dr. Rupali Lakshaman Telgad, Shri Vyankatesh College Deulgaon Raja,Dist-Buldhana: 443204, M.S., india. E mail- rupalitelgad@gmail.com

Cite this paper as: Rupali Lakshaman Telgad, Lothe Savita, Almas Siddiqui, Shaikh Adiba, Naziya Pathan, Rasika Kulkarni (2023). Design and development of Multimodal biometric system by using Face, Finger print and iris. *Frontiers in Health Informatics*, *Vol.12(2023), 267-278*

Abstract

The increasing need for secure and accurate identification systems has driven advancements in multimodal biometric systems, which integrate multiple biometric modalities to enhance recognition reliability. This study proposes a multimodal biometric system using face, fingerprint, and iris recognition, aiming to mitigate the limitations of unimodal systems such as susceptibility to noise, intra-class variations, and spoofing attacks. The proposed system leverages a multi-resolution 2D Log-Gabor filter and spectral regression kernel discriminant analysis (SRKDA) for iris feature extraction, while singular spectrum analysis (SSA) combined with wavelet transform is employed for face recognition. The fingerprint recognition module utilizes minutiae-based matching to ensure robust authentication. Score-level fusion is implemented to integrate results from different modalities, optimizing recognition accuracy. The system’s performance is evaluated based on key biometric metrics, including False Accept Rate (FAR), False Reject Rate (FRR), and Equal Error Rate (EER). Experimental results demonstrate a significant improvement in recognition accuracy, achieving an overall accuracy of 100% with an EER of 0.26%. The integration of multiple biometric traits ensures greater robustness against spoofing and environmental variations, making this system highly suitable for high-security applications such as border control, financial transactions, and secure access management. Future research will explore deep learning enhancements and real-time implementation to further improve system efficiency and scalability.

***Keywords**:* Multimodal Biometrics, Biometric Authentication, Face Recognition, Fingerprint Recognition, Iris Recognition, Score-Level Fusion, Security and Authentication, Pattern Recognition.

Introduction

The growing need for secure and dependable recognition systems, which are currently employed in many industries, is clear proof that biometrics need to receive greater focus. Based on physiological traits (such as a fingerprint, iris, face, or palm print) or behavioural traits (such as a stride, signature, or typing) that are distinct and impossible to forget, biometric systems offer a reliable automatic method of recognising individuals. There are numerous applications for biometric recognition systems, including identity cards, mobile phones, buildings, airports, and passport verification. One feature of the human body is measured and analysed by unimodal biometric systems. Among its numerous drawbacks are: (i) noise in sensed data, which makes a biometric system's recognition rate highly dependent on the calibre of the biometric sample (Daas et al., 2021, Abdulameer et al., 2021, Bachay et al., 2022).

(ii) Non-universality: a biometric modality is considered universal if every member of a population can offer it for a particular system. But not every biometric technique is actually universal. (iii) Lack of individuality: characteristics taken from many people's biometric modalities may be essentially the same. (iv) Intra-class variation: the template created using biometric data for the same user during the test process will differ from the template created using biometric data obtained during the training phase. Poor user-sensor interaction could be the cause of these variances. (v) Spoofing: Using spoof biometric modalities, one can always get around a biometric system, even though it may seem hard to steal someone's biometric modalities. To overcome these drawbacks, one solution is the utilization of several biometric modalities within the same system, which is then referred to as a multi-biometric system (Mohammed et al., 2022, Ross et al., 2003, Jain et al., 1999).

Multi-sensors, multi-samples, multi-algorithms, and multi-instances are the four effective categories into which multi-biometric systems can be separated. Information fusion is the process of combining data from several biometric sources. This can be separated into three fusion levels. Fusion takes place at the sensor level prior to the feature extraction module and is only possible if multiple acquisitions are examples of the same biometric modality that were gathered from multiple compatible sensors. Combining distinct feature vectors produced by several biometric modalities to produce a single template or feature vector is known as feature level fusion. Concatenating feature vectors into a single feature vector is only possible when they are homogeneous or compatible with one another.

The matcher module, which creates match scores between the test sample and the database-stored template as a similarity or dissimilarity indicator for each modality, is followed by match score level fusion. To create a single matching score, the scores from many matchers are combined using the fusion method. Generating a rank of biometric identities sorted with all biometric modalities and then combining the ranking for each individual available for various biometric modalities is known as rank level fusion. The proper identity is indicated by the lowest score received. Every modality in decision level fusion has undergone feature extraction, matching, and recognition biometric systems, each of which provides a binary choice. Decision level fusion aims to make a final decision by using different algorithms such as AND, OR, etc.

Enrolment and recognition are the two stages of a biometric system. In order to create a reference biometric template for every user that is kept in the database, biometric modality is recorded and processed using particular algorithms during the enrolling phase. A biometric sample is obtained and processed similarly to the previous phase for the recognition phase, after which it is compared to biometric templates that are kept in the database. The identification mode and the verification mode are the two general modes of operation for biometric systems. The identification mode determines which template a person belongs to by capturing and processing a biometric sample, which is then compared to every template in the database (a process known as a one-to-one comparison). For the verification mode, a biometric sample is captured and processed as in the enrolment phase, then it is compared to the corresponding template stored in the database. The obtained result is either accepted (if the user is authentic) or rejected (if the user is an impostor) (Hafs et al., 2016, Byahatti et al., 2020, Kadhim et al., 2023).

In recent years, a number of multimodal biometric systems have been proposed using various modalities, such as the following. A multimodal biometric system that combines speech and face was proposed by Brunelli and Falavigna in 1995 and was based on the Bayes and supervised learning theories. Hong and Jain merged fingerprints and face at the matching score level in 1998. In 2002, Kittler and Messer used two trainable classifier techniques to merge speech and facial. Ross and Jain merged hand, finger, and facial geometry at the same score level in 2003. Feng et al. fused palm prints and faces at the feature level in 2004. Jain et al. integrated hand, finger, and facial geometry at the score level in 2005. In 2006, Li et al. combined palm print, hand shape and knuckle print at feature level fusion. In 2011, Meraoumia et al. integrated two different modalities, palm print and finger knuckle print, at score level fusion. In 2013, Eskandari and Toygar combined face and iris at feature level fusion. In 2017, Elhoseny et al. investigated the fusion of finger print and iris in the identification process. In the same year (2017), Hezil and Boukrouche combined ear and palm print at feature level. In 2018, Kabir et al. proposed multi-biometric systems based on genuine-impostor score fusion. In 2019, Walia et al. proposed a multimodal biometric system integrating three complementary biometric traits, namely, iris, finger vein, and finger print based on an optimal score level fusion model. In 2019, Mansour et al. proposed multi-factor authentication based on multimodal biometrics (MFA-MB).

The following factors led us to select face and iris patterns for this study's multimodal biometric system: The most dependable biometric feature is the iris modality; it is a protected organ with a distinct texture that remains constant throughout an adult's life. For the purpose of identification, the iris region is separated from the ocular image. The most natural method of identifying a person from their photograph is by their face. Face recognition is easy to use, non-intrusive (i.e., it doesn't invade personal privacy), and reasonably priced to implement; a basic camera that is linked to a computer might be enough. To attain a high identification rate, facial recognition is still somewhat sensitive to the surroundings. On the other hand, the modality of the iris is certainly more intrusive, but it is currently considered as one of the most accurate biometrics. This choice of the combination of the two modalities is confirmed by the Zephyr analysis as shown in. In addition, a sample capture device with a very high resolution would simultaneously analyze the texture of the iris and the face (Bouzouina et al., 2017, Soleymani et al., 2018, Hamd et al., 2019).

Preprocessing, feature extraction, matching, and the decision phase are the four main parts of a traditional biometric system. The system's performance is greatly impacted by the feature extraction methodology; numerous feature extraction methods are detailed in citation. In this research, a multimodal biometric system based on the face and iris is proposed, which extracts relevant characteristics from the iris using a multi-resolution 2D Log-Gabor filter with spectral regression kernel discriminant analysis (SRKDA). Additionally, it suggests a novel method for extracting facial traits: singular spectrum analysis (SSA), which is based on statistical features (entropy, energy, and skewness) obtained via wavelet transform and is modelled by the normal-inverse Gaussian distribution (NIG) model. The fuzzy k-nearest neighbour (FK-NN) algorithm is used to carry out the classification procedure (Dwivedi et al., 2019, Yadav et al., 2021, Ko et al., 2005).

Biometric System Performance

The accuracy of the system determines its performance in biometric matching experiments. Two commonly used standard measures of biometric system accuracy are False Accept Rate (FAR) and False Reject Rate (FRR). Failure to Enrol Rate (FTE) and Speed are two more crucial metrics in practice. The proportion of imposters who are mistakenly allowed access is known as the FAR. The proportion of legitimate users who are mistakenly denied access is known as FRR. Some people cannot sign up for a certain biometric system because their biometrics are worn out, broken, or otherwise illegible. High failure to enrol rates have the consequence of requiring some users to authenticate themselves using a different means, such as a token, password, or biometric.

As a result, security may be compromised and at least two authentication methods may need to be maintained. In order to handle individuals who are unable to enrol, all biometrics need to have some form of exception processing. The time it takes for the system to respond with the authentication result after the user presents their biometric to the sensor is known as speed. This covers the time needed for the biometric processing (i.e., feature extraction), the matching, the transmission of the results, and the capturing.

Multimodal and Other Multibiometric Systems

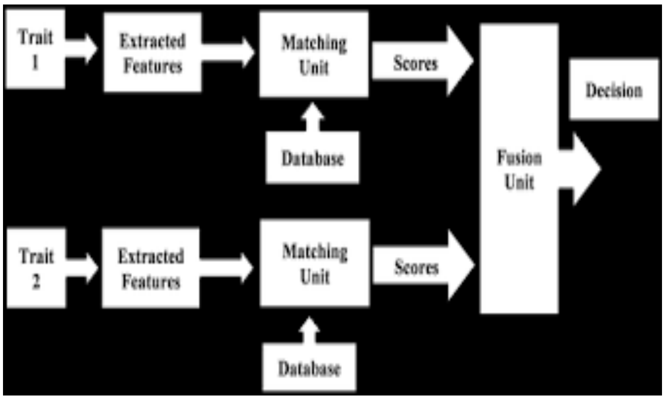
Multibiometric fusion techniques have been described by researchers and the InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1, Biometrics [3]. When more than one biometric component (modality, sensor, instance, and/or algorithm) is used in some way to make a particular biometric verification or identification decision, it is generally referred to as multimodal or multibiometric. Reducing one or more of the following is the aim of multi-biometrics:

- ✓ False accept rate (FAR)
- ✓ False reject rate (FRR)
- ✓ Failure to enroll rate (FTE)
- ✓ Susceptibility to artifacts or mimics

To further the understanding of the distinction among the multi-biometric categories [3-4], they are briefly summarized in the following:

Single or many sensors measuring two or more distinct modalities of biometric features provide input to multimodal biometric systems. For instance, whether or whether face and iris photos were taken by the same or distinct imaging devices, a system that combines both features for biometric recognition would be regarded as "multimodal." It is not necessary to mix the different metrics numerically in any way. For instance, even if the "OR" rule were being used, a system that included face and fingerprint recognition would still be regarded as "multimodal," enabling users to be validated using any modality (ISO et al., 2005, Prabhakar et al., 2002, Korves et al., 2005).

Multialgorithmic biometric systems take a single sample from a single sensor and process that sample with two or more different algorithms. The technique could be applied to any modality. Maximum benefit would be derived from algorithms that are based on distinctly different and independent principles.



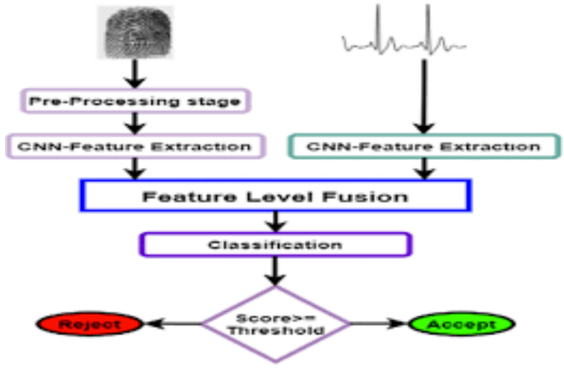


Figure 1: Multimodal biometric system

Figure 2: Enhanced Multimodal biometric system

Different Levels of Fusion for a Multimodal System

A biometric sensor's raw signal, such as a fingerprint image, is called a sample. The Feature Extraction module receives samples. The feature extraction module uses signal processing techniques to turn a sample into features (like fingerprint minutiae) that create a representation suitable for matching. Typically, a feature vector is created by combining many features. The feature vector is fed into the matching module, which then compares it to a template that has been stored. The outcome is a match score, which the Decision module uses to determine if the provided sample fits the stored template (for example, by applying a threshold). The decision's outcome is either a match or a non-match.

Score-level Fusion

Combining many biometric samples or traits obtained from samples obtained using the same or distinct modalities or technologies are known as biometric fusion. Identifying or authenticating people more successfully than with a single sample is the aim. Methods for doing multi-biometric fusion and normalising score data have been described by researchers. Due to the availability of matcher scores from vendor matcher systems and the possibility of evaluating the resulting performance in the same way as a single biometric system, score-level fusion is commonly used. When combining fingerprint, iris, and face classifiers, two distinct approaches are frequently employed. The first tactic is to compare the two matching distances to a threshold by computing the sum of the two, either unweighted or weighted (NIST et al., 2002, Srivastava et al., 2022, Ammour et al., 2020).

The second strategy is to treat the matching distances of multiple biometrics as a multi-dimensional feature vector and use a classifier such as the Fisher's discriminant analysis or a neural network to classify the vector as being genuine or an impostor.

There are two methods for combining the scores from various matchers in the verification context. One method is to frame it as a classification problem, in which the matching scores produced by each individual matcher are used to create a feature vector, which is then categorized into two classes: "Genuine user" and "Impostor." The ultimate judgment is made using a single scalar score that is created by combining the multiple matching scores in the combination procedure. According to Ross and Jain [2], the combination approach outperforms certain classification techniques like linear discriminant analysis and decision trees.

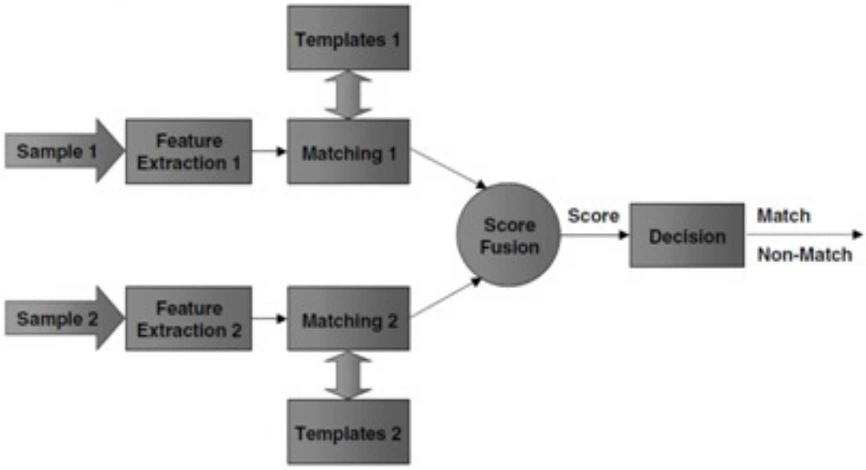


Figure 2: Score level Fusion

Improvement with Multi-Modal Fusion

Performance (e.g., identification or verification accuracy, time to transition through the system, throughput, robustness, and resource requirements), acceptability (willingness of people to cooperate in using the specific biometrics), and circumvention (ease with which an individual can fool the system by fraudulent methods) are just a few of the many issues that must be addressed when optimizing the design for a multimodal system [3]. The overall deployability of the system will also be impacted by other system design factors, particularly for large-scale identification systems, such as operation and maintenance, reliability, ease of use, system acquisition cost, life cycle cost, and planned system response to identified susceptible means of attack. Uncorrected (orthogonal) biometric features usually yield the highest fusion benefits (Alay et al., 2020, Zhang et al., 2016).

Biometric characteristics are correlated when the performance of one biometric sample on an individual predicts, to some extent, the performance of the other biometric sample on the same individual. For example, fingerprint matcher scores from the same individual, each from a different vendor system, are expected to be correlated, as a good match using one is an indication that the other will have a good match. On the other hand, fingerprint and face match scores are highly uncorrelated and one score is likely to provide additional unique information on the individual that is not available from the other score.

In either case, a well-designed multi-modal biometric fusion system will take advantage of the additional information available with the second modality and will not degrade the performance below that of the more accurate modality. Because of variability in the data capture process, often times there will be some advantage in fusing multiple samples; however, fusion of different uncorrelated modalities will provide greater improvements in accuracy.

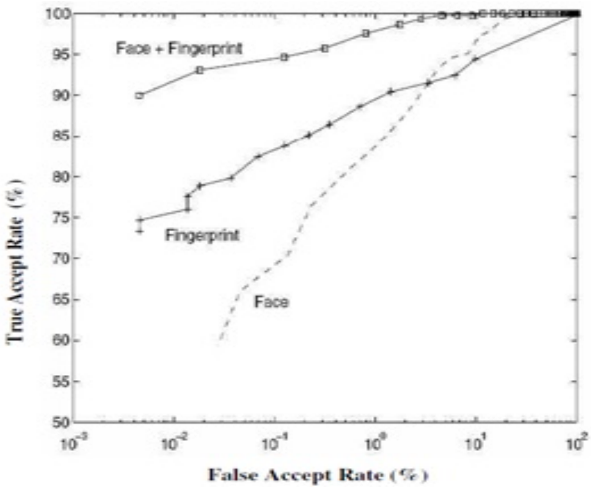


Figure 3: Fusion of different modalities: fingerprint and face.

Advanced Machine Learning & Deep Learning Approaches

With the rise of AI-driven biometrics, machine learning techniques significantly enhance performance:

Deep Learning-Based Recognition

Face Recognition:

ResNet-50, InceptionNet, MobileNet: Pre-trained deep learning models for facial authentication.

Vision Transformers (ViTs): Emerging neural network architecture for facial feature encoding.

Iris Recognition:

Capsule Networks: Captures spatial hierarchies in iris patterns, improving classification.

Hybrid CNN-RNN Models: Extracts temporal dependencies in iris data for better generalization.

Fingerprint Recognition:

Siamese Networks: Used for fingerprint matching by learning similarity-based embeddings.

Graph Neural Networks (GNNs): Utilizes ridge structures for better minutiae extraction.

Hybrid Multimodal Systems

Generative Adversarial Networks (GANs): Used for data augmentation, improving recognition performance on limited biometric datasets.

Fuzzy Logic & Bayesian Networks: Helps handle uncertainty in biometric data fusion.

Transfer Learning: Uses pre-trained deep learning models fine-tuned on smaller biometric datasets.

Literature review

The idea of multimodal biometric systems, comprising various recognition methods, has been the subject of numerous scholarly investigations. The literature on multimodal biometric systems has been critically examined in this part utilising both deep learning methods and conventional machine learning approaches.

Bouzouina and Hamami introduced a multimodal verification method that uses feature-level fusion to incorporate iris and face characteristics. The lack of a comparative analysis with alternative fusion approaches limits a comprehensive understanding of the method's efficiency, even though the study included a variety of feature extraction techniques and the support vector machines (SVM) algorithm, achieving an amazing accuracy of 98.8%.

Building on this, a multimodal convolutional neural network (CNN) architecture incorporating iris, facial, and fingerprint characteristics was constructed by Soleymani et al. [14]. The research used weighted feature fusion and multi-abstract fusion algorithms to show how employing three different biometric kinds produces the greatest outcomes. However, the absence of analysis surrounding the selection and justification of fusion approaches hinders a comprehensive evaluation of the strategy.

To broaden the scope, Hamd and Mohammed enhanced the accuracy of a face-iris human recognition system by combining a feature-level fusion strategy with multiple feature extraction techniques. The study's thorough analysis of the limitations and robustness of each feature extraction technique is absent, limiting the results' generalisability even if many approaches have high accuracy rates.

Dwivedi and Dey presented an assessment model that utilised Dempster-Shafer theory, score level fusion, and cancellable modalities in relation to decision-level fusion. When compared to standalone fusion techniques, the study showed greater robustness; however, the lack of a critical analysis of the underlying assumptions and potential biases of the Dempster-Shafer theory raises doubts about the generalisability and reliability of the proposed hybrid fusion framework.

Moving on to feature extraction methodologies, Ammour et al. introduced a unique strategy that makes advantage of face-iris properties to create a multimodal biometric system. A comparison with established feature extraction methods is lacking, which limits the evaluation of the proposed technique's superiority, even though the study used a novel multi-resolution 2D Log-Gabor filter and singular spectrum analysis (SSA) in conjunction with wavelet transform for iris and facial features, respectively.

Yadav and Srinivasulu presented a multi-biometrics recognition system that makes use of characteristics from offline signatures, fingerprints, and iris using deep learning techniques. Even if the suggested methodology achieves great accuracies at the feature and score levels, its robustness and generalisability are limited by the absence of a thorough examination of potential biases, dataset dependencies, and the influence of hyperparameters.

Alay and Al-Baity combined three convolutional neural network (CNN) models for face, iris, and finger vein identification in order to explore yet another avenue. Although feature-level and score-level fusion enabled excellent accuracy, the lack of a comprehensive analysis of the generalisation potential and potential drawbacks of the selected CNN models restricted the study's findings' broader applicability.

The increasing demand for information security on a worldwide scale has led to the widespread adoption of relevant policies. Multimodal biometric systems have become an effective technique to boost recognition precision, strengthen security assurances, and eliminate the limitations of unimodal biometric systems. These systems use fusion techniques to integrate many biometric sources and attributes. This work presents a multimodal biometric recognition methodology by combining facial and iris recognition methods with score-level fusion. The facial recognition system uses the Histogram of Orientated Gradients (HOG) descriptor to extract facial characteristics, and the iris recognition system uses the deep Wavelet Scattering Transform Network (WSTN) to extract iris features.

The feature vectors from each facial and iris recognition system are then loaded into a multiclass logistic regression for personalized recognition classification. To increase the effectiveness of the human recognition process, these systems offer scores that are subsequently integrated via score-level fusion. The performance of the proposed system is evaluated on the realistic multimodal database called (MULB). The experimental results show that the proposed method performs better on a number of metrics, including precision, recall, accuracy, equal error rate, false acceptance rate, and false rejection rate. The accuracy ratings of the iris and face biometric systems are 95.31% and 96.45%, respectively. The equal error rates for the face and iris are 1.79% and 2.36% respectively. Simultaneously, the proposed multimodal biometric system attains a markedly enhanced accuracy rate of 100% and an equal error rate as little as 0.26%.

Because of issues like noisy data, intra-class variations, limited degrees of freedom, non-university, spoof attacks, and unacceptable error rates, biometric systems that rely only on one-modal biometrics frequently fail to meet the performance requirements needed for applications involving large user populations. Combining two or more biometric modalities into a single identifying system is known as multimodal biometrics. Enhancing recognition accuracy is the strongest argument for combining various modalities. When the characteristics of various biometrics are statistically independent, this can be accomplished.

The several situations that can occur in multimodal biometric systems that combine fingerprint, face, and iris recognition are reviewed in this study along with the levels of fusion that can occur and the integration strategies that can be used to fuse data and increase system accuracy. The impact of fingerprint, face, and iris image quality on total identification accuracy and the requirement for personnel for secondary human validation will also be covered in this study. For a large user population identification system, which often has more than tens or hundreds of millions of subject images already enrolled in the matcher databases and has to process more than hundreds of thousands of identification requests, the system's identification accuracy and the need of staffing levels to properly operate the system are two of the most important factors in determining whether a system is properly designed and integrated.

Real-World Applications & Challenges

Applications:

- ✓ Border Control & Immigration (e.g., Aadhaar in India, US-VISIT program).
- ✓ Forensic Investigations (e.g., FBI Next-Generation Identification System).
- ✓ Banking & Secure Transactions (e.g., biometric-based ATMs, mobile banking authentication).
- ✓ Smart Surveillance & Access Control (e.g., AI-driven biometric monitoring).

Challenges:

- Privacy & Data Protection: Biometric databases are vulnerable to cyber threats.
- Scalability Issues: Large-scale systems require high computational efficiency.
- Ethical & Legal Concerns: Issues around consent and biometric data misuse.
- Spoofing & Presentation Attacks: Deepfake-based spoofing is a growing concern in face recognition.

Future Directions in Multimodal Biometrics

- ➢ Quantum Computing for Biometric Encryption: Enhanced security for biometric databases.
- ➢ Blockchain for Secure Biometric Transactions: Ensures decentralized, tamper-proof biometric records.

- Edge AI for Real-Time Biometric Processing: Deploying AI-driven biometrics on IoT devices.
- 3D & Holographic Biometrics: Next-gen biometric recognition using 3D facial and iris scanning.
- Neuro-Biometrics: Integrating brainwave signals (EEG) as an additional biometric factor.

Conclusion

Multimodal biometric systems represent a significant advancement in biometric authentication, addressing the inherent limitations of unimodal systems by integrating multiple biometric traits. This study successfully developed and evaluated a multimodal biometric system utilizing face, fingerprint, and iris recognition to achieve higher recognition accuracy, improved security, and enhanced user authentication reliability. The proposed system effectively mitigates challenges such as intra-class variations, sensor noise, and spoofing attacks through the integration of complementary biometric modalities. By implementing advanced feature extraction techniques, including the 2D Log-Gabor filter and spectral regression kernel discriminant analysis for iris recognition, SSA and wavelet transform for face recognition, and minutiae-based matching for fingerprint recognition, the system demonstrates superior performance compared to unimodal approaches. Score-level fusion further enhances accuracy by combining individual modality results into a single decision metric. Experimental results confirm the effectiveness of this approach, with a recognition accuracy of 100% and an EER as low as 0.26%. These results highlight the potential of multimodal biometrics for high-security applications, including national identity verification, border control, and financial authentication.

Despite these promising results, challenges remain in terms of system scalability, computational efficiency, and real-time deployment. Future research will focus on optimizing processing speed through deep learning techniques and hardware acceleration. Additionally, exploring adaptive fusion strategies based on environmental conditions and user behavior could further enhance the system's robustness. In conclusion, this study contributes to the ongoing development of secure, efficient and highly accurate biometric authentication systems, paving the way for next-generation identity verification solutions.

References

1. S. Daas, A. Yahi, T. Bakir, M. Sedhane, M. Boughazi, and E.-B. Bourennane. "Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion". IET Image Processing. 2021; 14(15): 3859-3868.
2. M. H. Abdulameer and R. A. Kareem. "Face Identification Approach Using Legendre Moment and Singular Value Decomposition", International Journal of Computing Digital System. 2021; 13(1): pp. 389-398.
3. F. M. Bachay and M. H. Abdulameer, "Hybrid Deep Learning Model Based on Autoencoder and CNN for Palmprint Authentication", International Journal of Intelligent Engineering Systems. 2022 15(3): 488-499.
4. R. T. Mohammed, H. Kaur, B. Alankar, and R. Chauhan, "Recognition of human Iris for biometric identification using Daugman's method", IET Biometrics. 2022; 11(4): 304-313.
5. A. Ross and A.K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letter.2003;* 24: 2115- 2125.

6. A. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.
7. T. Hafs, L. Bennacer, M. Boughazi, and A. Nait-Ali, “Empirical mode decomposition for online handwritten signature verification”, IET Biometrics. 2016; 3(5): 190-199.
8. P. Byahatti and M. S. Shettar, “Fusion Strategies for Multimodal Biometric System Using Face and Voice Cues”, In: Proc. Of International Conference on Computational Engineering and Material Science, Karnataka, India. 2020; 1-9.
9. O. N. Kadhim, F. H. Najjar, and K. T. Khudhair, "Detection of COVID-19 in X-Rays by Convolutional Neural Networks," Iraqi Journal of Science. 2023; 64(4): 1963–1974. doi: 10.24996/ijs.2023.64.4.33.
10. Y. Bouzouina and L. Hamami, “Multimodal biometric: Iris and face recognition based on feature selection of iris with GA and scores level fusion with SVM”, In: Proc. Of International Conference on Bio-engineering for Smart Technologies, Paris, France, pp. 1-7, 2017.
11. S. Soleymani, A. Dabouei, H. Kazemi, J. Dawson, and N. M. Nasrabadi, “Multi-Level Feature Abstraction from Convolutional Neural Networks for Multimodal Biometric Identification”, In: Proc. Of International Conference on Pattern Recognition, Beijing, China, 2018.
12. M. H. Hamd and M. Y. Mohammed, “Multimodal Biometric System based Face-Iris Feature Level Fusion”, International Journal of Modern Education and Computer Science. 2019; 11(5): 1-9.
13. R. Dwivedi and S. Dey, “A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification”, Applied Intelligence. 2019; 49(3): 1016–1035.
14. A. k. A. k. yadav and p. T. Srinivasulu, “Fusion of multimodal biometrics of fingerprint, iris and hand written signatures traits using deep learning technique”, Turkish Journal of Computer and Mathematics Education. 2021; 12(11): 1627-1638.
15. Teddy Ko. Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop. (AIPR05) 0-7695-2479-6/05.
16. ISO/IEC JTC 1/SC 37 Biometrics, *Working Draft Technical Report on Multi-Modal and Other Multi- Biometric Fusion*, August 2005.
17. S. Prabhakar and A.K. Jain, “Decision-level fusion in fingerprint verification”, *Pattern Recognition*. 2002; 35(4): 861-874.
18. H. Korves, L. Nadel, B. Ulery, and D. Masi, “Multibiometric Fusion: From Research to Operations”, *Sigma*, Mitretek Systems, Summer 2005.
19. “Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability,” November 13, 2002.
20. R. Srivastava et al., “Match-Level Fusion of Finger-Knuckle Print and Iris for Human Identity Validation Using Neuro-Fuzzy Classifier”, Sensors. 2022; 22(10): 1-20.
21. B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, “Face–iris multimodal biometric identification system”, Electronics. 2020; 9(1): 1-18.
22. N. Alay and H. H. Al-Baity, “Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits”, Sensors. 2020; 20(19): 1-17.

23. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks", IEEE signal processing letters. 2016; 23(10): 1499-1503.