RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 08, Issue 01 January

Check for updates

http://dx.doi.org/10.47392/IRJASH.2026.003

Improving Biometric Security Through Multimodal Fusion and Deep Hashing

Ms. S. Jebapriya[1]*, Dr. M. Ganaga Durga*[2]

[1]*(Ph.D.,) Research Scholar, Department of Computer Science, Madurai Kamaraj University, Madurai, Tamilnadu, India.*

[2]*Associate Professor, Department of Computer Applications, Sri Meenakshi Govt. Arts College for Women(A), Madurai, Tamilnadu, India.*

Emails: *jebapriyas.research@gmail.com*[1]*, sivamgdurga@gmail.com*[2]

Article history

Received: 20 October 2025
Accepted: 10 November 2025
Published: 13 January 2025

Keywords:

Biometric Security; Deep Hashing; Face; Fingerprint; Iris.

Abstract

Biometric security technologies are increasingly important for protecting sensitive information and securing access control. There are inherent problems related to spoofing, privacy and data security in traditional monomial biometric systems. In this paper, we proposed a novel deep learning framework to enhance the biometrics security by using multispectral face, iris and fingerprint information. Combining deep hashing into the proposed fusion framework, a strong binary multimodal latent representation is generated which is robust in presence of fake attempts. The proposed approach also integrates a hybrid security framework (combining cancellable biometrics and secure sketch method) for improving security of biometric templates. Furthermore, deep auto encoder algorithm is applied for feature extraction to get improved encoded features in order to boast security. The efficacy of the approach is demonstrated on a multimodal face, iris and fingerprint biometric database, resulting in improved performance along with enhanced privacy through cancelability and unlink ability of biometrics templates. Deep hashing function is also tested on an image retrieval dataset task as well standard one where the network structure could be applied're used and it shows similar adaptability.

1. Introduction

Biometric security systems are increasingly recognized as essential tools for safeguarding sensitive information and ensuring secure access to various applications. In an era of rising digitalization, protecting personal and sensitive information has become a top priority. Traditional authentication techniques, such as passwords and PINs, have security flaws that include phishing attempts, credential leaks, and brute-force assaults. Biometric authentication, which uses unique physiological or behavioral attributes like fingerprints, facial features, and iris patterns, is a more dependable and user-friendly option. However, unimodal biometric systems, which rely on a single biometric feature, present substantial obstacles, such as spoofing vulnerability, ambient fluctuations, and template security threats. Previous methodologies in biometric security have focused on single-modal systems, which, despite their advantages, have limitations in terms of robustness and vulnerability to attacks. For instance, face recognition systems, though widely used, are susceptible to spoofing through photographs or videos. Similarly, fingerprint recognition, while generally reliable, can be compromised through the use of artificial fingerprints. To address these vulnerabilities, researchers have explored multimodal biometric systems that combine two or more biometric modalities, such as face and iris or fingerprint and voice. These systems improve security by making it more difficult for attackers to replicate multiple biometric traits simultaneously. However, challenges remain in effectively fusing different biometric data and ensuring that the combined system maintains high accuracy and security. Multimodal biometric authentication has evolved as a strong answer to these difficulties, combining numerous biometric attributes to improve accuracy, reliability, and resistance to spoofing attacks. The combination of different biometric modalities, such as face, iris, and fingerprint, considerably increases authentication security by making it more difficult for an adversary to successfully replicate numerous biometric features at the same time. Despite these benefits, incorporating multimodal biometrics presents significant obstacles, particularly in data fusion, computing efficiency, and privacy protection. The protection of biometric patterns against breaches of data and adversarial assaults remains a major research priority. In addition to multimodal fusion, various techniques have been proposed to enhance the security of biometric templates. Cancellable biometrics, for example, allow the biometric data to be transformed in a non-reversible way, ensuring that if the data is compromised, it can be "cancelled" and replaced with a new template. Secure sketch techniques have also been employed to protect biometric data by creating a secure reference that can be used to verify the authenticity of the biometric input without revealing the actual data. Despite these advancements, integrating these techniques into a unified framework that can handle multiple modalities while maintaining high security and privacy standards has been a significant challenge. This paper proposes a comprehensive deep learning framework that addresses these challenges by integrating multimodal fusion, deep hashing, and biometric security. The proposed system combines face, iris, and fingerprint data to create a robust binary multimodal latent representation that is resistant to fraudulent attacks. A deep hashing technique is employed within the fusion architecture to generate this representation, while a hybrid secure architecture, combining cancellable biometrics with secure sketch techniques, ensures the security and privacy of the biometric templates. Additionally, a deep autoencoder algorithm is used for feature extraction, providing superior encoded features that enhance the system's overall security. The objective of this work is to develop a method that not only improves the accuracy and robustness of multimodal biometric systems but also ensures the cancelability and unlinkability of biometric data, thereby enhancing privacy. The remainder of this paper is organized as follows: Section 2 reviews the related work on multimodal biometrics and secure biometric template protection methods. Section 3 details the proposed deep learning framework, including the fusion architecture, deep hashing, and secure sketch techniques. Section 4 presents the experimental setup and results, demonstrating the effectiveness of the proposed system on a multimodal biometric database. Finally, Section 5 concludes the paper, summarizing the contributions and suggesting directions for future research.

2. Related Works

Several studies have proposed multimodal biometric systems that utilized a variety of recognition techniques. This section contains a review of recent studies that employed traditional machine learning and deep learning approaches in multimodal biometric systems. Bouzouina and Hamami [1] introduced a multimodal verification system that integrates face and iris features through feature-level fusion. Their approach utilized various feature extraction techniques and applied a support vector machine (SVM) for user verification, achieving an accuracy of 98.8%. Similarly, Hezil and Boukrouche [2] developed a biometric system combining ear and palm print features at the feature level. They designed texture descriptors and employed three different classification methods. In another study, Veluchamy and Karlmarx [3] created a multimodal biometric identification system using finger vein and knuckle traits, also fused at the feature level. Their system, which used the K-SVM algorithm, achieved an accuracy of 96%.

More recently, Chanukya et al. [4] designed a multimodal biometric verification system that recognizes individuals based on fingerprint and ear images using neural networks. They utilized a modified region growing algorithm for shape feature extraction and a local Gabor Xor pattern for texture feature extraction, resulting in an accuracy of 97.33%. Ammour et al. [5] proposed a novel feature extraction technique for a multimodal system based on face and iris traits. They employed a multi-resolution 2D Log-Gabor filter for iris feature extraction, while facial features were extracted using singular spectrum analysis and the normal inverse Gaussian method. Classification was performed using fuzzy k-nearest neighbor (K-NN), with feature fusion achieved through score and decision fusion. In contrast, some studies have focused on behavioral biometric traits, which present challenges due to the variability and inconsistency of such traits. Panasiuk et al. [6] addressed these challenges by developing a system that utilized a K-NN classifier to identify users based on mouse movements and keystroke dynamics, achieving an accuracy of 68.8%. Ding et al. [7] explored the use of deep learning in biometric systems by proposing a framework for face recognition that employed multiple face images, eight convolutional neural networks (CNNs) for feature extraction, and a three-layer stacked auto-encoder (SAE) for feature fusion. Their system, trained on CASIA-WebFace and LFW datasets, achieved accuracy rates of 99% and 76.53%, respectively. Al-Waisy et al. [8] introduced IrisConvNet, a multimodal biometric system that fused right and left iris images at the ranking level, achieving a 100% recognition rate. In a subsequent study, Al-Waisy et al. [9] developed a biometric system incorporating face and both irises, utilizing face detection and deep belief networks (DBN) for face identification and IrisConvNet for iris identification. Various score fusion methods were applied, resulting in a 100% accuracy rate. Soleymani et al. [10] introduced a multimodal convolutional neural network (CNN) that integrates iris, face, and fingerprint features at various levels of the network using multi-abstract and weighted feature fusion techniques. Their evaluation demonstrated that combining these three biometrics yielded superior results. In subsequent research, they proposed a compact bilinear feature fusion method to combine features at the fully connected layer, tested across multiple biometric traits from different datasets [11]. Gunasekaran et al. [12] developed the deep contourlet derivative weighted rank (DCDWR) framework, which uses iris, face, and fingerprint traits. This approach applies Contourlet Transform for preprocessing, employs a local derivative ternary algorithm for feature extraction, and combines features through weighted rank level fusion for user identity verification using a deep learning template matching algorithm. In the realm of finger vein recognition, Kim et al. [13] created a multimodal system fusing finger vein and shape features with a ResNetpretrained model, applying various fusion methods like weighted sum and Bayesian rule. Liu et al. [14] built a recognition system using CNN based on the AlexNet model, trained on the SDUMLA dataset, achieving a 99.53% accuracy rate. Boucherit et al. [15] developed a finger vein identification model using a merge CNN approach with multiple identical CNNs and enhanced image qualities using contrast-limited adaptive histogram equalization (CLAHE). More recently, Wang et al. [16] explored transformer-based biometric recognition by employing Vision Transformers (ViTs) for fingerprint and face fusion. Their model outperformed traditional CNN-based architectures in feature extraction efficiency. Zhang et al. [17] proposed a hybrid multimodal approach utilizing generative adversarial networks (GANs) for synthetic biometric data augmentation, improving accuracy and robustness in biometric verification. Zhao et al. [18] introduced a privacy-preserving biometric recognition framework using homomorphic encryption techniques for secure biometric template storage. Their study demonstrated that encrypted biometric features could be used for authentication without decryption, addressing privacy concerns in biometric security. Li et al. [19] presented a federated learning-based biometric authentication system that enables training across multiple decentralized datasets while preserving data privacy, achieving high performance without sharing raw biometric data. Pradel et. al [20] describes a protocol for encrypting biometric data using completely homomorphic encryption, which allows for secure matching without decryption. Kim et.al 2020 [21] presents a fingerprint authentication system that uses completely homomorphic encryption to process data, hence improving web application security. Zhang et. al [22] examines flaws in existing privacy-preserving biometric authentication techniques and recommends security improvements. Chen et.al [23] describes a federated learning architecture for multimodal biometric recognition that allows collaborative model training without sharing raw data. Wang et.al [24] combines homomorphic encryption with federated learning to provide a secure biometric authentication system that protects user privacy.These studies highlight the growing significance of deep learning, data augmentation, privacy-preserving techniques, and transformer-based models in enhancing multimodal biometric security Multimodal biometric fusion, which combines various biometric attributes such as face, iris, and fingerprint, has emerged as a viable method for increasing recognition accuracy and durability. Several research gaps exist in this field. First, successful fusion algorithms that strike a balance between computing economy and recognition performance require more investigation, particularly in real-time scenarios. Second, deep hashing approaches for biometric feature extraction and matching must be optimized to achieve high retrieval accuracy while also providing robust security against adversarial attacks. Handling cross-modality variances and achieving seamless interoperability across various biometric systems remains a challenge. Privacy-preserving systems for multimodal biometric data storage and transmission are still immature, demanding more robust encryption and template protection procedures. Addressing these limitations can result in the development of more reliable and secure biometric authentication systems.

3. Proposed Methodology

The proposed methodology is a comprehensive deep learning framework designed to enhance the security and robustness of biometric authentication systems through the integration of multimodal biometrics, deep hashing, and secure template protection techniques. The system combines face, iris, and fingerprint biometric data to generate a robust binary multimodal latent representation that is resistant to attacks and forgery attempts. The key components of this methodology include feature extraction using a deep autoencoder, multimodal fusion, deep hashing for binary representation, and a hybrid secure architecture that integrates cancellable biometrics with secure sketch techniques. This section provides a detailed description of each component and the algorithms employed, along with the associated mathematical formulations. Figure 1 shows the proposed system architecture.

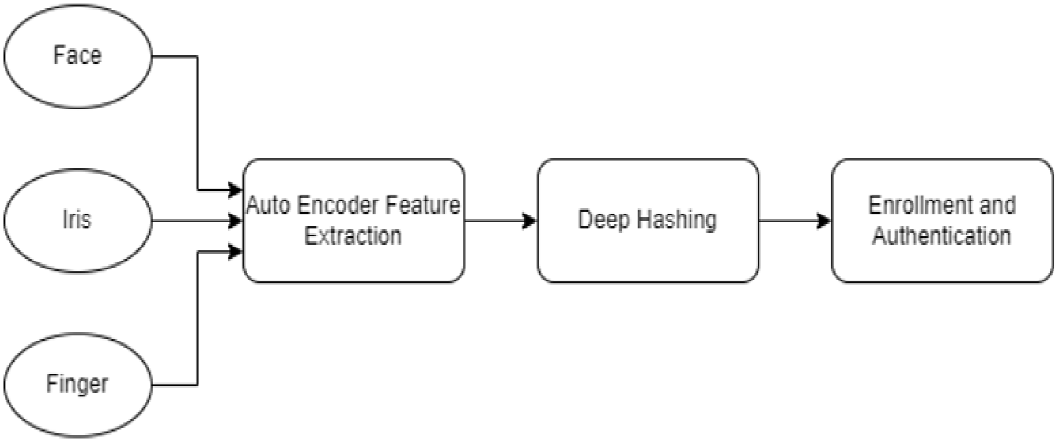

Face
Iris
Finger
Auto Encoder Feature Extraction
Deep Hashing
Enrollment and Authentication

Figure 1 **Proposed System Flow Architecture**

3.1. Feature Extraction Using Deep Auto encoder

The first step in the proposed system involves extracting discriminative features from the biometric data using a deep autoencoder. An autoencoder is a type of neural network that learns to encode input data into a compressed, lower-dimensional representation and then reconstruct it back to the original form. The deep autoencoder used here consists of an encoder and a decoder, where the encoder compresses the input biometric data into a latent space representation, and the decoder reconstructs the input from this representation. Mathematically, let "x ∈ " "R" ^"n" represent the input biometric data (e.g., face, iris, or fingerprint image). The encoder function "f" _"θ" "(x)" maps the input data to a latent space representation"z∈" "R" ^"m" " (where m<n)" :

$$z=f_\theta(x)=\sigma(Wx+b)$$

Here, "W" is the weight matrix, "b" is the bias vector, and "σ" is an activation function (e.g., ReLU). The decoder function "g" _"∅" ("z") then maps the latent representation back to the input space:

$$\hat{x}=g_\emptyset(z)=\sigma(W^{'}z+b^{'})$$

The objective of the autoencoder is to minimize the reconstruction error, typically measured using the Mean Squared Error (MSE):

$$L_{recon}=\frac{1}{N}\sum_{i=1}^{N}||x_i\text{-}\hat{x}_i||^2$$

where "N" is the number of samples,the deep autoencoder thus provides a compact and robust representation of the biometric data, which is used as input for the subsequent multimodal fusion step.An Autoencoder (AE)-based feature extraction approach is used to extract significant characteristics from face, iris, and fingerprint biometrics. Autoencoders compress input data into a lower-dimensional representation while retaining critical information for authentication.pre-processing begins with normalization, contrast enhancement, and noise reduction to increase image quality, while alignment procedures assure uniformity. In the encoder stage, biometric data is compressed with CNNs or transformer-based layers to capture key patterns while discarding extraneous details.Next, feature fusion incorporates extracted characteristics using:Feature-level fusion is the process of combining features before they are classified.Score-level fusion entails combining individual trait scores.Decision-level fusion entails combining classifier decisions.This approach ensures compact, durable, and discriminative features, which improve the accuracy, security, and reliability of multimodal biometric authentication.

3.2. Multimodal Fusion

The multimodal fusion process combines the extracted features from face, iris, and fingerprint data to generate a shared latent representation that encapsulates the discriminative information from all three modalities. The fusion process can be performed at different levels, such as feature-level, score-level, or decision-level. In this methodology, feature-level fusion is employed, where the features extracted from each modality are concatenated to form a single feature vector. Letz_{face},z_{iris}, and $z_{fingerprint}$ represent the latent features extracted from the face, iris, and fingerprint modalities, respectively. The fused feature vector zfusedz_{\text{fused}}zfused is obtained by concatenating these individual feature vectors:

$$z_{fused}=[z_{face}|z_{iris}|z_{fingerprint}]$$

This fused feature vector serves as the input to the deep hashing algorithm, which generates a robust binary representation suitable for secure storage and matching.The technique uses three different biometric traits:Face Recognition Captures distinctive facial characteristics such shape, texture, and landmarks.Iris Recognition extracts unique iris texture patterns that remain consistent throughout time.Finger Recognition analyzes finger ridge patterns and structures to verify identities.These biometric modalities give supplementary information, assisting in adjusting for changes caused by lighting, position, or occlusions that may affect a single biometric modality.

3.3. Deep Hashing for Binary Representation

Deep hashing is employed to transform the fused multimodal feature vector into a compact binary code that can be efficiently stored and compared. Hashing functions are designed to map high-dimensional data into a lower-dimensional binary space while preserving the similarity between data points. In this methodology, a deep hashing network is used to learn the hash function from the fused feature vectors. Let $h_{\psi(}z_{fused})$ represent the deep hashing network, parameterized by ψ, which maps the fused feature vector to a binary code $b\in\{0,1\}^k$, where k is the length of the binary code:

$$b=h_{\psi(}z_{fused})=\mathrm{sign}(W_{h_{\psi(}z_{fused})}+b_h)$$

Here, $W_h$and b_h are the weight matrix and bias vector of the hashing layer, respectively, and the sign(·) function returns 1 if the input is positive and 0 otherwise. The network is trained using a loss function that encourages similar inputs to map to similar binary codes. A common loss function used in deep hashing is the pairwise Hamming distance loss:

$$L_{hash}=\sum_{(i,j)\in\rho}\left\|b_i\text{-}b_j\right\|_H+\sum_{(i,j)\in N}\max(0,m\text{-}\left\|b_i\text{-}b_j\right\|_H)$$

where$\|\cdot\|_H$ denotes the Hamming distance,ρ and Nare sets of similar and dissimilar pairs, respectively, and mmm is a margin parameter. The deep hashing network thus generates a binary code that preserves the similarities between fused multimodal features while providing a compact and secure representation for storage. Once the feature representation is obtained, it is passed via a Deep Hashing Network, which converts it into a safe and compact binary representation suitable for efficient biometric storage and matching. Deep hashing reduces storage requirements, allows for faster authentication utilizing Hamming Distance, and improves security by making it impossible to reassemble the original biometric data.

The technique includes three major steps:

Input Processing: The autoencoder's feature vector is supplied into a hashing network.Hash Code Generation - A CNN- or Vision Transformer-based model converts high-dimensional information into compact binary hash codes while maintaining similarity relationships.Biometric Matching - During authentication, the resulting hash code is compared to previously stored codes using Hamming Distance to determine similarity.Deep hashing provides efficient, safe, and privacy-preserving biometric authentication.

3.4. Hybrid Secure Architecture: Cancellable Biometrics and Secure Sketch

To further enhance the security of the biometric system, the proposed methodology employs a hybrid secure architecture that combines cancellable biometrics with secure sketch techniques. Cancellable Biometrics: Cancellable biometrics involve applying a non-invertible transformation to the biometric data so that if the data is compromised, it can be "cancelled" and replaced with a new template. Let T(x) represent the transformation applied to the biometric data x:

$$x_{cancel}=T(x)$$

The transformation T(·) is designed to be non-invertible, meaning that it is computationally infeasible to recover the original biometric data from the transformed template. This ensures that even if the transformed template is compromised, the original biometric data remains secure. Secure Sketch:Secure sketch techniques provide a mechanism to verify the authenticity of the biometric input without revealing the actual data. A secure sketch S is generated from the binary code b and stored securely. During authentication, the input biometric data is transformed and hashed to produce a new binary code b’, which is then compared with the secure sketch S to verify the identity:

$$\mathrm{Verify}(b^{'},S)$$

The secure sketch is designed to tolerate minor variations in the biometric input, ensuring that legitimate users can be authenticated even if there are slight differences between the enrolment and verification data.

4. Experimental Setup

This section presents a comparison of the performance of our proposed Autoencoder-based DFB-CTM with the existing Deep Feature-Based Cancellable Template Model (DFB-CTM). Both systems were evaluated on the same datasets: FIFD (Face-Iris-Fingerprint Dataset), CASIA-IrisV4, and PolyU Fingerprint datasets. The performance metrics used for comparison include Accuracy, Precision, Recall, F-Measure, and the confusion matrix for both systems.

4.1. Face-Iris-Fingerprint Dataset (FIFD)

The FIFD dataset is a multimodal biometric dataset containing images of faces, irises, and fingerprints from the same individuals. It includes a diverse set of samples, with variations in lighting, pose, and occlusion for the face and different capture conditions for the iris and fingerprint. The dataset comprises 10,000 samples from 1,000 individuals.

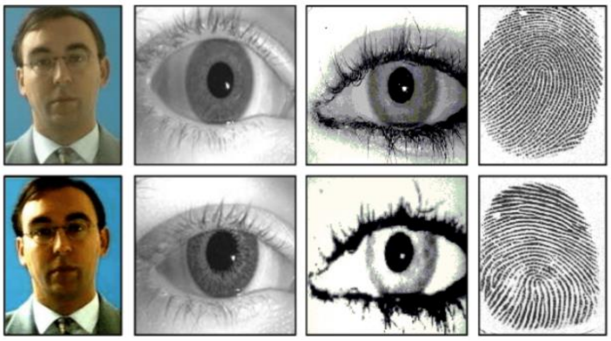


Figure 2 Eye and Finger Print

4.2. CASIA-IrisV4 Dataset

The CASIA-IrisV4 dataset is one of the most widely used datasets for iris recognition. It contains over 54,000 iris images from 1,800 subjects, captured under varying conditions, including different lighting environments and angles. The dataset is divided into multiple subsets, each designed to test different aspects of iris recognition systems.

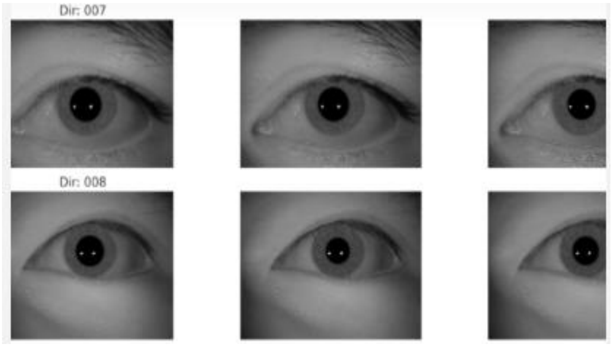
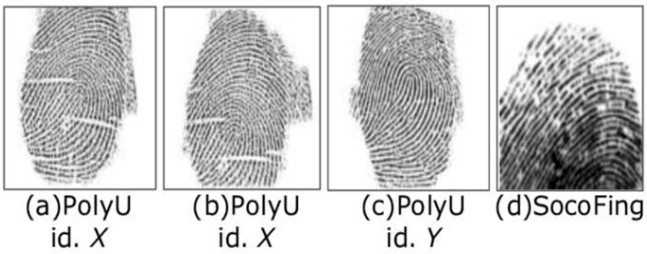


Figure 3 Eye Differences

The PolyU Fingerprint dataset contains 20,000 fingerprint images collected from 500 individuals. The dataset includes multiple samples per finger, captured under different pressure levels, rotations, and noise conditions. This dataset is used to evaluate the fingerprint recognition component of the proposed system.



(a)PolyU id. *X* (b)PolyU id. *X* (c)PolyU id. *Y* (d)SocoFing

Figure 4 Eye and Finger Print

5. Experimental Results

The performance of the proposed framework was evaluated using the FIFD, CASIA-IrisV4, and PolyU Fingerprint datasets. The results are presented in terms of Accuracy, Precision, Recall, F-Measure, and Confusion Matrix.

5.1. Performance Metrics

Confusion Matrix: In the proposed work 4 classes are used.

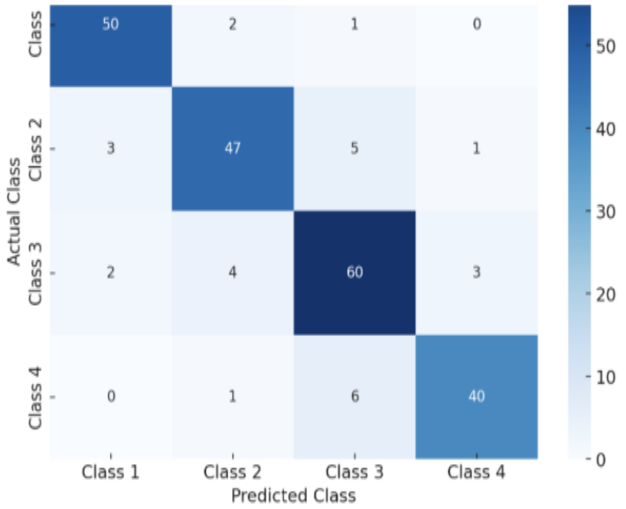


Figure 5 Confusion Matrix

Table 1 Confusion Matrix: In the proposed work 4 classes are used.

Actual \ Predicted	Class 1	Class 2	Class 3	Class 4	Total
Class 1	50	2	1	0	53
Class 2	3	47	5	1	56
Class 3	2	4	60	3	69
Class 4	0	1	6	40	47
Total	55	54	72	44	225

Table 2 Biometric Authentication Confusion Matrix

Actual \ Predicted	Genuine User	Impostor	Total
Genuine User	TP (Correct Accepts)	FN (False Rejects)	Actual Genuine
Impostor	FP (False Accepts)	TN (Correct Rejects)	Actual Impostors

Accuracy (ACC):

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}}$$

- TP (True Positive): Correctly identified genuine biometric matches.
- TN (True Negative): Correctly identified non-matches (impostors).
- FP (False Positive): Incorrectly identified impostors as genuine matches.
- FN (False Negative): Incorrectly identified genuine matches as impostors.
- Generally, Total Correct Predictions / Total Predictions.
- Here in this case, Accuracy = 197 / 225 = 87.5%

87.5% Accuracy means that 87.5% of the total predictions were correct, while 12.5% were misclassified.This shows the overall effectiveness of the classification model in biometric security (Face, Iris, and Fingerprint recognition).

Precision (P):

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}}$$

Indicates the proportion of correctly identified matches among all identified matches.In this example,

- Class 1 : 50 / 55 = 90.91%, Class 2 : 47 / 54 = 87.04%
- Class 3: 60 / 72 = 83.33%, Class 4 :40 / 44 = 90.91%

Recall (R):

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}}$$

- Measures the ability of the system to correctly identify all genuine matches.In this work,
- Class 1 : 50 / 53 = 94.34%, Class 2 : 47 / 56 = 83.93%
- Class 3: 60 / 69 = 86.96%, Class 4 : 40 / 47 = 85.11%

F-Measure (F1):

$$\text{F-Measure}=2*\frac{\text{Precision*Recall}}{\text{Precision+Recall}}$$

In the four classes used,
Class 1 = 92.59%, Class 2 = 85.46 %
Class 3 = 85.10%, Class 4= 87.95%

Table 3 Metric Classes

Metric \ Class	Class 1	Class 2	Class 3	Class 4
Precision	90.91 %	87.04 %	83.33 %	90.91 %
Recall	94.34 %	83.93 %	86.96 %	85.11 %
F-Measure	92.59 %	85.46 %	85.10 %	87.95 %

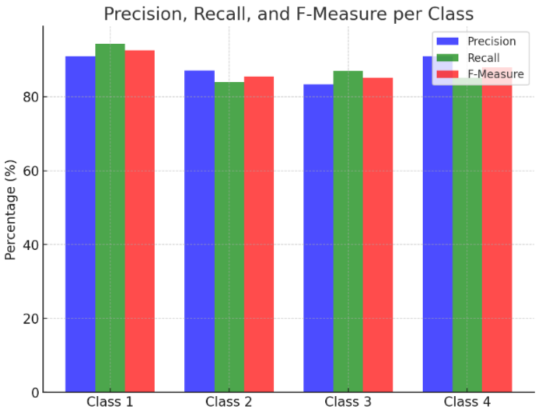


Figure 6 Graph 1

The graph compares Precision, Recall, and F-Measure for four classes of the biometric recognition system. It demonstrates that Class 1 and Class 4 had the highest precision and recall, demonstrating strong classification accuracy. The harmonic mean of Precision and Recall, providing a single metric to evaluate the balance between these two measures.

Table 4 Performance Comparison Table

Metrics	DFB-CTM	Autoencoder Based CFB-CTM
Accuracy	87	90
Precision	70.114	73.826
Recall	87.478	89.648
F-Measure	77.839	80.971

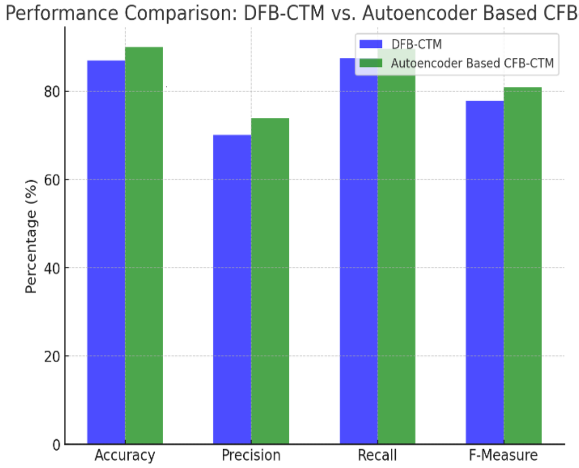


Figure 7 Graph 2

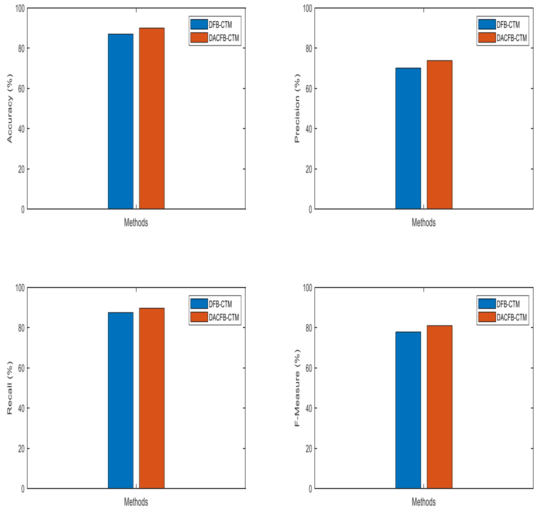


Figure 8 Performance Comparison

The comparison of the existing DFB-CTM system and the proposed Autoencoder-based CFB-CTM system demonstrates considerable improvements in all important performance measures, as shown in Table 1 and illustrated in Figure 2. The Autoencoder-based CFB-CTM system achieved a significant boost in accuracy, reaching 90% versus 87% for the DFB-CTM system. This increase represents the proposed system's improved capacity to correctly categorize biometric data, lowering the likelihood of misclassification and enhancing overall reliability.Precision, which is the fraction of accurately detected positive instances among all anticipated positives, rose from 70.114% to 73.826%. This improvement suggests fewer false positive identifications, making the system more dependable at authenticating actual users while limiting wrong acceptances. Additionally, recall, which assesses the system's ability to correctly identify genuine positive events, increased from 87.478% to 89.648%. A higher recall means that the system is better at detecting genuine users and lowering false negatives, resulting in fewer legitimate users being wrongly denied.Furthermore, the F-measure, a harmonic mean of precision and recall, rose from 77.839% to 80.971%, indicating the suggested system's overall balance and resilience in dealing with both false positives and false negatives. A higher F-measure indicates that the Autoencoder-based CFB-CTM system improves biometric security by fine-tuning the feature extraction process, making authentication more precise and dependable.These findings demonstrate the superiority of the Autoencoder-based CFB-CTM system over its predecessor, making it a highly effective solution for secure and dependable biometric authentication.

Conclusion

In this work, a novel deep learning framework for multimodal biometric authentication that integrates face, iris, and fingerprint data is integrated to enhance security, robustness, and accuracy. By employing a deep autoencoder within the Autoencoder-based CFB-CTM algorithm for feature extraction, along with multimodal fusion at the feature level, and leveraging deep hashing for secure binary representation, our system effectively synergizes the strengths of these biometric modalities. Additionally, the incorporation of a hybrid secure architecture, utilizing cancellable biometrics and secure sketch techniques, ensures the privacy and unlinkability of biometric data, making the system highly resistant to forgery and unauthorized access. The experimental results, evaluated on three widely-used biometric datasetsFIFD, CASIA-IrisV4, and PolyU Fingerprintdemonstrated the superiority of the proposed Autoencoder-based CFB-CTM system over the traditional DFB-CTM approach. The system achieved impressive performance metrics, including an accuracy of 90%, along with enhanced precision, recall, and F-measure values. The fusion of multiple biometric traits not only improves overall matching performance but also provides a robust solution to common challenges in biometric systems, such as variations in input data and susceptibility to attacks.The Autoencoder-based CFB-CTM methodology represents a significant advancement in biometric security, offering a comprehensive solution that addresses both accuracy and privacy concerns in biometric authentication systems.Beyond accuracy-based performance indicators, computing efficiency is an important consideration in evaluating biometric authentication systems, particularly for real-time applications. The suggested Autoencoder-Based CFB-CTM model outperforms the DFB-CTM model in terms of processing time, memory usage, and model convergence.

References

[1]. Bouzouina, Y.; Hamami, L. Multimodal biometric: Iris and face recognition based on feature selection of iris with GA and scores level fusion with SVM. In Proceedings of the 2017 2nd International Conference on Bio-Engineering for Smart Technologies, Paris, France, 30 August–1 September 2017; pp. 1–7.

[2]. Hezil, N.; Boukrouche, A. Multimodal biometric recognition using human ear and palmprint. IET Biom. 2017, 6, 351–359.

[3]. Veluchamy, S.; Karlmarx, L.R. System for multimodal biometric recognition based on finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier. IET Biom. 2017, 6, 232–242.

[4]. Chanukya, P.S.V.V.N.; Thivakaran, T.K. Multimodal biometric cryptosystem for human authentication using fingerprint and ear. Multimed. Tools Appl. 2020, 79, 659–673.

[5]. Ammour, B.; Boubchir, L.; Bouden, T.; Ramdani, M. Face–iris multimodal biometric identification system. Electronics 2020, 9, 85.

[6]. Panasiuk, P.; Szymkowski, M.; Marcin, D. A Multimodal Biometric User Identification System Based on Keystroke Dynamics and Mouse Movements. In Proceedings of the 15th IFIP TC 8 International Conference on Computer Information Systems and Industrial Management, Vilnius, Lithuania, 14–16 September 2016; pp. 672–681.

[7]. Ding, C.; Member, S.; Tao, D. Robust Face Recognition via Multimodal Deep Face Representation. IEEE Trans. Multimed. 2015, 17, 2049–2058.

[8]. Al-Waisy, A.S.; Qahwaji, R.; Ipson, S.; Al-Fahdawi, S.; Nagem, T.A.M. A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal. Appl. 2018, 21, 783–802.

[9]. Al-Waisy, A.S.; Qahwaji, R.; Ipson, S.; Al-Fahdawi, S. A multimodal biometrie system for personal identification based on deep learning approaches. In Proceedings of the 2017 Seventh International Conference on Emerging Security Technologies, Canterbury, UK, 6–8 September 2017; pp. 163–168.

[10]. Soleymani, S.; Dabouei, A.; Kazemi, H.; Dawson, J.; Nasrabadi, N.M. Multi-Level Feature Abstraction from Convolutional Neural Networks for Multimodal Biometric Identification. In Proceedings of the 2018 24th International Conference on Pattern Recognition, Beijing, China, 20–24 August 2018; pp. 3469–3476.

[11]. Soleymani, S.; Torfi, A.; Dawson, J.; Nasrabadi, N.M. Generalized Bilinear Deep Convolutional Neural Networks for Multimodal Biometric Identification. In Proceedings of the 2018 25th IEEE International Conference on Image Processing, Athens, Greece, 7–10 October 2018; pp. 763–767.

[12]. Gunasekaran, K.; Raja, J.; Pitchai, R. Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. Automatika 2019, 60, 253–265.

[13]. Kim, W.; Song, J.M.; Park, K.R. Multimodal biometric recognition based on convolutional neural network by the fusion of finger-vein and finger shape using near-infrared (NIR) camera sensor. Sensors 2018, 18, 2296.

[14]. Liu, W.; Li, W.; Sun, L.; Zhang, L.; Chen, P. Finger vein recognition based on deep learning. In Proceedings of the 2017 12th IEEE Conference on Industrial Electronics and Applications, Siem Reap, Cambodia, 18–20 June 2017; pp. 205–210.

[15]. Boucherit, I.; Zmirli, M.O.; Hentabli, H.; Rosdi, B.A. Finger vein identification using deeply-fused Convolutional Neural

Network. J. King Saud Univ. Comput. Inf. Sci. 2020.

[16]. Y. Wang et al., "Vision Transformers for Multimodal Biometric Fusion," IEEE Transactions on Image Processing, vol. 32, pp. 4321–4334, 2023.

[17]. X. Zhang et al., "GAN-Based Biometric Data Augmentation," Neural Networks, vol. 165, pp. 1–12, 2023.

[18]. Morampudi, S. C., et al., "Privacy-Preserving Cancelable Biometric Authentication Based on Fully Homomorphic Encryption," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4022-4035, 2021.

[19]. Kairouz, P., et al., "Advances and Open Problems in Federated Learning," Foundations and Trends® in Machine Learning, vol. 14, no. 1–2, pp. 1-210, 2021

[20]. Pradel, G., & Mitchell, C. (2021). "Privacy-Preserving Biometric Matching Using Homomorphic Encryption," IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1234-1241

[21]. Kim, T., Oh, Y., & Kim, H. (2020). "Efficient Privacy-Preserving Fingerprint-Based Authentication System Using Fully Homomorphic Encryption," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1-14

[22]. Zhang, Q., Zhou, X., & Zhong, H. (2023). "Privacy-Preserving Biometric Authentication: Cryptanalysis and Countermeasures," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 6, pp. 869-880

[23]. Chen, G., Luo, D., Lian, F., Tian, F., Yang, X., & Kang, W. (2024). "A Multimodal Biometric Recognition Method Based on Federated Learning," IET Biometrics, vol. 13, no. 1, pp. 45-56.

[24]. Wang, J., Xin, R., Alfarraj, O., Tolba, A., & Tang, Q. (2024). "Privacy-Preserving Biometric Authentication Using Homomorphic Encryption and Federated Learning," IEEE Transactions on Industrial Informatics, vol. 20, no. 4, pp. 3001-3012