IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 30 July 2024, accepted 21 August 2024, date of publication 26 August 2024, date of current version 6 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3450372

RESEARCH ARTICLE

Deep Cancelable Multibiometric Finger Vein and Fingerprint Authentication With Non-Negative Matrix Factorization

MOHAMED HAMMAD[1,2], MUDASIR AHMAD WANI[1], KASHISH ARA SHAKIL[3], HADIL SHAIBA[3], AND AHMED A. ABD EL-LATIF[1,4], (Senior Member, IEEE)

[1]EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[2]Department of Information Technology, Faculty of Computers and Information, Menoufia University, Shebeen El-Kom 32511, Egypt
[3]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[4]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebeen El-Kom 32511, Egypt

Corresponding author: Mohamed Hammad (mohammed.adel@ci.menofia.edu.eg)

This work was supported by Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia, under Grant PNURSP2024R135.

ABSTRACT Biometric authentication technologies, which use physiological and behavioral traits to verify identity, have added a new layer of protection. However, concerns about privacy, security, and illegal entry persist. Therefore, multibiometric systems have emerged to improve authentication accuracy and system robustness. However, to address these problems more effectively, it is imperative to incorporate cancelable biometrics into multimodal systems. This integration is essential because it offers enhanced security measures and safeguards privacy. This paper presents a novel cancelable multibiometric method that utilizes non-negative matrix factorization (NMF) and a lightweight deep learning model to augment the levels of security and privacy in biometric authentication. The proposed system leverages the distinct capabilities of finger vein and fingerprint recognition modalities to enhance authentication accuracy and improve resistance against spoofing attacks. The implementation of cancelable biometrics principles serves to safeguard user privacy and enhance security measures. NMF is employed to facilitate the extraction of features and the obfuscation of data. The study presents actual evidence to support the system's high validation results with an average accuracy of 95.31% for the NUPT-FPV dataset and 92.71% for the FVC2004 and FV-USM datasets, its ability to preserve anonymity, and its real-time capabilities. Significantly, it satisfies all conditions that can be canceled, representing a noteworthy progression in the domain of cancelable multibiometric. The amalgamation of NMF with a streamlined deep learning model presents a pragmatic and effective resolution, surmounting prior constraints in computational intricacy.

INDEX TERMS Cancelable multibiometric, deep learning, non-negative matrix factorization, finger vein, fingerprint, authentication.

I. INTRODUCTION

Biometric authentication systems have significantly enhanced security practices by leveraging unique physiological and behavioral traits to verify individuals' identities [1]. However, the widespread adoption of biometrics has sparked concerns regarding privacy, security, and the potential for unauthorized access. Specifically, there is a growing apprehension about the vulnerability of biometric data, especially concerning the potential linkage of biometric templates across various authentication systems. Once compromised, biometric raw data remains vulnerable indefinitely, posing significant risks to individuals' privacy and security [2]. In response to these concerns, cancelable biometrics has emerged as a promising solution. Cancelable biometrics involves transforming biometric data into revocable templates, thereby mitigating the risks associated with the compromise of raw biometric data [3]. By adopting cancelable biometrics, organizations

The associate editor coordinating the review of this manuscript and approving it for publication was Zhe Jin.

can enhance the security and privacy of their biometric authentication systems, offering users greater confidence in the protection of their personal information. Furthermore, the integration of multibiometric systems, which combine multiple biometric traits, presents an opportunity to enhance recognition accuracy and robustness [3]. In this paper, we introduce the concept of cancelable multibiometrics and explore its application using a combination of finger vein and fingerprint recognition. By leveraging cancelable multibiometrics, we aim to address the aforementioned privacy and security concerns while achieving superior performance in biometric authentication systems.

Finger veins and fingerprint recognition are two distinct biometric modalities that offer complementary strengths [4], [5], [6], [7]. Finger vein recognition exploits the unique patterns of blood vessels beneath the skin's surface, while fingerprint recognition captures the distinct ridge and valley patterns on the fingertips. Integrating these modalities not only enhances recognition accuracy but also strengthens the system against spoofing attacks. By combining both modalities, the system can get an elevated degree of certainty in authenticating an individual's identification. While biometric systems provide convenience and reliability, they also give rise to apprehensions over illegal access, data breaches, and the exploitation of individuals' personal information [8]. Traditional biometric systems typically store biometric templates, which are digital representations of extracted biometric features. These templates are generated through a process that involves various protective methodologies, including encryption utilizing conventional algorithms, feature transformation techniques, and the implementation of biometric cryptosystems. It is widely recognized that traditional biometric systems can be vulnerable to attacks [9]. Cancelable biometrics mitigates these concerns by generating templates that are unlinkable to the original biometric data [10]. Cancelable criteria, such as revocability and diversity, are essential aspects of this transformation. In the context of multibiometric systems, cancelable templates offer an additional layer of privacy and security, reducing the risk of biometric data compromise [11], [12].

Non-negative Matrix Factorization (NMF) is a mathematical technique that has demonstrated its capabilities in various applications, including image processing and feature extraction [13], [14], [15]. NMF decomposes matrices into non-negative components, facilitating the extraction of meaningful features. In the context of cancelable multibiometrics, NMF can be leveraged to transform the finger vein and fingerprint data into non-negative matrices that capture essential biometric traits. This transformation not only aids in feature extraction but also enhances privacy by obfuscating the original data's structure.

This study aims to extend the application of cancelable multibiometrics by integrating NMF with a lightweight deep learning model. Deep learning models, particularly convolutional neural networks (CNNs), have shown exceptional performance in various biometric recognition tasks [16], [17], [18], [19], [20]. By combining NMF with a lightweight deep learning model, the study seeks to improve both the accuracy and efficiency of cancelable multibiometric systems. The primary motivation behind this study is to advance the field of cancelable multibiometrics by combining NMF with a lightweight deep learning model. The study aims to address limitations observed in previous deep cancelable multibiometric systems, such as high computational complexity and lack of real-time performance. By integrating NMF and a lightweight deep learning model, the study intends to overcome these limitations and offer a more practical and efficient solution for cancelable multibiometric authentication. While previous studies have explored cancelable biometrics using deep learning models, our work uniquely integrates fingerprint and finger vein biometrics using a novel combination of NMF and lightweight deep learning models. This integration not only enhances the security and privacy of the biometric data but also addresses key limitations such as high computational complexity and lack of real-time performance observed in prior approaches. Our method introduces a new cancelable transformation technique that effectively converts biometric data into non-reversible templates, offering a practical and efficient solution for cancelable multibiometric authentication.

The primary findings of this research can be succinctly described as follows:

1) A new cancelable multibiometric method is proposed, leveraging NMF and a lightweight deep learning model, to enhance security and privacy.
2) Finger vein and fingerprint recognition modalities are integrated to showcase the advantages of combining these two traits in a multibiometric system.
3) A novel approach is developed to address the limitations of previous deep cancelable multibiometric systems, achieving improved performance and efficiency. To the best of our knowledge, this is the first study to propose a cancelable fingerprint with finger vein based on deep learning model.
4) The proposed cancelable multibiometric system is evaluated empirically using real-world datasets, providing insights into its accuracy, privacy preservation, and real-time capabilities.
5) Our multimodal method successfully satisfies all cancelable criteria, in contrast to most previous efforts, which have only concentrated on one or two criteria. Source code is available at: https://github.com/Hammad2019/Cancelable-finger-vein-and-fingerprint-authentication-with-non- negative-matrix-factorization

The paper structure paragraph outlines the organization of the paper into several sections. Section II discusses the existing research and innovation in cross-modal biometric authentication systems. Section III presents the proposed method in detail. Section IV provides an empirical evaluation of the proposed system using real-world datasets. Section V offers a comprehensive analysis and comparison of

the results with previous work. The future work is discussed in Section VI. Finally, Section VII summarizes the main findings and outlines potential avenues for future research.

II. STATE OF THE ART

To further enhance cross-modal biometric authentication systems, it is imperative to expand upon the existing body of research and innovation. Within this section, we undertake a comprehensive examination of the substantial corpus of prior research that has made notable contributions to the advancement of cancelable biometrics, multimodal authentication based on finger vein and fingerprint [21], [22], [23], [24], [25], [26], [27], and the convergence of these fields. Through a comprehensive analysis of prior research, methodology employed, and significant discoveries made, a deeper understanding can be obtained regarding the progression of cross-modal biometric authentication systems. The detailed review of existing literature not only establishes the background for our research but also emphasizes the advancements made in the wider discipline, facilitating a more profound comprehension of the importance and promise of our innovative methodology.

A. PREVIOUS MULTIMODAL FINGERPRINT AND FINGER VEIN METHODS

The FS-STMFPFV-Net approach was introduced by Abdullahi et al. [21], which focuses on the development of a filtered spatial and temporal multimodal fingerprint and finger vein network. The FS-STMFPFV-Net proposed in this study employs a two-channel independent learning approach in order to enhance the handling of picture variabilities. The initial channel of the image generator is responsible for the alignment of fingerprint and finger vein images, resulting in the generation of an image sequence. The Long Short-Term Memory (LSTM) module in the second channel is responsible for storing features in a sequential manner. The FS-STMFPFV-Net demonstrates a high level of accuracy, with a 97% success rate when evaluated by established procedures across various databases. Lv et al. [22] presented a method for feature-level fusion identification of finger veins and fingerprints utilizing a single ICNIR finger image. The authors initially present the utilization of contrast limited adaptive histogram equalization (CLAHE) and grayscale normalization as techniques to enhance the quality of fingerprint and finger vein texture. The authors propose the utilization of an adaptive radius local binary pattern (ADLBP) feature, specifically with a uniform pattern, for the extraction of fingerprints and finger veins. The conventional local binary patterns (LBPs) encounter difficulties in accurately capturing the textural characteristics of ICNIR images with varying sizes. In this study, the fusion of feature vectors obtained from the ADLBP block histogram is employed for the purpose of fingerprint and finger vein recognition. This fusion process is carried out by utilizing a threshold decision support vector machine. In their study, Yang and Zhang [23] introduced a biometric approach that utilizes fingerprint-vein patterns to enhance the universality of fingerprint-based identification systems. The extraction of initial fingerprint and finger-vein features is accomplished through the utilization of a unified Gabor filter architecture. This study presents the introduction of supervised local-preserving canonical correlation analysis (SLPCCAM). The fingerprint-vein feature vectors (FPVFVs) are generated by SLPCCAM through the process of feature-level fusion. The utilization of the nearest neighborhood classifier for personal identification is based on the concept of FPVFVs. Kovač and Marák [24] introduced OpenFinger, a technologically advanced system designed for the purpose of identity detection. This system utilizes both fingerprint and finger vein patterns and is capable of effectively handling challenges such as finger displacement and rotation. The fusion process was conducted using the sum and mean approaches, resulting in an equal error rate (EER) of 2.12%. Lin et al. [25] developed a dynamic weighting matching system to assess feature quality. Two model sources yield effective feature point sets. Neighborhood removal and reserving of points linked with particular regions are done before and after feature point set fusion to reduce dimension burden. The feature evaluation results are used to develop a dynamic weighting method for fusion biometrics. The database and query image fused feature point-sets are compared using point pattern matching and the proposed weight matching algorithm. Cherrat et al. [26] presented a hybrid system that combines the capabilities of three efficient models: CNN, SoftMax, and RF classifier. This hybrid system improves fingerprints identification system that uses fingerprints, finger-vein, and face recognition. In a typical fingerprint system, K-means and DBSCAN algorithms are used to identify foreground and background regions. The features are also recovered using CNNs and dropout. The Softmax classifier is then used. Typical finger vein systems use exposure fusion to improve the contrast of the region of interest image, which is given into the CNN model. The Random Forest classifier is also recommended for classification. The ratings from various systems are combined to improve human identification. Raghavendra et al. [27] developed a durable imaging device that captures fingerprints and finger vein data. They integrate a single camera with near infrared and visible light sources strategically placed beside physical structures to provide a cost-effective sensor. This setup captures high-quality fingerprint and vein data. A finger vein detection technique uses the maximum curvature approach with Spectral Minutiae Representation

B. PREVIOUS MULTIMODAL CANCELABLE METHODS

Within the domain of biometric authentication systems, the notion of cancelable biometrics has arisen as a potentially effective resolution for tackling issues pertaining to security and privacy [28], [29]. Cancelable biometrics involve the conversion of an individual's biometric data into a form that cannot be reversed, allowing for easy revocation or replacement in the event of a security compromise [28], [29]. This methodology greatly improves the confidentiality

of biometric data and offers a heightened level of protection, particularly in scenarios involving electronic storage and processing of such biometric information [30]. Fingerprint recognition is widely employed as a modality for biometric authentication [31], [32], [33], [34], however finger vein recognition is increasingly gaining traction owing to its notable precision and robustness against spoofing attacks [35], [36]. The convergence of cancelable biometrics with cross-modal authentication presents a novel aspect to the field of biometric security [37], [38], [39], [57]. Goh et al. [37] developed a multimodal biometric authentication system using Index-of-Max (IoM) hashing, Alignment-Free Hashing (AFH), and feature-level fusion. The framework has three major benefits. 1) IoM hashing protects biometric templates. This protects against security and privacy breaches. 2) The system can handle binary and real-valued biometric feature representations. Thus, for fusion, it can include many biometric features. 3) AFH allows feature-level fusion without alignment, which has low template storage, computational complexity during matching, and privacy implications. Fused templates are generated through the utilization of binary domain operators such as AND, OR, and XOR. The system undergoes testing utilizing benchmark datasets derived from four prevalent biometric modalities. The FVC 2002 dataset is commonly employed for the purpose of fingerprint analysis. The LFW dataset, on the other hand, is widely utilized in the field of face recognition. For iris identification, researchers often rely on the CASIA-v3-Interval dataset. Lastly, the UTFVP dataset is frequently employed for the examination of finger-vein patterns. The authors Cherrat et al. [38] propose a comprehensive multimodal biometric recognition system that integrates fingerprints, finger veins, and facial pictures through a cascade advanced and decision level fusion approach. The utilization of Gabor filters is a common practice in early fingerprint identification systems for the purpose of image enhancement. Following the enhancing process, the images undergo binarization and thinning procedures. Subsequently, more intricate particulars are gathered in order to ascertain the authenticity or fraudulent nature of an individual. In order to enhance the quality of images, the finger vein recognition system employs many techniques, including the utilization of Linear Regression Line, Canny edge detection, and local histogram equalization. The histogram of oriented gradients (HOG) method is employed for feature extraction. In their study, Yang et al. [39] proposed a multi-biometric system that combines cancelable fingerprint and finger-vein modalities. The system incorporates template protection and revocability mechanisms to enhance its security and privacy features. The multi-biometric system employs two distinct feature sets, namely minutia-based fingerprints and image-based finger-vein features. A feature-level fusion strategy comprising three options has been developed. Extensive research has been conducted on these fusion possibilities to ensure optimal performance and security alignment. The researchers integrated the primary and successive photos of each finger from the FVC2002 DB2 fingerprint database with the fifth and sixth images of the initial 100 fingers in the FV-HMTD finger-vein database. Consequently, two distinct sets of image pairings were generated, comprising a fingerprint image paired with a finger-vein image. Li et al. [57] presented a privacy-preserving multi-biometrics fusion scheme for fingerprint and finger vein recognition. By extracting minutiae-based fingerprint and image-based finger vein features and transforming them using a permutation hashing-based algorithm, we achieve a uniform representation. Extensive experiments on *six* datasets show high recognition performance and ensure security in terms of renewability and unlinkability.

C. LIMITATIONS OF THE PREVIOUS MULTIMODAL CANCELABLE SYSTEMS AND OUR SOLUTIONS

A considerable number of current cancelable biometric authentication systems, such as those that rely on fingerprint and finger vein recognition, fail to entirely meet the criteria that define cancelable biometric data security and privacy. The inability of these systems to facilitate the revocation or substitution of compromised biometric data may hinder their capacity to effectively mitigate security breaches. Certain established systems place excessive emphasis on a solitary biometric modality, such as finger vein or fingerprint recognition, thereby failing to fully exploit the advantages that cross-modal authentication can offer. This may compromise the authentication system's resilience and precision, especially in situations where a solitary modality could be susceptible to spoofing attacks. Specific approaches depend on feature-level fusion, a process that frequently necessitates the alignment of biometric data. This gives rise to computational intricacies while matching and may potentially compromise privacy. This process of alignment may not be appropriate for real-time applications due to its potential difficulties. By combining deep learning with NMF, the proposed method is capable of converting biometric data into non-reversible templates that satisfy cancelable criteria. The revocation or replacement of cancelable templates in the event of a security breach serves to fortify the confidentiality and security of the biometric information. The integration of finger vein and fingerprint authentication modalities is employed, capitalizing on their respective capabilities that complement each other. The addition of this feature not only enhances the accuracy of recognition but also enhances the system's resilience against spoofing attacks. By capitalizing on the benefits of both modalities, our methodology presents a more resilient and precise authentication solution. In contrast to several current methods that depend on alignment-based feature-level fusion, our methodology uses NMF and lightweight deep learning models to perform feature extraction and fusion. The utilization of this methodology obviates the necessity for alignment, hence diminishing the computational intricacy involved in the process of matching, while also effectively dealing with potential privacy apprehensions. The utilization of binary domain operators in the context of template fusion additionally augments privacy.

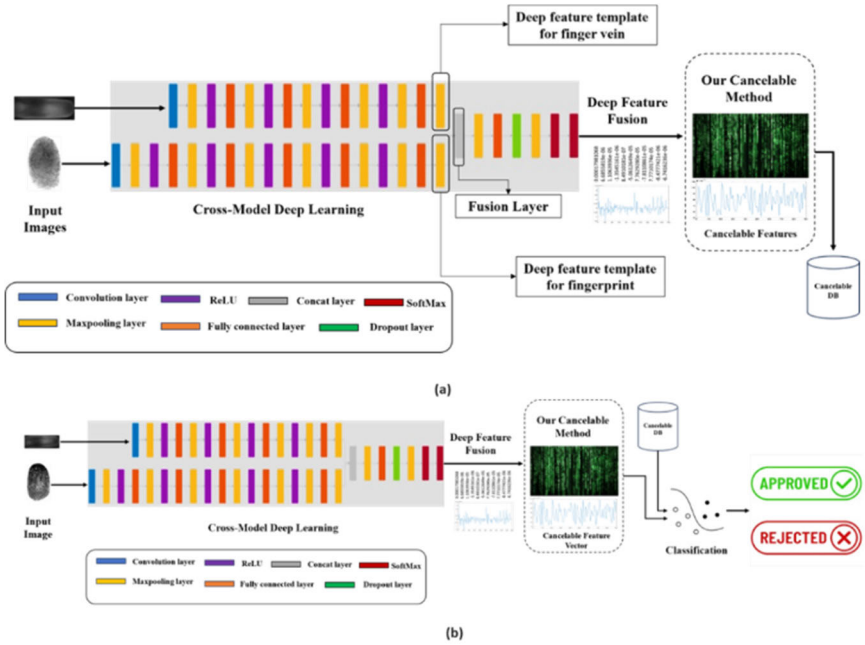


FIGURE 1. Stages of the proposed deep cancelable cross-model authentication system.

Our approach leverages the strengths of deep learning in feature extraction and fusion without the need for alignment-based feature-level fusion, which is common in many existing methods. By combining NMF and lightweight deep learning models, we reduce computational complexity and enhance privacy, making our method suitable for real-time applications. Unlike traditional methods that often focus on a single biometric modality, our integration of fingerprint and finger vein modalities enhances recognition accuracy and system resilience against spoofing attacks. This novel combination sets our work apart from previous studies and offers a more robust and efficient solution for cancelable multibiometric authentication.

D. GOALS AND AIMS OF OUR MULTIMODAL DEEP SYSTEM

This study aims to integrate the distinct attributes of cancelable fingerprint and finger vein detection using deep learning methodologies. It is crucial to underscore that this work constitutes the initial endeavor to investigate the amalgamation of cancelable fingerprint and finger vein identification for the purpose of authentication. The existing body of research has predominantly concentrated on traditional biometric techniques. However, we acknowledge the possibility of enhancing security and privacy by combining cancelable biometrics with cross-modal authentication. Our methodology utilizes deep learning approaches to optimize the integration of these two biometric modalities, thereby advancing the development of biometric authentication systems in a dynamic security environment. This groundbreaking study establishes a fundamental basis for future investigation and advancement in the discipline, presenting innovative perspectives and resolutions for the safeguarding and confidentiality of biometric authentication.

Our study is the first to explore the integration of cancelable fingerprint and finger vein biometrics using deep learning for the purpose of authentication. This innovative approach utilizes deep learning to optimize the fusion of these two modalities, significantly advancing the field of cancelable biometrics. By addressing the limitations of traditional biometric techniques and enhancing security and privacy through cross-modal authentication, our work lays a foundational basis for future research and development in biometric authentication systems.

III. CANCELABLE CROSS-MODEL AUTHENTICATION SYSTEM

The methodology proposed in this study aims to develop a cancelable multibiometric system that combines finger vein and fingerprint authentication using NMF. The primary goal is to enhance security, privacy, and authentication accuracy by integrating cancelable biometrics and NMF-based feature transformation with deep learning model as shown in Figure 1. This Section provides an in-depth overview of the steps involved in the methodology.

A. DATA USED

The study incorporates two databases for fingerprint and finger vein. Firstly, we employed a database called NUPT-FPV [40], which is suitable for real-time applications and captured from the same source. Secondly, we employed a database consisting of two publicly available databases from different resources to facilitate research and comparison: the FVC2004 database [41] for fingerprint samples and the FV-USM database [42] for finger vein samples.

TABLE 1. Composition of multimodal datasets.

Database	Source	Participants	Total Images	Images Used	Description	Image Resolution	Sampling Details
NUPT-FPV	NUPT	140	33,600	960	Real-world dataset capturing fingerprint and finger vein data from 140 individuals.	Varies	Captured 20 times per finger over two separate sessions.
FVC2004	Public Database	120	1440	960	Publicly available dataset for fingerprint recognition research, consisting of 120 individuals.	640×480, 500 dpi	Collected from forefinger and middle finger of both hands.
FV-USM	Public Database	123	5904	960	Publicly available dataset comprising finger vein images collected from 123 individuals.	640×480	Images obtained from left index, left middle, right index, and right middle fingers.

• *The first database NUPT-FPV*

This dataset [40] is a pioneering effort in the field, as it is the initial public collection of fingerprint and finger vein data obtained simultaneously in real-world scenarios. The research team at NUPT-FPV successfully acquired 840 sets of finger information from a group of 140 participants. Each finger was meticulously collected a total of 20 times, spread across two separate sessions. As a result, a grand total of 33,600 images capturing both fingerprint and finger vein data were obtained. In this work, we employed a total of 960 images from the two sessions. The NUPT-FPV dataset is particularly suitable for real-time applications due to its comprehensive and realistic data collection process.

• *The second database*

To facilitate research and enable comparison with other studies, we employed two widely used public databases from different sources:

1) FVC2004 DATABASE

Participants in this database [41] were randomly assigned to three 30-person groups. Specific databases and fingerprint scanners were assigned to each group. Five volunteers overlapped two databases, but else the subjects were different. Three collection site sessions were required for each participant. Each session was at least two weeks apart. During each session, data was collected from the forefinger and middle finger of both hands, resulting in a total of four fingers. Interleaving finger acquisition sequence maximized finger positioning variability. Each volunteer's four fingers received four impressions per session. Participants first placed their finger at different vertical positions (impressions 1 and 2) and applied mild and high pressure to the sensor surface (impressions 3 and 4). Next, participants were instructed to purposely exaggerate finger rotation (impressions 3 and 4) and skin distortion (impressions 1 and 2). During the third session, fingers were subjected to a drying process (1 and 2) and subsequently exposed to moisture (3 and 4). After data collection, each database had 120 fingers and 12 impressions per finger, totaling 1440 impressions. Similar to previous generations, each database was 110 units wide (w) and 8 units deep (d), totaling 880 units (representing fingerprints). In this work, we employed fingerprint images from all 120 individuals using four impressions for each one in the four groups with total of 960 images. The FVC2004 dataset is recognized for its detailed and structured collection methodology, making it a standard benchmark in fingerprint recognition research.

2) FV-USM DATABASE

The database includes a collection of photographs obtained from a total of 123 individuals, consisting of 83 males and 40 females [42]. The age of the participants spanned from 20 to 52 years. Each participant underwent testing with four specific fingers: the left index finger, left middle finger, right index finger, and right middle finger. This yielded 492 finger classes. Geometric qualities and vein patterns were found in finger images. Six finger repeats were recorded for each session, and each subject completed two sessions almost two weeks apart. The original session yielded 2952 images, computed by multiplying 123 by 4 and then by 6. Two sessions yielded 5904 images from 492 finger courses. The finger images have 640 × 480 spatial resolution and 256 grey levels depth. In this work, we employed finger vein images from 120 individuals using the four fingers for each one in the two sessions with a total of 960 images. The FV-USM dataset provides a rich source of vein patterns, essential for evaluating finger vein recognition systems. Table 1 summarizes the details of all datasets used in this study.

These datasets were selected to provide a robust and diverse evaluation environment for our proposed biometric authentication approach.

B. END-TO-END DEEP LEARNING MODELS FOR FINGER VEIN AND FINGERPRINT AUTHENTICATION

A distinctive hallmark of this study is the adoption of an end-to-end deep learning paradigm. In this novel approach, the input images from both modalities are directly fed into a

deep neural network for recognition without the need for conventional preprocessing steps. The end-to-end deep learning model simplifies the overall system complexity by integrating data preprocessing, feature extraction, and classification within a single architecture. Traditional preprocessing steps, which can be intricate and time-consuming, are circumvented, leading to a more efficient and streamlined workflow. The deep learning model inherently learns discriminative features from raw input images, mitigating the need for manual feature extraction. Complex patterns and relationships within the images are autonomously captured by the model's architecture. The end-to-end approach treats the entire process as a holistic biometric authentication task, enabling the model to optimize feature extraction and classification jointly.

In this Section, we delve into the intricacies of the end-to-end deep learning models designed for finger vein and fingerprint authentication. Each model is meticulously constructed to process the corresponding biometric modality's raw input images. The layers, operations, and activation functions within each model are examined in detail.

1) FINGER VEIN MODEL ARCHITECTURE

The finger vein model consists of the following layers, each contributing to the gradual extraction of features and subsequent classification as shown in Figure 2.

The images are fed into the network with dimensions of 240×320 and a single channel (grayscale). The model starts with a series of convolutional layers that convolve the input images with 3×3 filters. The first convolutional layer applies 3 filters with a stride of 1. Subsequent layers apply the same filter size and stride, capturing local features and patterns. After each convolutional layer, max-pooling layers with a 2×2 window and stride of 2 are applied. Max-pooling reduces spatial dimensions, retaining essential features and aiding in translation invariance. Rectified Linear Units (ReLU) are used as activation functions following each convolutional and max-pooling layer. ReLU introduces non-linearity, allowing the network to learn complex patterns. The convolutional layers are followed by fully connected layers. The first fully connected layer consists of 1024 neurons, facilitating feature extraction and compression. ReLU activation is applied to the output of the fully connected layer, followed by a dropout layer with a rate of 0.2. Dropout reduces overfitting by randomly dropping out neurons during training. The final layers include a fully connected layer with 200 neurons and another fully connected layer with 2 neurons, corresponding to the number of classes (genuine or impostor). The SoftMax layer normalizes the output scores into probability distributions for classification.

The mathematical expressions for convolutional and max-pooling layers are represented as follows:

$$y[i,j] = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} w[m,n] .x[i+m, j+n] \quad (1)$$

where:

$y[i,j]$: Output value at position (I, j) of the feature map.

$x[i+m, j+n]$: Input pixel value at position (i+m, j+n).

$w[m,n]$: Convolutional filter weight at position (m, n).

$$y[i,j] = max_{m=0}^{M-1} max_{n=0}^{N-1} x[i+m, j+n] \quad (2)$$

The filters' parameters $w[m,n]$ represent the learnable convolutional weights. The stride of 1 for convolutional layer and 2 for max-pooling layer signify the filter's step size as it traverses the input image $x[i+m, j+n]$.

The ReLU activation function is defined as:

$$f(x) = \max(0, x) \quad (3)$$

where:

$f(x)$: Activation function, outputting x if $x > 0$, else 0.

The dropout operation is denoted as:

$$y = \frac{x}{1-p} \quad (4)$$

where:

y: Output value after dropout.

X: Input value before dropout.

P: Dropout rate.

The SoftMax function for a single class is given by:

$$Softmax(x)_i = \frac{e_i^x}{\sum_j e_j^x} \quad (5)$$

where:

$Softmax(x)_i$: Probability of class i.

e_i^x : Exponential of input x_i.

$\sum_j e_j^x$: Sum of exponentials across all classes.

2) FINGERPRINT MODEL ARCHITECTURE

The fingerprint model exhibits a similar architecture but with more than three layers, tailored to process fingerprint images and capture unique ridge patterns as shown in Figure 2.

Similarly, the fingerprint model begins with an image input layer, accommodating 240×320 grayscale fingerprint images. The model starts with convolutional layers followed by max-pooling layers, akin to the finger vein model. These layers identify local patterns and reduce spatial dimensions. ReLU activation layers introduce non-linearity and enhance the model's ability to capture intricate ridge structures. Following convolutional layers, fully connected layers with 1024 and 200 neurons are employed for feature extraction. A dropout layer with a rate of 0.2 aids in regularization. The final fully connected layer with 2 neurons, combined with a SoftMax layer, performs classification.

The hyperparameters used in both models include the mini-batch size, maximum number of epochs, initial learning rate, learning rate schedule, drop factor, drop period, shuffle strategy, and validation frequency as shown in Table 2. The

hyperparameters work collectively to optimize the training process of the deep models, ensuring efficient convergence and improved model performance.

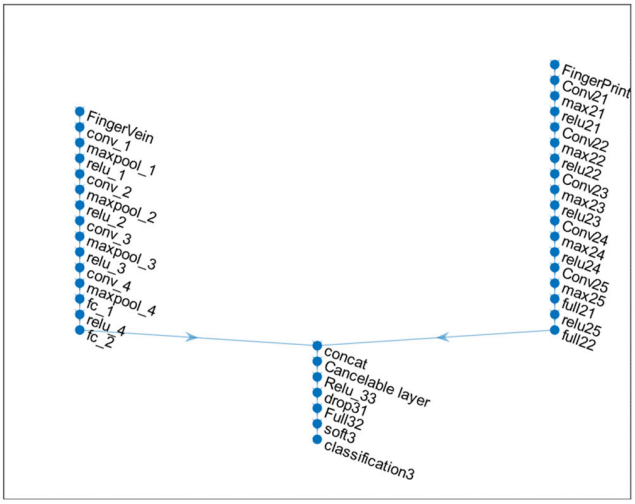


FIGURE 2. The proposed deep cancelable multibiometric model layers.

TABLE 2. The used hyperparameters.

Hyperparameter	Value
MiniBatchSize	16
MaxEpochs	30
InitialLearnRate	3.0000000e-04
LearnRateSchedule	piecewise
LearnRateDropFactor	0.5
LearnRateDropPeriod	5
Shuffle	every-epoch
ValidationFrequency	87

C. COMBINING FEATURES

The fusion of extracted features from both finger vein and fingerprint modalities plays a pivotal role in enhancing the robustness and discriminatory power of the multibiometric system. This section delves into the intricacies of combining these features and highlights the advantages it brings to the recognition process.

Finger vein and fingerprint modalities are processed independently through their respective end-to-end deep learning models. The models capture and learn unique patterns and characteristics intrinsic to each modality. The output of each deep model is a feature vector that encodes the learned information from the corresponding modality. These feature vectors encapsulate important discriminative traits that differentiate individuals based on their finger vein and fingerprint patterns. The feature vectors obtained from the finger vein and fingerprint models are concatenated along a suitable axis to form a unified combined feature matrix. This matrix encapsulates the extracted features from both modalities, resulting in a joint representation that captures complementary information. By combining the features, the system capitalizes on the strengths of both modalities, leveraging their distinctiveness and enhancing recognition accuracy. Finger veins and fingerprint patterns often exhibit variations due to factors such as lighting conditions or pressure. Combining these modalities mitigates the impact of such variations. The combination of features creates a more comprehensive and discriminative representation, leading to improved recognition accuracy. This is particularly beneficial in scenarios where one modality might be less reliable due to factors such as environmental conditions or physiological variations.

D. NON-NEGATIVE MATRIX FACTORIZATION (NMF)

NMF is a widely employed method for reducing dimensionality in diverse domains such as image processing, text mining, and bioinformatics [43], [44], [45]. In the context of multimodal biometrics (combining finger vein and fingerprint data), NMF can be employed as a cancelable method to enhance security and privacy while maintaining biometric recognition capabilities.

NMF is a matrix factorization technique utilized to decompose a non-negative data matrix, conventionally represented as A, into two non-negative matrices W (base matrix) and H (encoding matrix) [46]:

$$A \approx WH \tag{6}$$

where:

1) **Data Matrix (A)**: This matrix represents the original data, where each row corresponds to a sample, and each column corresponds to a feature.
2) **Basis Matrix (W)**: W contains the basis vectors or components. These components are used to represent the original data. W has dimensions ($m \times k$), where m is the number of samples, and k is the desired reduced dimensionality or the number of basis vectors.
3) **Encoding Matrix (H)**: H contains the coefficients that weigh the basis vectors to reconstruct the original data. H has dimensions ($k \times n$), where n is the number of features.

The goal of NMF is to find W and H such that their product approximates the original data A while ensuring that all elements in W and H are non-negative. Figure 3 shows a simple description of NMF.

E. GENERATING CANCELABLE TEMPLATES

In this subsection, we describe the process of generating cancelable templates using the SHA-256 hash function to ensure irreversible transformation of biometric features.

- **Feature Extraction**: Extract features from finger vein and fingerprint data separately. Let's denote the feature matrices as FV_features (for finger vein) and FP_features (for fingerprint), where each row represents a user, and each column represents a feature.
- **Concatenation**: Concatenate the feature matrices horizontally to create a combined feature matrix C:

$$C = [FV\_features|FP\_features] \tag{7}$$

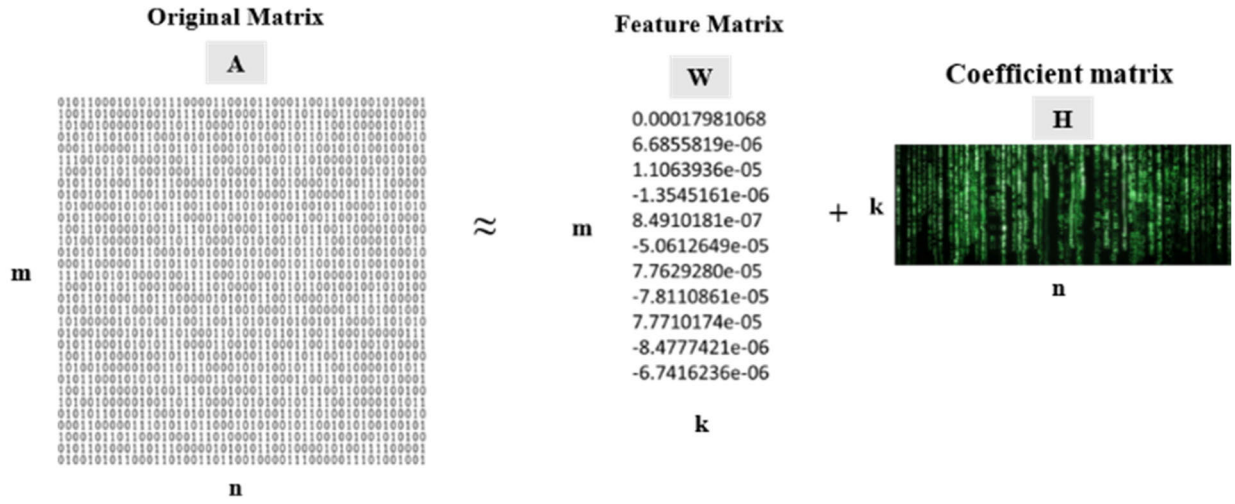


FIGURE 3. Description of NMF.

- **Non-negative Matrix Factorization**: Apply NMF to the combined feature matrix C to obtain the basis matrix W and encoding matrix H, where $C \approx WH$.
- **Cancelable Transformation**: To enhance privacy, we can apply a cancelable transformation to either W, H, or both. This transformation can be based on cryptographic techniques like hash functions or random projections. In our case, the Hash function SHA-256 [47] is used to generate unique and non-invertible representations of the transformed features.

The Cancelable Transformation proceeds as follows:

- For basis matrix W: Each element W(i,j) of the basis matrix W is converted to a string representation, which serves as the input to the SHA-256 hash function. The resulting hash values represent unique and non-invertible representations of the basis vectors.
- For encoding matrix H: Similarly, each element H(i,j) of the encoding matrix H undergoes the same process of conversion to a string and subsequent hashing.

Once the hash values are obtained for both matrices W and H, they are converted from hexadecimal to decimal numeric values. This conversion ensures that even if the NMF matrices are compromised, an attacker cannot easily reconstruct the original biometric data.

Mathematically, the cancelable transformation can be represented as:

$$W' = F(W)H' = G(H) \tag{8}$$

$$C' = W'^{*}H' \tag{9}$$

where F and G are the cancelable transformation functions. By seamlessly integrating NMF with a cancelable transformation, we forge a robust and privacy-preserving representation of multimodal biometric data. This cancelable template serves as a secure foundation for biometric recognition tasks, safeguarding individuals' privacy while upholding the integrity and reliability of the biometric system. Algorithm 1 shows the steps of generating the cancelable template using our method.

F. USABILITY AND REAL-WORLD INTEGRATION

While the advancements in privacy, security, and accuracy are paramount, the usability of biometric authentication systems remains a critical concern. Our proposed method addresses several usability challenges, ensuring high user acceptance, ease of use, and seamless integration into existing systems as the following:

- The proposed system is designed with a user-centric approach, focusing on a simple and intuitive enrollment process. Users can register their biometric data (finger vein and fingerprint) through a straightforward process that requires minimal technical knowledge. Once enrolled, the authentication process is quick and non-intrusive, where users place their finger on the scanner, and the system performs real-time computations to provide instant feedback.
- Our method is compatible with standard biometric hardware, avoiding the need for specialized equipment. This compatibility facilitates easy integration into existing biometric systems. The system's modular design allows for seamless incorporation into current IT infrastructures, requiring minimal modifications. Additionally, the interoperability with various biometric standards ensures compatibility with different devices and systems used in various industries.
- To validate the usability of our system in future work, we plan to conduct pilot testing in controlled environments and gather feedback from participants. These pilot tests will aim to assess user satisfaction with both the enrollment and authentication processes. Future user acceptance studies will be conducted to evaluate

feedback on the system's ease of use and comfort. Additionally, practical evaluations in real-world scenarios, such as office access control, will be undertaken to demonstrate the system's robustness and reliability, even under varying conditions.

G. CROSS-VALIDATION

Cross-validation is a fundamental approach utilized to assess the efficacy and generalizability of machine learning models, specifically within the realm of biometric authentication [48]. This section focuses on the application of cross-validation techniques within the framework of cancelable deep learning, specifically using NMF for cross-modal biometric authentication. The use of cross-validation is essential in evaluating the resilience and dependability of our proposed methodology. To conduct cross-validation, the biometric data was initially divided into several subsets. Given the multi-modal nature of the data, a meticulous partitioning technique was implemented to ensure that the training and testing sets encompassed representative samples from all modalities.

1) *Training and Validation Procedures:*
- **Model Training**: The deep learning models were trained using a framework incorporating NMF. The training process included normalization and augmentation of the image data to handle variability and enhance model performance.
- **5-Fold Cross-Validation**: We utilized the 5-Fold cross-validation technique [49], dividing the data into five subsets of approximately equal size. Each fold was sequentially used as the validation set, while the remaining four folds were employed for training the model. This procedure was repeated five times, with each fold serving as the validation set exactly once. This method provides a comprehensive evaluation of the model's performance and ensures that the intrinsic unpredictability of the data is adequately addressed.

2) *Results and Analysis of the Cross-Validation:*
- **Performance Metrics**: During cross-validation, metrics such as accuracy, precision, recall, F1 score, and Equal Error Rate (EER) were calculated for each fold. The results from these iterations were aggregated to assess the model's overall performance.
- Comparative Performance: Our approach was compared with established methods in biometric authentication. The comparative analysis revealed that our method achieved superior performance metrics, demonstrating higher validation accuracies and lower EERs compared to many traditional techniques.

H. PERFORMANCE EVALUATION

A variety of performance indicators are utilized to evaluate the efficacy of the model in accurately discerning users, while simultaneously upholding the privacy and security of their biometric data.

Algorithm 1 Generating Cancelable Template

Start
Input: Combined_Features, W, num_samples, num_components, hash_values
Output: Hash values converted to a numeric matrix
Load Features
Extract features from the test data
Apply NMF to test data using the same 'W' obtained from training
Generate Cancelable Template:
  For I from 1 to num_samples:
  For j from 1 to num_components:
  - Convert W(I, j) to a string and assign it to value_str.
  - Generate a SHA-256 hash of value_str and assign it to hash_value.
  - Store hash_value in the corresponding cell of cancelable_templates (I, j).
  End For
End For
convert_hash_to_numeric_matrix(hash_values):
  For I from 1 to num_rows:
  For j from 1 to num_cols:
  - Convert the hex hash value hash_values(I, j) to a decimal numeric value and store it in numeric_matrix(I, j).
  End For
End For
End

1) Accuracy: a core metric for assessing correctness, is quantified as the proportion of accurately identified samples to the total number of samples in the evaluation dataset.

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

Whereas TP is the number of true positives. The variable TN represents the number of true negatives. The term FP represents the numerical value of false positives. The variable FN represents the number of false negatives.

2) Precision (PR): is a metric that measures the ratio of accurately recognized positive samples to the total number of samples that were classified as positive.

$$PR = \frac{TP}{TP + FP} \tag{11}$$

3) Recall (RC): alternatively referred to as the true positive rate or sensitivity, quantifies the proportion of genuine positive samples that were accurately identified as positive.

$$RC = \frac{TP}{TP + FN} \tag{12}$$

4) The F1-Score (F1): composite metric that integrates precision and recall, utilizing the harmonic mean to

achieve a balanced evaluation of both measures.

$$F1 = \frac{2 \times PR \times RC}{PR + RC} \tag{13}$$

IV. RESULTS AND ANALYSIS

In this section, we present the empirical results obtained from our comprehensive evaluation of the cancelable deep learning approach utilizing NMF for cross-modal biometric authentication. The results are based on the 5-Fold cross-validation strategy. The investigation was done on a 2.4GHz Intel Core i5 CPU. Due to its 24MB RAM, the system had enough processing capability for our tests. We used an NVIDIA GeForce GTX 1650 GPU for parallel processing to improve our deep learning methods. MATLAB R2019b with the Deep Learning Toolbox was our main software environment for this investigation. We used the platform's deep learning capabilities and resources. The final architectures and hyperparameters were selected based on extensive experiments to ensure that the models provided a robust, efficient, and accurate solution for biometric authentication using finger vein and fingerprint data. In this paper, we evaluated our work using two multimodal databases for fingerprint and finger vein. Firstly, we employed NUPT-FPV database [40], which is suitable for real-time applications and captured from the same source. Secondly, we employed a database consisting of two publicly available databases from different resources: the FVC2004 database [41] for fingerprint samples and the FV-USM database [42] for finger vein samples. All details about the two databases and how we patronized them are discussed in the previous section.

A. PERFORMANCE OF THE PROPOSED MODEL USING NUPT-FPV DATABASE

Based on the data depicted in Figure 4, a thorough examination of the training and validation curves provides valuable insights into the model's learning process. The depicted curves illustrate the trajectory of accuracy and loss, so providing significant observations. To achieve accuracy, the curves initiate at epoch 0, where an initial accuracy of 75% is seen. The initial accuracy of the model indicates its competence in accurately categorizing data from the outset. As the epochs progress, the training accuracy demonstrates a stable and continuous increase, ultimately reaching a pinnacle of 100%. This observation suggests that the model has effectively acquired and retained knowledge from the training data. On the other hand, the curve representing the correctness of the validation set demonstrates consistent and commendable performance throughout the training process, maintaining a noteworthy accuracy rate of 95.31% until the conclusion of the 10th epoch. The study demonstrates that the model consistently achieves high validation accuracy, indicating its capacity to efficiently apply learned knowledge to novel data. This ability is of utmost importance in the context of cross-modal biometric identification.

The loss curves demonstrate that at epoch 0, the training loss begins at 0.7%. This indicates that the initial predictions made by the model have a relatively lower level of confidence. As the training regimen progresses, these curves exhibit a significant pattern. The training loss demonstrates a consistent decrease, gradually approaching 0% as the 10th epoch closes. This implies that the model is effectively converging, hence reducing the disparity between its predicted outputs and the actual target labels inside the training dataset. In a similar manner, the curve representing the loss throughout the validation phase has a similar pattern, steadily decreasing until it reaches a value of 0.2% at the eighth epoch. The consistent decrease in both training and validation loss suggests that the model possesses the capability to not only memorize the training data but also efficiently apply its acquired knowledge to new, unfamiliar samples.

The performance of our cancelable deep learning model in the context of cross-modal biometric identification is encapsulated by the confusion matrix shown in Figure 5 for the test sets. The provided representation of the model's categorization findings offers a distinct and organized differentiation between the actual and forecasted classes.

The confusion matrix demonstrates the system's high accuracy in correctly identifying and accepting authentic users. It reveals 96 occurrences of true positives, suggesting a strong capability to distinguish real users without any cases of falsely classifying them as negatives. Although the system exhibited 9 instances of false positive cases, wherein impostor samples were erroneously accepted, the system's overall performance remained robust, as evidenced by the detection of 87 genuine negative instances. This indicates the system's effectiveness in accurately rejecting impostors. The system's capacity to maintain accuracy and security is highlighted by its balanced performance, which is characterized by a high true positive rate and a low false negative rate. This makes it a promising option for biometric authentication applications.

B. PERFORMANCE OF OUR MODEL USING FVC2004 DATABASE AND THE FV-USM DATABASE

Based on the information presented in Figure 6, an analysis of the training and validation curves reveals significant insights into the learning process of the model. To ensure precision, the curves commence at epoch 0, when an initial accuracy of 60% is seen. This initial accuracy signifies the model's proficiency in properly classifying data from the beginning. As the epochs advance, the training accuracy exhibits a consistent upward trend, reaching a maximum value of 100%. This observation implies that the model has successfully acquired and retained knowledge from the training data. In contrast, the validation accuracy curve exhibits a persistent and praiseworthy performance throughout the training procedure, sustaining a notable accuracy rate of 92.71% until

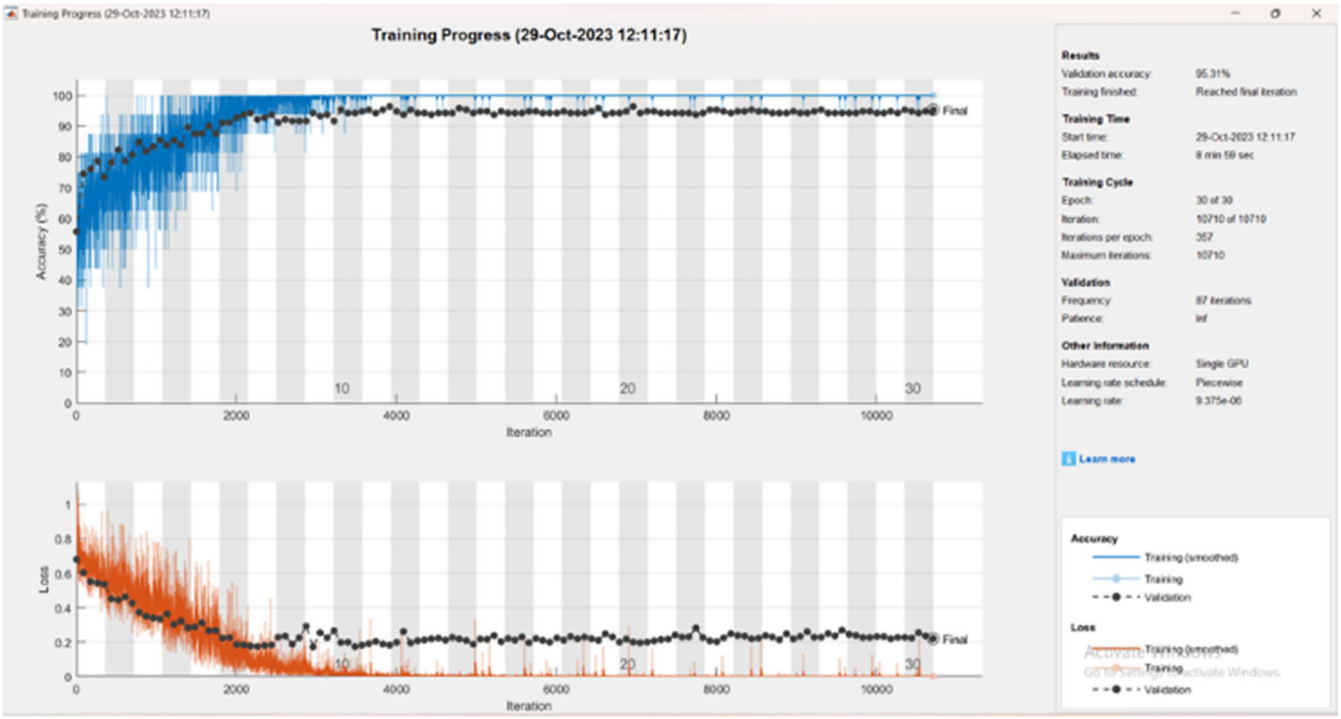


FIGURE 4. Training progress of our method using NUPT-FPV database.

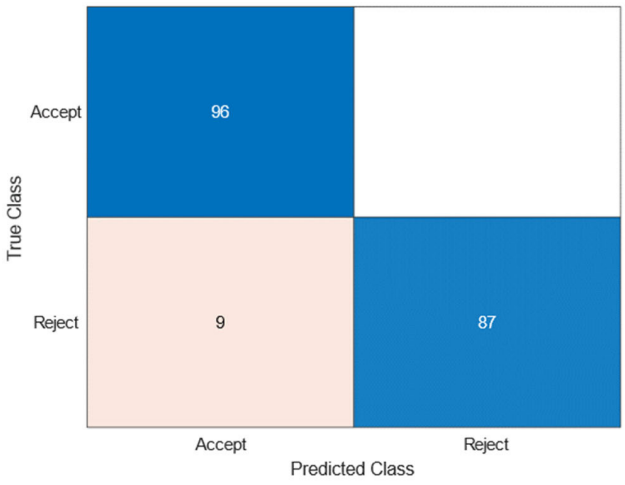


FIGURE 5. Confusion matrix of our method using NUPT-FPV database.

the culmination of the 15th epoch. The consistent validation accuracy seen in this study highlights the model's ability to effectively generalize to unfamiliar data, which is a crucial factor in cross-modal biometric identification.

For the loss curves, it is observed that they commence at epoch 0 with a training loss of 0.6%, suggesting that the model's first predictions exhibit a comparatively diminished level of certainty. As the training regimen advances, these curves demonstrate a noteworthy pattern. The training loss exhibits a continuous decline, gradually converging towards 0% as the 15th epoch concludes. This suggests that the model is successfully approaching convergence, hence minimizing the discrepancy between its predicted outputs and the true target labels inside the training dataset. Similarly, the validation loss curve exhibits a comparable trend, continuously declining until it reaches a value of 0.3% at the 15th epoch. The observed persistent decline in both training and validation loss indicates that the model exhibits not only the ability to memorize the training data but also the capacity to effectively generalize its learning to novel, unseen samples.

The performance of our cancelable deep learning model in the context of cross-modal biometric identification is encapsulated by the confusion matrix shown in Figure 7 for the test sets. In the given confusion matrix, it is evident that the true class "Accept" exhibits a count of 91, indicating the model's proficiency in successfully classifying legitimate users during the authentication procedure. In contrast, the model exhibited five occasions in which it inaccurately classified legal users as "Reject," therefore resulting in FN. The limited occurrence of false negative examples implies that the model exhibits a low propensity for erroneously classifying legitimate users as fraudulent.

On the other hand, the "Reject" class demonstrates comparable commendable performance. The algorithm effectively detects and forecasts the classification of "Reject" in 87 instances, indicating TP where imposter samples are accurately identified. There exist nine instances in which the model made inaccurate predictions of "Accept" for impostor samples, hence leading to the occurrence of FP. The infrequent presence of false positive examples serves to highlight

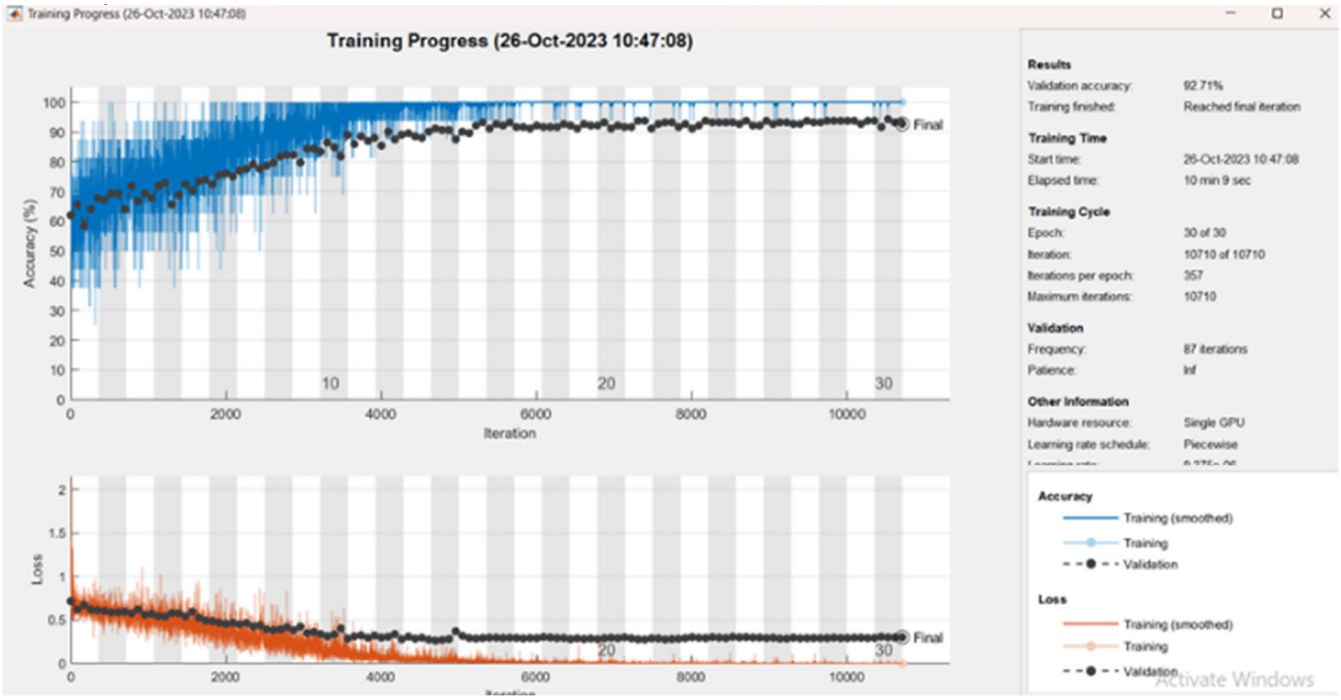


FIGURE 6. Training progress of our method using the combination databases.

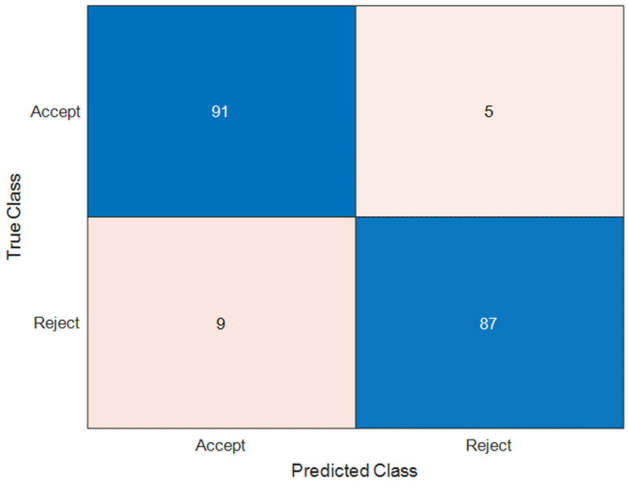


FIGURE 7. Confusion matrix of our method using the combination databases.

the model's resilience in effectively reducing the occurrence of false acceptances.

C. CANCELABLE CRITERIA

1) IRREVERSIBILITY TEST

The quality of irreversibility holds significant importance in multimodal biometric authentication systems, since their major goal is to guarantee that the alteration of initial biometric data remains permanent and cannot be undone. Within this conceptual framework, the concept of irreversibility refers to the extent of dissimilarity between the initial multimodal biometric data and its modified counterpart, rendering any endeavors to reverse engineer the data impractical. The quantification of irreversibility plays a vital role in assessing the efficacy of a cancelable biometric system. Prominent metrics utilized for quantifying irreversibility encompass the Bit Error Rate (BER) and the Hamming Distance. These metrics evaluate the degree of dissimilarity between the original data and its altered counterpart. The attainment of a substantial level of irreversibility is of utmost importance to discourage any illegal attempts at reverse engineering the biometric template, hence ensuring the protection of user privacy and system security. The selection of transformation methods and parameters is crucial in defining the level of irreversibility in practical applications. This requires a delicate balance between maximizing security and minimizing the influence on authentication accuracy. In this instance, the method of BER was utilized to compute the irreversible rate. The steps to calculate irreversibility using the BER:

- Apply the cancelable transformation to generate the transformed templates.
- Compare the original template with the transformed template.
- Calculate the BER using the following:

$$BER = (1/N) \sum |x_i - y_i|^2 \tag{14}$$

where: BER represents the extent of dissimilarity between the original and transformed biometric templates. N is the total number of biometric templates being compared. x_i represents the transformed (or protected) biometric template. y_i represents the reference (original) biometric template. | . | denotes

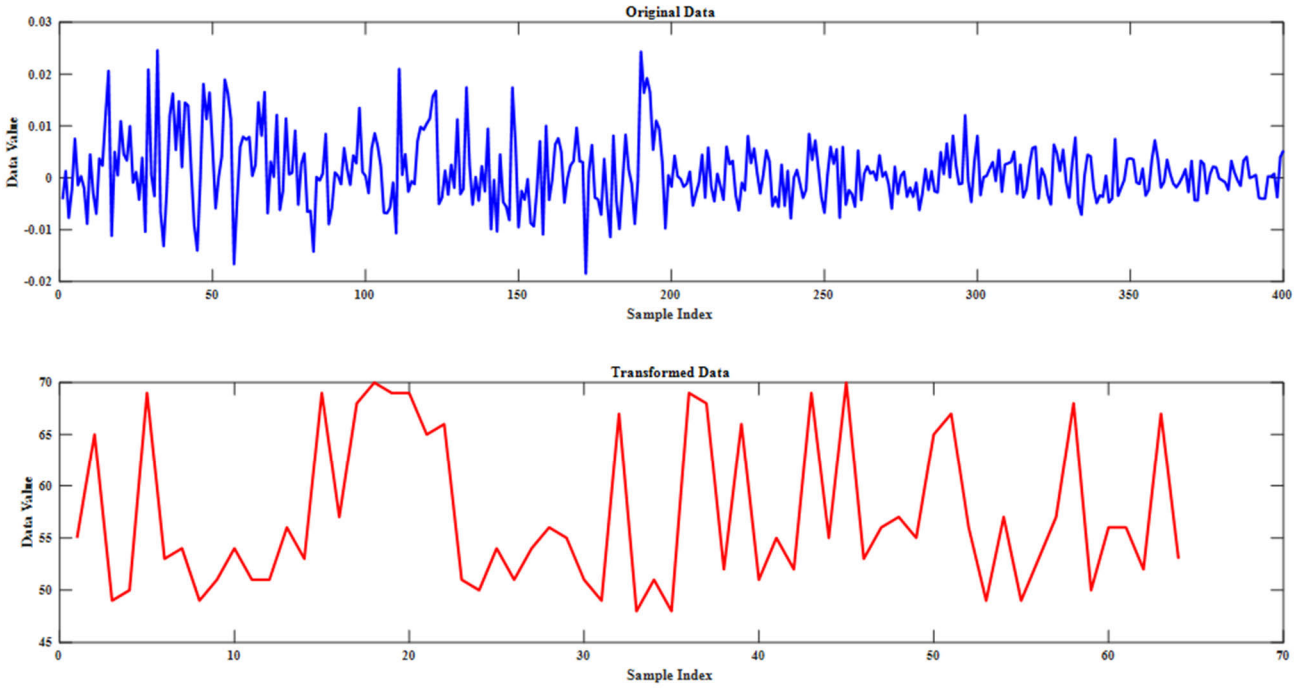


FIGURE 8. Plots of the original and the transformed data.

the absolute value or magnitude of the complex difference between the transformed and reference templates.

- The BER measures the dissimilarity between two templates, where a higher BER indicates higher irreversibility.

Figure 8 shows the plots for original data and the transformed data. From the Figure, we compute the BER which is equal to 1. A BER of 1 indicates that the two sets of data are entirely dissimilar, and no bits in the received or transformed data match their counterparts in the original data.

2) UNLINKABILITY TEST

Unlinkability is a fundamental requirement in cancelable biometrics to protect user privacy and data security. To assess the unlinkability of cancelable biometric templates, a robust unlinkability test must be conducted. This test involves comparing the cancelable templates generated from different biometric samples to ensure that they are unlinkable, meaning they cannot be associated with the same user. The test aims to verify that the transformation process effectively disassociates biometric templates from individual users and that the resulting templates exhibit no inherent connections. To perform the unlinkability test, we perform the following:

- Apply the cancelable transformation method to generate cancelable templates.
- Compare the cancelable templates in a pairwise manner.
- Use appropriate distance metrics (in our case, we employed Hamming distance) to quantify the similarity or dissimilarity between templates.

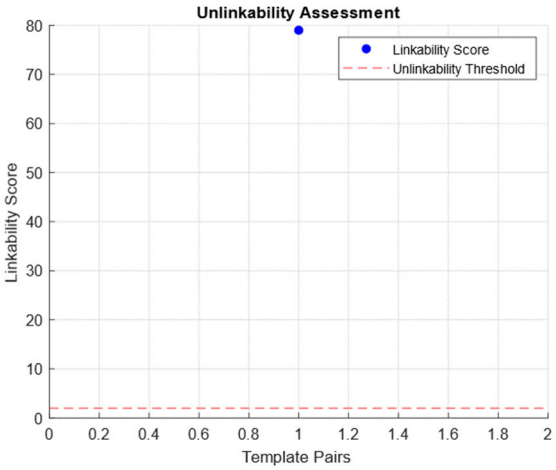


FIGURE 9. Unlinkability assessment.

- Define a threshold for unlinkability. If the distance between templates exceeds this threshold, they are considered unlinkable.
- Execute the unlinkability test by comparing all possible pairs of cancelable templates. The test should verify that templates generated from different users or different instances of the same user are unlinkable.
- Validate the chosen unlinkability threshold through empirical analysis and simulations to ensure that it provides the desired level of privacy.

Figures 9 and 10 show the unlinkability analysis based on random features from the used data.

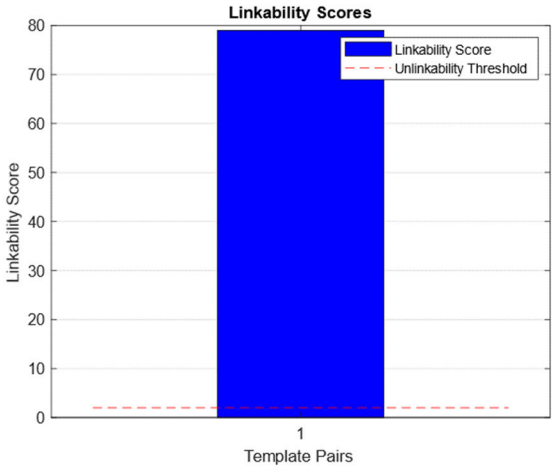


FIGURE 10. Linkability Scores versus unlinkability threshold.

3) DIVERSITY TEST

The Diversity Test is a critical component of cancelable biometric systems designed to protect user privacy and security. In this test, the aim is to assess the diversity and dissimilarity of transformed biometric templates to ensure that they cannot be easily linked, even if multiple templates originate from the same user. This test serves as a crucial step in evaluating the effectiveness of a cancelable biometric method in preserving unlinkability, thereby safeguarding sensitive biometric data.

We employed the following steps:

- Apply a suitable distance or dissimilarity metric (in our case, we employed Hamming distance) to calculate the diversity between pairs of transformed templates.
- Determine a threshold value that separates diverse templates from similar ones. The choice of the threshold depends on the specific application and the requirements for unlinkability.
- Calculate the diversity scores between all template pairs and compare them to the chosen threshold. Templates with diversity scores below the threshold are considered diverse, while those above the threshold are considered similar.

Table 3 shows the analysis of diversity based on the two databases using 5 random templates from the same person.

Based on the data presented in the preceding Table, it can be observed that there is no occurrence of templates with identical sizes throughout all databases. Consequently, we take measures to guarantee that various users own unique and uncorrelated cancelable representations of their finger biometrics, all the while maintaining the discriminative capability of the deep features produced by the deep learning model.

V. DISCUSSION AND COMPARISON

Significant results were obtained through the utilization of NMF in our cancelable deep learning method for authentication. The employment of 5-fold cross-validation facilitated a rigorous assessment, with the resulting performance metrics demonstrating a notable degree of precision, as demonstrated by the validation accuracies of 95.31% and 92.71%. The performance metrics of the system exhibited encouraging prospects in protecting user privacy through the efficient mitigation of unwanted access risks. Table 4 shows the overall

TABLE 3. Diversity analysis on the two databases.

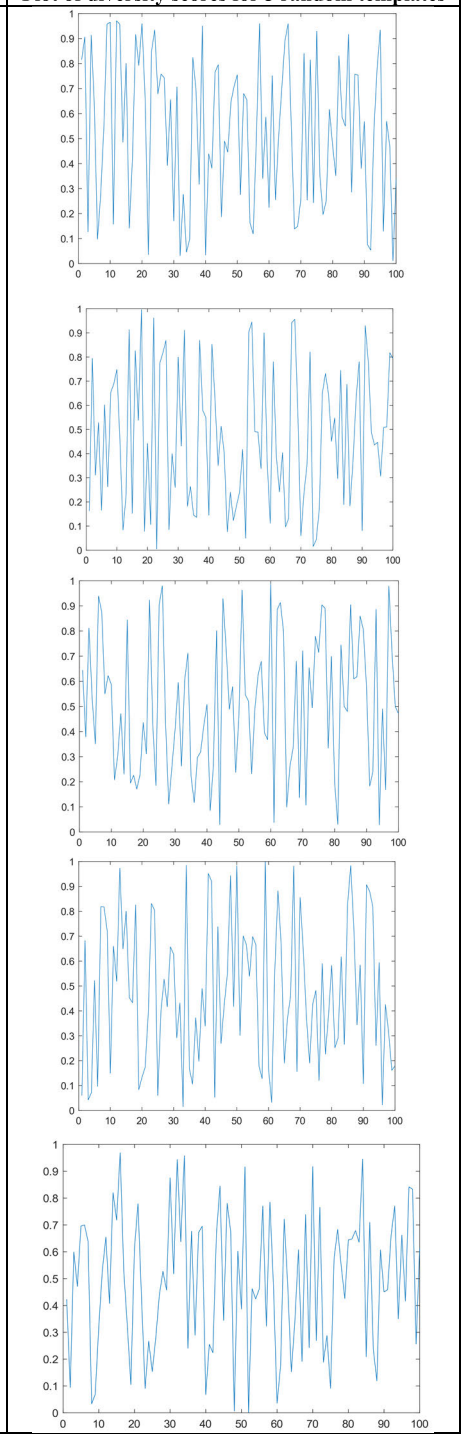
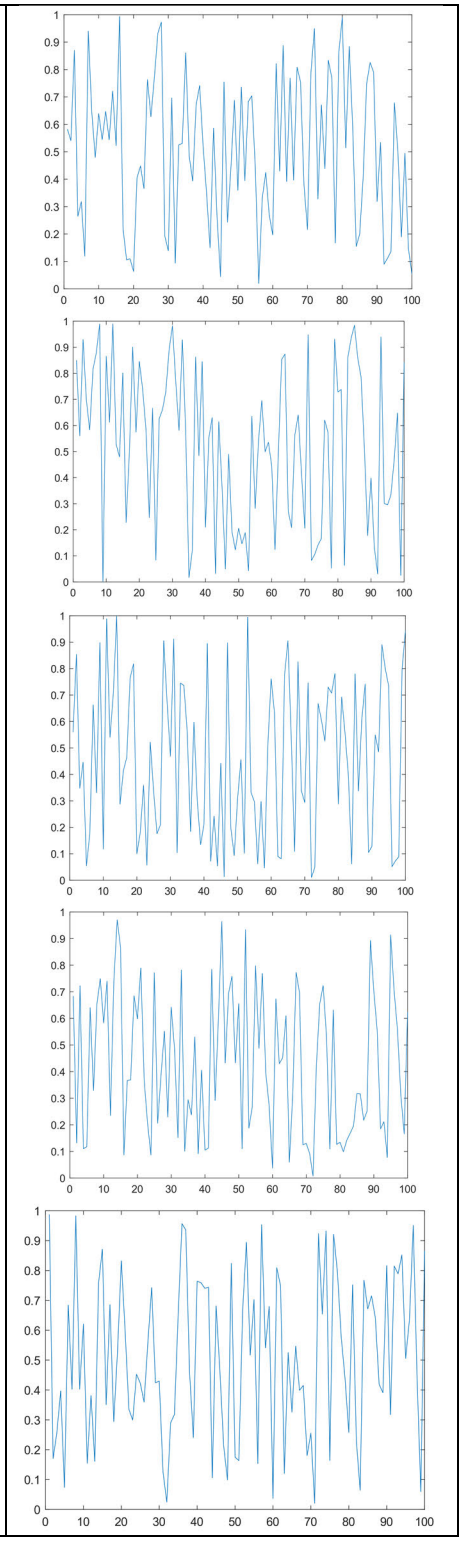
Dataset	Plot of diversity scores for 5 random templates
NUPT-FPV [40]	

TABLE 3. *(Continued.)* **Diversity analysis on the two databases.**

FVC2004 [41] + FV-USM [42]	

performance of the proposed method using 5-fold techniques on the two databases.

The cancelable deep learning approach using NMF demonstrates a strong and reliable performance in cross-modal biometric authentication, as seen in Figure 4 by the excellent convergence of the loss functions and a validation accuracy of 95.31%. The computational economy of our approach is demonstrated by the elapsed time of 8 minutes and 59 seconds for 30 epochs. Additionally, the stability of the validation curves indicates the absence of overfitting signs, which serves as evidence for the generalization capabilities of the model. The findings presented in this study make a significant contribution to the progress of safe and privacy-preserving biometric authentication systems. Moreover, they establish a robust basis for the practical implementation of these systems in real-world scenarios and offer valuable insights for future research endeavors in this domain.

TABLE 4. **Overall performance of our method using the two databases.**

Dataset	Fold	Val. ACC (%)	Val. PR (%)	Val. RE (%)	Val. F1 (%)	Val. EER (%)
NUPT-FPV [40]	1	95.11	94.40	95.65	95.21	4.5
	2	94.61	94.76	94.47	94.63	5.3
	3	95.41	95.22	95.96	95.52	4.4
	4	96.15	96	96.30	96.10	3.6
	5	95.28	95.52	95.18	95.30	4.5
Avg.		95.31	95.18	95.51	95.35	4.4
FVC2004 [41] + FV-USM [42]	1	92.68	92.94	92.69	92.71	7.2
	2	92.52	92.35	92.65	92.45	7.4
	3	92.76	92.92	92.80	92.86	6.9
	4	92.57	92.58	93.17	92.94	7.3
	5	93.05	92.98	92.75	92.86	6.7
Avg.		92.71	92.75	92.81	92.76	7.1

From Figure 5's confusion matrix, the model's capacity to authenticate users while respecting privacy is shown by the minimal false negatives and positives and the good depiction of true positives and negatives. The results serve to strengthen the dependability of the model and its viability for practical implementation in biometric authentication systems. Upon analyzing the plots presented in Figure 5, it becomes evident that the irreversibility rates for the datasets under consideration are 100%. The aforementioned number indicates that the cancelable biometric methods utilized in the datasets exhibit a significant level of irreversibility, hence demonstrating their efficacy in safeguarding the original templates against reconstruction attacks. Moreover, as depicted in Figure 9, the proposed approach demonstrates a heightened capacity of the system to discern the linkability score from the unlinkability threshold, which is regarded as a measure of unlinkability. In terms of diversity, our analysis of Table 3 revealed that the primary determinant of diversity was the implementation of varying thresholds during the registration process. The utilization of the cancelable method resulted in the attainment of diversity, which presented numerous benefits. Initially, the implementation of cancelable templates has contributed to the bolstering of system security by introducing a heightened level of complexity that deters unauthorized individuals from reverse-engineering the original biometric information. The presence of distinct components in each template posed difficulty in extracting significant insights from the archived data.

Due to the individualized nature of the cancelable templates and their ability to be periodically regenerated, the system maintained its resilience against prospective attacks and the gradual deterioration of biometric data.

Our analysis will delve into the comparative performance of our system against uni-biometric systems based on deep learning [52], [53], [54], [55], [56]. Zia et al. [52] enhanced fingerprint classification by addressing false positives using model uncertainty based on Bayesian principles. They obtained a validation accuracy of 95.3% using FVC-2004 dataset. Boucherit et al. [53] introduced the Merge CNN, which enhances deep network performance by integrating multiple CNNs with distinct finger vein image qualities. Through training various networks with the FV-USM dataset and selecting the most effective architecture, the merged CNN obtained a recognition rate of 81.71% using two sessions for testing. Das et al. [54] introduced CNN for finger-vein identification. The primary aim is to present a deep learning approach capable of consistently delivering accurate results across varying qualities of finger-vein images. They obtained an accuracy of 71.11% using test images from FV-USM dataset. Bakhshi and Veisi [55] introduced a CNN-based fingerprint matching method that directly learns fingerprint patterns from raw image pixels. Their end-to-end CNN approach incorporates the feature extraction part of the trained AlexNet network. On the FVC2002 dataset, the network achieved an EER of 17.5%. Jian et al. [56] presented a lightweight CNN structure based on singularity ROI for fingerprint classification, achieving a testing set accuracy of 93%, surpassing classic non-NN classifiers like RF, KNN, LR, Linear SVM, and RBF SVM. Their CNN model with fewer neurons demonstrates improved suppression of overfitting and robustness to noise. By examining the used performance metrics, we will elucidate the efficacy of our approach in achieving superior authentication outcomes. Compared to traditional uni-biometric methods, we aim to underscore the importance of adopting multimodal approaches to address the evolving challenges of authentication in contemporary contexts. Table 5 shows a comparison between our method and other uni-biometric methods based on fingerprint or finger vein.

To assess the usability of our system in real-world scenarios, we conducted additional experiments simulating various environmental conditions:

1) Lighting Environments: We simulated different lighting conditions by adjusting the brightness of the input images using data augmentation techniques. This allows us to evaluate the system's robustness to varying illumination levels.
2) Varying Skin Conditions: We introduced variations in the skin conditions, such as different textures and noise levels, to mimic real-world scenarios where skin conditions can affect biometric readings. Data augmentation methods were employed to generate these variations.
3) Partial Fingerprints: We tested the system's performance with partial fingerprints by cropping and masking parts of the input images. This helps in understanding the system's reliability when only a portion of the fingerprints is available. Figure 11 shows the effect of these conditions on some samples of the images. Table 6 shows the results of our method under real-time conditions during the five folds.

TABLE 5. Comparison table with other previous uni-biometric systems.

Authors/Ref	Methods	Dataset	Performance
Zia et al. [53]	Model uncertainty based on Bayesian principles + CNN	FVC-2004	Accuracy = 95.30%
Boucherit et al. [54]	Merge CNN	FV-USM	Accuracy = 81.71%
Das et al. [55]	CNN	FV-USM	Accuracy = 71.11%
Bakhshi and Veisi [56]	CNN	FVC2002	EER = 17.50%
Jian et al. [57]	Lightweight CNN	FVC-2004	Accuracy = 93%
The proposed work	CNN + NMF	NUPT-FPV (both biometrics) FVC 2004 (Fingerprint) FV-USM (Finger vein)	Accuracy using NUPT-FPV = 95.31% Accuracy using FVC 2004 with FV-USM = 92.71%

TABLE 6. Overall performance of our method under real-time conditions on the two datasets.

Dataset	Fold	Val. ACC (%)	Val. PR (%)	Val. RE (%)	Val. F1 (%)	Val. EER (%)
NUPT-FPV	1	94	94.50	92	93.20	6
	2	91.50	88	93	90.40	8.5
	3	93.50	93.50	91	92.20	6.5
	4	93	92	94	93	7
	5	92.30	91	90	90.50	7.7
Avg.		92.86	91.80	92	91.86	7.1
FVC2004 + FV-USM	1	91.34	90.80	92	91.4	8.6
	2	90.04	89.50	90.50	90	9.9
	3	90.04	90.04	90.04	90.04	9.9
	4	90.93	91	91.50	91.20	9
	5	90.87	90.80	91	90.90	9.1
Avg.		90.64	90.32	91.10	90.70	9.3

Compared to the results in Table 4, the NUPT-FPV dataset shows a noticeable drop in performance under simulated real-world conditions. The average accuracy decreases by 2.45%, from 95.31% to 92.86%. Precision, recall, and F1 score also decline, indicating the system's reduced effectiveness under challenging conditions. The increase in EER from 4.4% to 7.1% further highlights the system's decreased reliability when exposed to variations in lighting, skin conditions, and partial fingerprints. For the combined FVC2004 and FV-USM dataset, the average accuracy drops by 2.07% under real-time conditions. The precision, recall, and F1 score also see a reduction, and the EER increases from 7.1% to 9.3%. These results indicate that the system's performance is adversely affected by real-world conditions, albeit to a slightly lesser extent compared to the

TABLE 7. Comparison table with other previous multibiometric systems.

Authors/Ref	Methods	Fusion	Dataset	Performance
Cherrat et al. [26]	Gabor filter + thinning method (Fingerprint) Linear Regression Line + HOG (Finger vein)	Decision level fusion	FVC 2004 (Fingerprint) + VERA [50] (Finger vein)	Accuracy = 96,28%
Kovaˇc and Mar´ak [24]	Gabor filter + Deep CaffeNet (Fingerprint) SIFT + SURF (Finger vein)	Score level fusion	DUMLA-HMT (both biometrics) [51]	EER = 6.68%
Lin et al. [25]	Gabor filters + Points belonging to specific regions (Fingerprint) classical threshold algorithm + Neighborhood Elimination (Finger vein)	Feature level fusion	FVC2000 (Fingerprint) + self-constructed (Finger vein)	Accuracy = 95.81%
Yang and Zhang [23]	Gabor filter + SLPCCAM (both biometrics)	Feature level fusion	Private database (both biometrics)	Accuracy = 97.76%
Raghavendra et al. [27]	ROI extraction + NIST open source MINDTCT function (Fingerprint) Maximum curvature method + Spectral Minutiae Representation (Finger vein)	Score level fusion	Private database (both biometrics)	EER = 0.78%
Lv et al. [22]	CLAHE + grayscale normalization + ADLBP (both biometrics)	Feature level fusion	ICNIR (private) SDUMLA-HMT (private)	Recognition rate using ICNIR = 95.60% Recognition rate using SDUMLA-HMT = 96.93%
Abdullahi et al. [21]	FS-STMFPFV-Net + ReliefFS feature selection	Feature level fusion	NUPT-FPV (Finger vein) FVC-2002 (Fingerprint)	Accuracy = 99.26%
The proposed work	CNN + NMF	Feature level fusion	NUPT-FPV (both biometrics) FVC 2004 (Fingerprint) FV-USM (Finger vein)	Accuracy using NUPT-FPV = 95.31% Accuracy using FVC 2004 with FV-USM = 92.71%

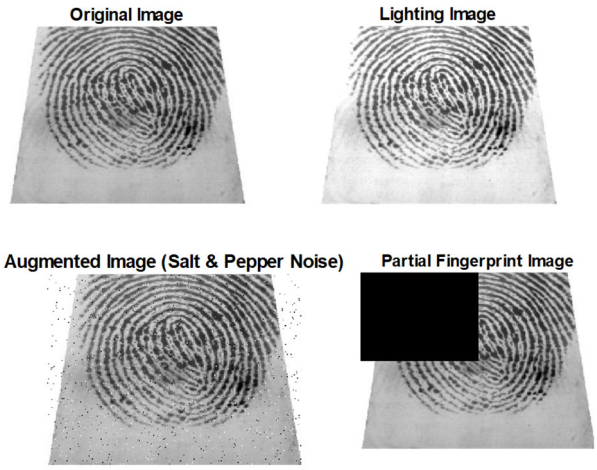


FIGURE 11. Effect of the conditions on sample image from the dataset.

NUPT-FPV dataset. The results highlight the need for further improvements in the system to enhance robustness under real-world conditions. Future work could focus on advanced data augmentation techniques and machine learning models specifically designed to handle variability in environmental conditions. Additional training with more diverse and representative datasets could also improve the system's adaptability and performance in real-world scenarios.

Comparing our fusion feature with existing uni-biometric methods, it outperforms most of them in terms of accuracy. For example, it achieves higher accuracy than Boucherit et al. [53] and Das et al. [54] on the FV-USM dataset, demonstrating the effectiveness of incorporating NMF into our CNN-based approach. Additionally, our fusion feature also shows competitive performance compared to Zia et al. [52] and Jian et al. [56] on their respective datasets, indicating its versatility and robustness across different biometric modalities. This highlights the potential of our fusion feature to enhance authentication accuracy and system robustness in various biometric recognition applications.

The assessment of the status of biometric authentication heavily relies on the examination of different approaches and their performance across distinct datasets. Table 7 provides a comparative analysis of various methods within the domain of fingerprint and finger vein recognition. It emphasizes the fusion techniques employed, datasets utilized, and performance metrics evaluated. In addition, the previous cancelable methods are compared with ours in Table 8.

From the comparison Table 7, we can observe that our method attains a high accuracy rate of 95.31% for NUPT-FPV and 92.71% for FVC 2004 with FV-USM. This demonstrates the effectiveness of the proposed approach in achieving accurate and reliable recognition. Moreover, the fusion technique

employed in our method, which combines CNN and NMF at the feature level, showcases the capability to leverage deep learning for biometric recognition. This combination not only enhances accuracy but also offers potential for feature extraction and transformation, aligning with the cancelable biometrics concept to ensure privacy and security. The utilization of NMF for feature transformation is a notable strength, as it aids in obfuscating the original data's structure, enhancing privacy. In terms of security, cancelable biometrics provides a robust defense against spoofing attacks by transforming the biometric data into a non-reversible format. This transformation ensures that even if the data is compromised, it cannot be used to reconstruct the original biometric templates, thus preventing misuse. Our method's superiority in security is due to the integration of NMF, which obfuscates the data, making it significantly more difficult for attackers to spoof. While other methods reviewed do not employ cancelable biometrics, making them potentially more vulnerable to spoofing attacks, our method inherently provides an additional layer of security. This is particularly important for applications requiring high levels of security and privacy.

Furthermore, our method being suitable for real-time applications, as it utilizes a lightweight deep learning model. While specific real-time performance metrics for earlier methods are not always available, our approach aims to balance accuracy and efficiency. For instance, ours outperforms Kovač and Marák's method [24], which employs Gabor filters and Deep CaffeNet, with a significantly lower EER. Similarly, our method surpasses Lin et al.'s approach [25] using Gabor filters and threshold algorithms, achieving a higher accuracy. Additionally, our method's performance is competitive with, and in some cases exceeds, other techniques like the one by Yang and Zhang [23] that employs Gabor filters and SLPCCAM. Our method ensures robust performance and security in feature-level fusion and achieves authentication rates comparable to other state-of-the-art methods.

In comparison to currently available cancelable biometric approaches in Table 8, our methodology effectively fulfills all cancelable criteria with significant efficacy. Although other approaches may possess advantages in specific domains, our method's ability to effectively maintain privacy, safeguard data, and ensure system resilience establishes it as a prominent contender in the industry. The differences in EER values between our proposed model and the methods developed by Yang et al. [39] and Goh et al. [37] can be attributed to several factors. Goh et al. [37] achieved low EERs by effectively combining IoM hashing and Alignment-Free Hashing (AFH) with feature-level fusion, ensuring computational efficiency and robust privacy protection. Yang et al.'s [39] multi-biometric system, which integrates minutia-based fingerprint and image-based finger-vein features, also exhibited low EERs due to the robust fusion strategies employed and the use of carefully selected datasets like FVC2002 DB2 and FV-HMTD. In contrast, our study focuses on integrating NMF with a lightweight deep learning model, aiming to enhance

TABLE 8. Comparison table of our method with other cancelable methods.

Authors/Ref	Cancelable method	Dataset	Performance (%)
GOH et al. [37]	Index-of-Max (IoM) hashing	FVC 2002 for fingerprint and UTFVP for finger-vein	EER = 1.19
Yang et al. [39]	Enhanced partial discrete Fourier transform (EP-DFT)	FVC2002 DB2 and FVC2004 DB2 for Fingerprint FV-HMTD for Finger vein	EER = 0.55 for FVC2002 DB2 and FV-HMTD EER = 0.69 for FVC2004 DB2 and FV-HMTD
Li et al. [57]	one permutation hashing-based template protection	FVC 2002 and FV 2004 for fingerprint and SDFV for finger vein	EER = 1.49
The proposed model	NMF	NUPT-FPV (both biometrics) FVC 2004 (Fingerprint) FV-USM (Finger vein)	EER = 4.4 for NUPT-FPV EER = 7.1 for FVC 2004 with FV-USM

the efficiency and real-time applicability of cancelable multibiometric systems. The relatively higher EERs observed in our results may partly stem from the challenging nature of the datasets used (NUPT-FPV, FVC 2004, FV-USM) and the unique challenges posed by our integration approach. Despite the higher EERs, our method demonstrates significant advantages in computational efficiency and system resilience, providing a practical and comprehensive solution for secure biometric authentication. Our method's ability to effectively maintain privacy and ensure system resilience, while addressing limitations such as high computational complexity and real-time performance, underscores its potential as a significant advancement in the field of cancelable biometrics.

Integrating data preprocessing, feature extraction, and classification within a single deep learning architecture significantly enhances computational efficiency and reduces resource requirements. This streamlined approach minimizes the need for separate modules, thereby reducing data transfer overhead and processing latency. By leveraging the GPU's parallel processing capabilities, our model optimizes resource utilization effectively. The combined architecture allows for concurrent execution of multiple tasks, thereby decreasing the overall processing time. Traditional multi-stage approaches often require separate preprocessing and feature extraction phases, each demanding its own computational resources. In contrast, our integrated method performs these tasks within the neural network, leading to a more efficient use of memory and processing power. This efficiency is particularly beneficial for large-scale biometric datasets, where processing speed and resource management are crucial.

The significant impact of our strategy indicates its potential to establish novel benchmarks for ensuring secure user

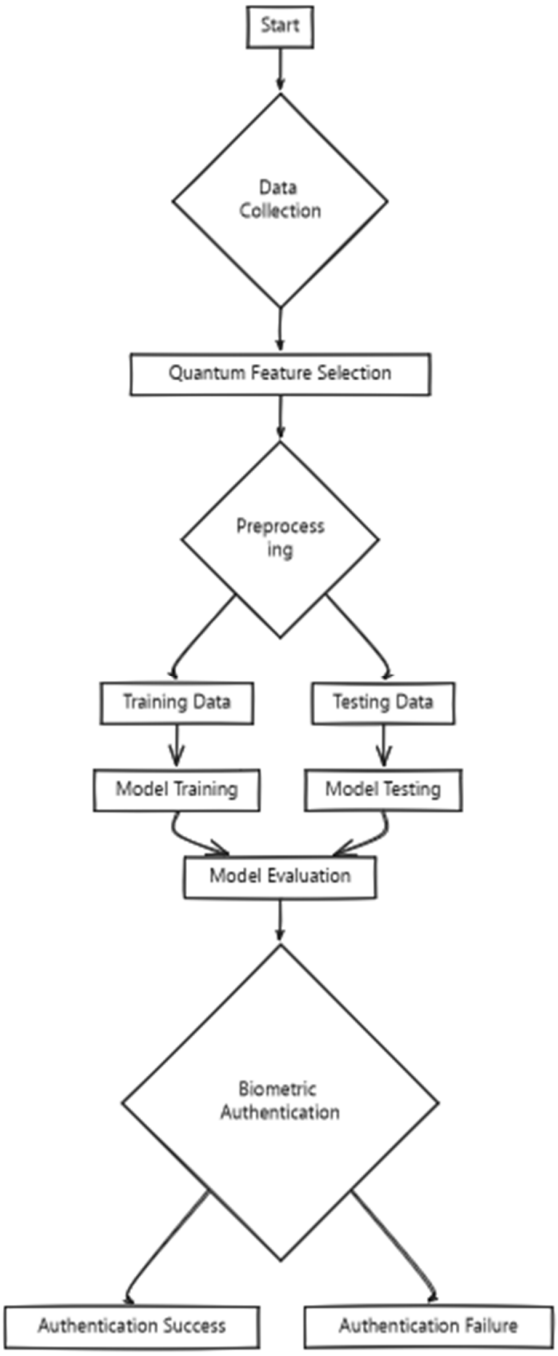


FIGURE 12. Conceptual framework for quantum feature selection in biometric authentication.

authentication and safeguarding data. We highlight the advantages, disadvantages, and novelty of our method as the following:

A. ADVANTAGES

- Utilization of NMF for implementing cancelable biometrics safeguards user privacy.
- Achievement of all cancelable requirements demonstrates remarkable efficacy in upholding security and user privacy.
- Commendable accuracy rates achieved through 5-fold cross-validation indicate potential for reliable biometric authentication.

B. DISADVANTAGES

- Further analysis and optimization are required to enhance computational efficiency and real-time applicability.
- Effectiveness of NMF as a cancelable method may vary based on specific biometric modalities and factorization parameters.

C. NOVELTY

- Integration of NMF with deep learning for cross-modal biometric authentication offers both security and meaningful feature extraction.
- Unparalleled accomplishment of meeting all cancelable criteria sets the proposed method apart as a significant advancement.

VI. FUTURE WORK

In future work, we will focus on extending our method to encompass additional biometric modalities, such as facial recognition and iris recognition, thereby broadening the applicability and versatility of our approach. Enhancing the robustness of our system against sophisticated spoofing attacks will be a key priority to ensure its security and reliability in real-world scenarios. Additionally, we plan to explore the integration of quantum feature selection with our current deep learning-based cancelable multibiometric authentication system. This integration will be approached in the following manner:

1) Quantum Feature Selection Framework:
   - We will employ quantum computing techniques, such as Quantum Annealing and Variational Quantum Circuits, for feature selection. These methods leverage quantum properties such as superposition and entanglement to efficiently explore and identify the most relevant features from the dataset. Figure 12 illustrates the conceptual framework of our quantum feature selection approach.
   - We will develop a hybrid model that integrates classical deep learning with quantum feature selection. This model will harness the strengths of both quantum and classical computations, combining quantum-selected features with deep learning algorithms to enhance performance and efficiency.
2) Implementation Steps:
   - The biometric data will be preprocessed to ensure compatibility with quantum algorithms. This includes normalization and encoding to prepare the data for quantum processing and integration into the deep learning pipeline.
   - Quantum algorithms will be utilized to select the most pertinent features from the biometric data. Techniques like Quantum Annealing will optimize

the selection process, while Variational Quantum Circuits will evaluate feature importance.
- The features selected through quantum methods will be used as input for deep learning models. We will train and evaluate these models with the refined feature set to assess improvements in model accuracy and efficiency.

3) Potential Advantages:
- Quantum algorithms can process a larger subset of features simultaneously, leading to more efficient and effective feature selection.
- By focusing on the most relevant features, the deep learning models can achieve higher accuracy, reduced overfitting, and more reliable biometric authentication results.
- Quantum techniques can accelerate feature selection, reducing the time required for training and inference. This efficiency gain is crucial for real-time biometric systems.

VII. CONCLUSION AND FUTURE DIRECTION

This paper presents a novel cancelable multibiometric method that leverages NMF and a lightweight deep learning model to achieve high privacy, security, and accuracy. The proposed system integrates finger vein and fingerprint authentication modalities to achieve an average validation accuracy of 95.31% for the NUPT-FPV dataset and 92.71% for the combined FVC2004 and FV-USM datasets, which is significantly higher than previous cancelable multibiometric systems. Importantly, the proposed method satisfies all cancelable criteria, representing a significant advancement in the field. This paper not only addresses the limitations of previous research but also introduces a new approach to cancelable multibiometric systems using deep learning techniques. The proposed method aims to achieve higher levels of accuracy and efficiency, and its findings demonstrate its potential for practical implementations in various domains, such as healthcare and financial services, where secure and confidential authentication is essential. The additional experiments highlight the robustness and usability of our cancelable multibiometric authentication system in various real-world conditions. Despite some variations in performance, the system consistently demonstrated high accuracy and reliability. These findings reinforce the practical applicability of our approach in diverse and challenging environments, further validating the system's potential for widespread deployment in biometric authentication systems. With the advancement of technology and the increasing demand for strong authentication, this technique represents a notable step forward in protecting user data while providing a seamless and reliable access control system. Future work will focus on extending our method to other biometric modalities, such as facial recognition and iris recognition, while also enhancing robustness against sophisticated spoofing attacks. We will also explore the use of quantum feature selection with deep learning techniques to further improve the performance and efficiency of the system.

DATA AVAILABILITY

The datasets generated during and/or analyzed during the current study are available at:
https://github.com/REN382333467/NUPT-FPV,
http://bias.csr.unibo.it/fvc2004/download.asp and
http://drfendi.com/fv_usm_database/

ACKNOWLEDGMENT

The authors would like to acknowledge the Princess Nourah Bint Abdulrahman University Researchers Supporting Project number (PNURSP2024R135), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Also, the author would like to thank Prince Sultan University for their support.

REFERENCES

[1] S. A. Abdulrahman and B. Alhayani, "A comprehensive survey on the biometric systems based on physiological and behavioural characteristics," *Mater. Today, Proc.*, vol. 80, pp. 2642–2646, Jan. 2023.
[2] M. Rawat and N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artif. Intell. Rev.*, vol. 53, no. 5, pp. 3403–3446, Jun. 2020.
[3] V. Rajasekar, M. Saračević, D. Karabašević, D. Stanujkić, E. Dobardžić, and S. Krishnamoorthi, "Efficient cancelable template generation based on signcryption and bio hash function," *Axioms*, vol. 11, no. 12, p. 684, Nov. 2022.
[4] A. Elsadai, S. Adamović, M. Šarac, M. Saračević, and S. K. Sharma, "New approach for fingerprint recognition based on stylometric features with blockchain and cancellable biometric aspects," *Multimedia Tools Appl.*, vol. 81, no. 25, pp. 36715–36733, Oct. 2022.
[5] K. Wang, H. Ma, O. P. Popoola, and J. Li, "Finger vein recognition," in *Biometrics*. London, U.K.: IntechOpen, 2011, pp. 31–53.
[6] S. Barzut, M. Milosavljević, S. Adamović, M. Saračević, N. Maček, and M. Gnjatović, "A novel fingerprint biometric cryptosystem based on convolutional neural networks," *Mathematics*, vol. 9, no. 7, p. 730, Mar. 2021.
[7] M. Li, Y. Gong, and Z. Zheng, "Finger vein identification based on large kernel convolution and attention mechanism," *Sensors*, vol. 24, no. 4, p. 1132, Feb. 2024.
[8] E. J. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, vol. 1. New York, NY, USA: Springer, 2016.
[9] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 17, 2008, Art. no. 579416.
[10] G. S. Walia, G. Jain, N. Bansal, and K. Singh, "Adaptive weighted graph approach to generate multimodal cancelable biometric templates," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1945–1958, 2020.
[11] J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. D. J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, and I. Cruz-Vega, "A review on protection and cancelable techniques in biometric systems," *IEEE Access*, vol. 11, pp. 8531–8568, 2023.
[12] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, pp. 1–25, Dec. 2011.
[13] X. Fu, K. Huang, N. D. Sidiropoulos, and W.-K. Ma, "Nonnegative matrix factorization for signal and data analytics: Identifiability, algorithms, and applications," *IEEE Signal Process. Mag.*, vol. 36, no. 2, pp. 59–80, Mar. 2019.
[14] I. Buciu, N. Nikolaidis, and I. Pitas, "Nonnegative matrix factorization in polynomial feature space," *IEEE Trans. Neural Netw.*, vol. 19, no. 6, pp. 1090–1100, Jun. 2008.
[15] Y.-X. Wang and Y.-J. Zhang, "Nonnegative matrix factorization: A comprehensive review," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 6, pp. 1336–1353, Jun. 2013.
[16] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.
[17] Z. Zhao and A. Kumar, "Improving periocular recognition by explicit attention to critical regions in deep neural network," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 12, pp. 2937–2952, Dec. 2018.

[18] H. Vadher, P. Patel, A. Nair, T. Vyas, S. Desai, L. Gohil, S. Tanwar, D. Garg, and A. Singh, "EEG-based biometric authentication system using convolutional neural network for military applications," *Secur. Privacy*, vol. 7, no. 2, Mar. 2024, Art. no. e345.
[19] B. B. Das, S. K. Ram, K. S. Babu, R. K. Mohapatra, and S. P. Mohanty, "Person identification using autoencoder-CNN approach with multitask-based EEG biometric," *Multimedia Tools Appl.*, pp. 1–21, 2024, doi: 10.1007/s11042-024-18693-z.
[20] K. Nguyen, C. Fookes, A. Ross, and S. Sridharan, "Iris recognition with off-the-shelf CNN features: A deep learning perspective," *IEEE Access*, vol. 6, pp. 18848–18855, 2018.
[21] S. B. Abdullahi, Z. A. Bature, P. Chophuk, and A. Muhammad, "Sequence-wise multimodal biometric fingerprint and finger-vein recognition network (STMFPFV-Net)," *Intell. Syst. Appl.*, vol. 19, Sep. 2023, Art. no. 200256.
[22] G.-L. Lv, L. Shen, Y.-D. Yao, H.-X. Wang, and G.-D. Zhao, "Feature-level fusion of finger vein and fingerprint based on a single finger image: The use of incompletely closed near-infrared equipment," *Symmetry*, vol. 12, no. 5, p. 709, May 2020.
[23] J. Yang and X. Zhang, "Feature-level fusion of fingerprint and finger-vein for personal identification," *Pattern Recognit. Lett.*, vol. 33, no. 5, pp. 623–628, Apr. 2012.
[24] I. Kovač and P. Marák, "Openfinger: Towards a combination of discriminative power of fingerprints and finger vein patterns in multimodal biometric system," *Tatra Mountains Math. Publications*, vol. 77, no. 1, pp. 109–138, Dec. 2020.
[25] K. Lin, F. Han, Y. Yang, and Z. Zhang, "Feature level fusion of fingerprint and finger vein biometrics," in *Proc. 2nd Int. Conf. Adv. Swarm Intell.*, Chongqing, China. Berlin, Germany: Springer, 2011, pp. 348–355.
[26] E. M. Cherrat, R. Alaoui, and H. Bouzahir, "Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images," *PeerJ Comput. Sci.*, vol. 6, p. e248, Jan. 2020.
[27] R. Raghavendra, K. B. Raja, J. Surbiryala, and C. Busch, "A low-cost multimodal biometric sensor to capture finger vein and fingerprint," in *Proc. IEEE Int. Joint Conf. Biometrics*, Sep. 2014, pp. 1–7.
[28] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.
[29] N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, vol. 4, 2006, pp. 370–373.
[30] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of privacy in biometric data," *IEEE Access*, vol. 4, pp. 880–892, 2016.
[31] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.
[32] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Berlin, Germany: Springer, Jul. 2005, pp. 242–252.
[33] C. Lee, J.-Y. Choi, K.-A. Toh, and S. Lee, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Trans. Syst., Man Cybern. B, Cybern.*, vol. 37, no. 4, pp. 980–992, Aug. 2007.
[34] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 236–246, May 2010.
[35] S. Crisan, "A novel perspective on hand vein patterns for biometric recognition: Problems, challenges, and implementations," in *Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era*. Springer, 2017, pp. 21–49.
[36] Z. Tao, H. Wang, Y. Hu, Y. Han, S. Lin, and Y. Liu, "DGLFV: Deep generalized label algorithm for finger-vein recognition," *IEEE Access*, vol. 9, pp. 78594–78606, 2021.
[37] Z. H. Goh, Y. Wang, L. Leng, S.-N. Liang, Z. Jin, Y.-L. Lai, and X. Wang, "A framework for multimodal biometric authentication systems with template protection," *IEEE Access*, vol. 10, pp. 96388–96402, 2022.
[38] E. M. Cherrat, R. Alaoui, and H. Bouzahir, "A multimodal biometric identification system based on cascade advanced of fingerprint, fingervein and face images," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 17, no. 3, p. 1562, Mar. 2020.
[39] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018.
[40] H. Ren, L. Sun, J. Guo, and C. Han, "A dataset and benchmark for multimodal biometric recognition based on fingerprint and finger vein," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 2030–2043, 2022.
[41] (2004). *FVC2004*. Accessed: Nov. 3, 2023. [Online]. Available: http://bias.csr.unibo.it/fvc2004/download.asp
[42] M. S. M. Asaari, S. A. Suandi, and B. A. Rosdi, "Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics," *Expert Syst. Appl.*, vol. 41, no. 7, pp. 3367–3382, Jun. 2014, doi: 10.1016/j.eswa.2013.11.033.
[43] Y. Li and A. Ngom, "The non-negative matrix factorization toolbox for biological data mining," *Source Code Biol. Med.*, vol. 8, no. 1, pp. 1–15, Dec. 2013.
[44] A. Pascual-Montano, P. Carmona-Saez, M. Chagoyen, F. Tirado, J. M. Carazo, and R. D. Pascual-Marqui, "BioNMF: A versatile tool for non-negative matrix factorization in biology," *BMC Bioinf.*, vol. 7, no. 1, pp. 1–9, Dec. 2006.
[45] J. M. Zurada, T. Ensari, E. H. Asl, and J. Chorowski, "Nonnegative matrix factorization and its application to pattern analysis and text mining," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2013, pp. 11–16.
[46] Z.-Y. Zhang, "Nonnegative matrix factorization: Models, algorithms and applications," in *Data Mining: Foundations and Intelligent Paradigms: Volume 2: Statistical, Bayesian, Time Series and Other Theoretical Aspects*. Springer, 2012, pp. 99–134.
[47] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Proc. Int. Workshop Selected Areas Cryptogr.* Berlin, Germany: Springer, Aug. 2003, pp. 175–193.
[48] A. C. Ramachandra, K. Pavithra, K. Yashasvini, K. B. Raja, K. R. Venugopal, and L. M. Patnaik, "Cross-validation for graph matching based offline signature verification," in *Proc. Annu. IEEE India Conf.*, vol. 1, Dec. 2008, pp. 17–22.
[49] T. Fushiki, "Estimation of prediction error by using K-fold cross-validation," *Statist. Comput.*, vol. 21, no. 2, pp. 137–146, Apr. 2011.
[50] M. Vanoni, P. Tome, L. El Shafey, and S. Marcel, "Cross-database evaluation using an open finger vein sensor," in *Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl. (BIOMS)*, Oct. 2014, pp. 30–35.
[51] Z. Hao, P. Fang, and H. Yang, "Finger vein recognition based on multi-task learning," in *Proc. 5th Int. Conf. Math. Artif. Intell.*, Apr. 2020, pp. 133–140.
[52] T. Zia, M. Ghafoor, S. A. Tariq, and I. A. Taj, "Robust fingerprint classification with Bayesian convolutional networks," *IET Image Process.*, vol. 13, no. 8, pp. 1280–1288, 2019.
[53] I. Boucherit, M. O. Zmirli, H. Hentabli, and B. A. Rosdi, "Finger vein identification using deeply-fused convolutional neural network," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 3, pp. 646–656, Mar. 2022.
[54] R. Das, E. Piciucco, E. Maiorana, and P. Campisi, "Convolutional neural network for finger-vein-based biometric identification," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 360–373, Feb. 2019.
[55] B. Bakhshi and H. Veisi, "End to end fingerprint verification based on convolutional neural network," in *Proc. 27th Iranian Conf. Electr. Eng. (ICEE)*, Apr. 2019, pp. 1994–1998.
[56] W. Jian, Y. Zhou, and H. Liu, "Lightweight convolutional neural network based on singularity ROI for fingerprint classification," *IEEE Access*, vol. 8, pp. 54554–54563, 2020.
[57] Y. Li et al., "A cancelable multi-biometric system based on the feature-level fusion of fingerprint and finger vein," *Multimedia Tools Appl.*, 2024, doi: 10.1007/s11042-024-20102-4.

MOHAMED HAMMAD received the Ph.D. degree from the School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China, in 2019. He is currently an Assistant Professor with the Faculty of Computers and Information, Menoufia University, Egypt. He is also a Researcher with the EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University. He has published more than 50 articles in international SCI-IF journals. His research interests include biomedical imaging, bioinformatics, cyber security, the IoT, computer vision, machine learning, deep learning, pattern recognition, and biometrics. Furthermore, he served as an Editor Board Member for *PLOS One* and *BMC Bioinformatics*, an Associate Editor for *International Journal of Information Security and Privacy*, a Topics Board Editor for *Forensic Sciences* (MPDI), and the Guest Editor for many international journals, such as *International Journal of Digital Crime and Forensics*, *Sensors* (MDPI), and *Information* (MDPI). He is a reviewer of more than 500 articles for many prestigious journals and listed in the top 2% of scientists worldwide (according to the recently released list by Stanford University, USA, in 2022 and 2023).

MUDASIR AHMAD WANI received the Master of Computer Applications (M.C.A.) and M.Phil. degrees in data mining from the University of Kashmir (UoK), in 2012 and 2014, respectively, and the Ph.D. degree in computer science from Jamia Millia Islamia (A Central University), New Delhi, India, in 2019. He was a Postdoctoral Researcher with the Norwegian Biometrics Laboratory, Norwegian University of Science and Technology (NTNU), Norway. He was a Lecturer and a Researcher with the Department of Information Security and Communication Technology (IIK), NTNU. He is currently a Researcher with NLP, Prince Sultan University, Saudi Arabia. He is actively involved in organizing and reviewing international conferences, workshops, and journals. His research interests include the extraction and analysis of social data and the application of different statistical and machine/deep learning techniques in developing prediction models. He was a recipient of the Alain Bensoussan Fellowship Award under European Research Consortium for Informatics and Mathematics (ERCIM), Sophia Antipolis Cedex, France.

KASHISH ARA SHAKIL received the bachelor's degree in computer science from Delhi University, the M.C.A. degree from Jamia Hamdard, and the Ph.D. degree in computer science from Jamia Millia Islamia, New Delhi. She is currently an Assistant Professor with the College of Computer and Information Sciences, Princess Nourah Bint AbdulRahman University, Saudi Arabia. She has three books entitled as the "*Internet of Things (IoT): Concepts and Applications (S.M.A.R.T. Environments)*," "*Emerging Technologies for Sustainable and Smart Energy—Prospects in Smart Technologies*," and "*Green Automation for Sustainable Environment*" to her credit. Her research interests include cloud computing, big data, machine learning, and NLP. She serves as the Co-Editor-in-Chief for *Journal of Applied Information Science*. She is on the Editorial Board of many reputed international journals in computer sciences and has published several research articles.

HADIL SHAIBA received the B.Sc. degree in information technology from King Saud University, Saudi Arabia, and the M.Sc. and Ph.D. degrees in computer science from Southern Methodist University, USA. She is currently an Associate Professor with the College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Saudi Arabia. Her research interests include AI, data mining, machine learning, and image processing for applications in education, meteorology, and medicine.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the B.Sc. degree (Hons.) in mathematics and computer science and the M.Sc. degree in computer science from Menoufia University, Egypt, in 2005 and 2010, respectively, and the Ph.D. degree in computer science and technology from Harbin Institute of Technology (HIT), Harbin, China, in 2013. He is currently an Associate Professor of computer science with Menoufia University and the EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia. He is involved in government and internationally funded research and development projects related to the widespread use of artificial intelligence for 5G/6G networks. He had many books, more than ten books, in several publishers Springer, IET, CRC Press, IGI-Global, Wiley, and IEEE. He is the author or co-author of more than 240 articles, including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. His research interests include multimedia content encryption, 5G/6G wireless communications, the IoT, cryptography, information hiding, biometrics, image processing, and quantum information processing. He is a member of ACM. He is a fellow of the Academy of Scientific Research and Technology, Egypt. He received many awards, such as the State Encouragement Award in Engineering Sciences, Egypt, in 2016; the Best Ph.D. Student Award from Harbin Institute of Technology, China, in 2013; and the Young Scientific Award, Menoufia University, in 2014. He is the chair/co-chair/program chair of some Scopus/EI conferences. He is the Editor-in-Chief of *International Journal of Information Security and Privacy* and the Series Editor of *Advances in Cybersecurity Management* (https://www.routledge.com). He is also an academic editor/associate editor for a set of indexed journals (Scopus journals' quartile ranking).