Appl. Comput. Math., Vol.25, No.2, Special Issue, 2026, pp.349-362
DOI: 10.30546/1683-6154.25.2.2026.349

PRIVACY-PRESERVING BIOMETRIC AUTHENTICATION: FINGERPRINT ENCRYPTION AND SECURE FEATURE EXTRACTION

D. LI[1,*], L. CHEN[1], Y. ZHONG[1], J. LIAN[1]

Abstract. This study proposes a secure fingerprint authentication framework specifically designed for Medical Cyber-Physical Systems (MCPS) environments to enable clinician authentication for medical equipment such as ventilators, infusion pumps, radiology systems, and remote healthcare infrastructures while ensuring secure and accurate user identification. The proposed framework consists of the following key stages: Data preprocessing, feature extraction, privacy-preserving protection using homomorphic encryption and secure multi-party computation, and Secure Hash Algorithm-3 (SHA-3), followed by authentication through a Transformer-based classifier for accurate and efficient fingerprint matching. To further enhance performance, a Hybrid Quantum Swarm Optimization Algorithm (HQSOA) is employed for optimal feature selection and hyperparameter tuning. The system is deployable across device controllers, nurse workstations, hospital edge servers, and cloud telemedicine services, ensuring low-latency, secure communication for repeated clinical workflows. Experimental evaluation on FVC2002, FVC2004, and LivDet 2015 datasets demonstrates superior performance in accuracy, FAR, FRR, and EER, and processing efficiency.

Keywords: Biometric Authentication, Fingerprint Encryption, Homomorphic Encryption, Secure Feature Extraction, Transformer Classifier, Medical Cyber-Physical Systems.

AMS Subject Classification: 62H30, 68T10, 68P25, 94A60.

1. Introduction

For identity verification, biometric authentication has emerged as a reliable and convenient strategy that is extensively used in many industries including finance, healthcare, and digital identity management in MCPS [17]. One of the most common biometric modalities is fingerprint recognition due to its uniqueness and the ease of acquisition [28]. Nonetheless, issues of storage and transfer of raw fingerprint data have posed crucial privacy and security issues [2]. The latest developments in cryptographic methods, feature extraction with deep learning, and optimization algorithms have led to more secure and efficient biometric authentication systems [24]. Homomorphic encryption, secure multi-party computation and deep learning models are privacy-preserving methods that are currently under investigation to protect biometric data in the authentication process [18]. Particularly, in MCPS where medical equipment, clinical information systems, and real-time monitoring platforms are interconnected in a highly integrated setting, secure and fast authentication is required to ensure patient safety, data integrity, and uninterrupted clinical processes.

Conventional fingerprint authentication systems can be compromised by security breaches, identity theft, and unauthorized access due to the fact that they usually store raw or partially processed biometric data [14]. The biometric traits cannot be revoked or changed like passwords,

[1]Key Laboratory of Intelligent Control Technology for Wuling-Mountain Ecological Agriculture in Hunan Province, Huaihua University, Huaihua, Hunan 418000, China
e-mails: c2375yu@163.com, zyf325255925@163.com, sakura0503@yeah.net
[*]Corresponding author e-mail: ldz1033115125@163.com
Manuscript received 17 November 2025.

and therefore more robust protection mechanisms are required. In addition, the conventional approaches to extracting features do not effectively balance accuracy and computational efficiency, thus limiting their application to real-time authentication. Although there are improvements in certain encryption and feature extraction methods, the existing solutions tend to be trade-offs between privacy protection, authentication speed, and accuracy of classification [21]. Therefore, there is an urgent need for an authentication system that is based on biometrics, and at the same time offers a high degree of security in encryption, feature extraction, and classification to safeguard the identity of users.

This research addresses these MCPS challenges by proposing a comprehensive fingerprint authentication framework that integrates advanced cryptographic protections with a hybrid feature extraction approach and an optimized Transformer-based classification model [7]. The main contribution of this research is a privacy-preserving fingerprint authentication framework as follows:

- Integration of Homomorphic Encryption, Secure Multi-Party Computation, and SHA-3 hashing to protect biometric data from unauthorized access.
- Utilization of a hybrid feature extraction strategy combining minutiae points, Gabor filters, Local Binary Patterns (LBP), and CNN-based deep embeddings to improve fingerprint representation.
- Introduction of a novel Hybrid Quantum Swarm Optimization Algorithm (HQSOA), combining Quantum Particle Swarm Optimization (QPSO) and Modified Grey Wolf Optimization (MGWO), for enhanced feature selection and hyperparameter tuning.

The remainder of this paper is organized as follows: Section 2 presents the literature review, Section 3 details the proposed methodology, Section 4 presents the experimental findings, Section 5 provides discussion, and Section 6 concludes the study with future research directions.

2. Literature review

In the past few years, we have seen the development of new advanced privacy-preserving biometric the authentication techniques based on fingerprint encryption and secure feature generation. The authors reviewed homomorphic encryption applications in biometric systems and showed the potential of using homomorphic encryption to perform computations on encrypted biometric data without decryption, which can increase data confidentiality during authentication processes [29].

The authors presented a biometric image encryption and digital signature method based on Arnold transformation and ElGamal encryption [20]. It provides encryption and authentication to the biometric images and thus increases the security of the data by ensuring its integrity and confidentiality.

In 2024, the authors proposed an innovative approach to fingerprint authentication in the realm of visual cryptography [1]. The visual cryptography scheme used in our method allows the fingerprint images to be encrypted into multiple shares without graying effects, such that the original fingerprint can only be reconstructed when all shares are combined, and hence data confidentiality is maintained. Their algorithm successfully achieves a peak signal-to-noise ratio of 100% and a mean squared error (MSE) of zero, indicating lossless, reconstructing precisely and losslessly.

The homomorphic encryption for multimodal biometric systems is explored to improve security. The authors combined iris and face feature vectors, and secured the fusion of databases and the matching of encrypted templates using fully homomorphic encryption [25]. This method achieves a 100% true acceptance rate (TAR) at a 0.1% false acceptance rate (FAR) in a faceiris fusion setting.

Furthermore, research on palmprint recognition has also been conducted. 2023, a framework for palmprint recognition based on homomorphic encryption is proposed [11]. In this approach,

the authors encrypt the recognition network layer by layer, obtaining both image and network keys, thus effectively reducing the risk of exposing plaintext images and model parameters and mitigating attacks on data and models.

In response to the privacy-preserving biometric authentication challenges, the authors proposed new constructions that use a helper server under strong threat models [5]. In particular, they generalize standard secure multi-party computation security definitions to a multi-phase setting and show that their solutions achieve practical performance for real-time authentication. The authors compared homomorphic encryption algorithms used in biometric systems [6]. The performance and security of different algorithms are evaluated in their study, providing insights into their suitability for biometric applications. In [9], Blind-Touch is an authentication system based on fingerprints that the authors proposed to conduct privacy-preserving neural network inference with the help of homomorphic encryption. Their technique uses the first fully connected plaintext layers on the client and subsequent layers on encrypted data at the server achieving good accuracy while maintaining data privacy.

3. Method

Fig.1 presents the overview of the proposed approach. The architecture combines fingerprint recognition, encryption, deep learning, and optimization techniques to enhance both security and authentication accuracy.

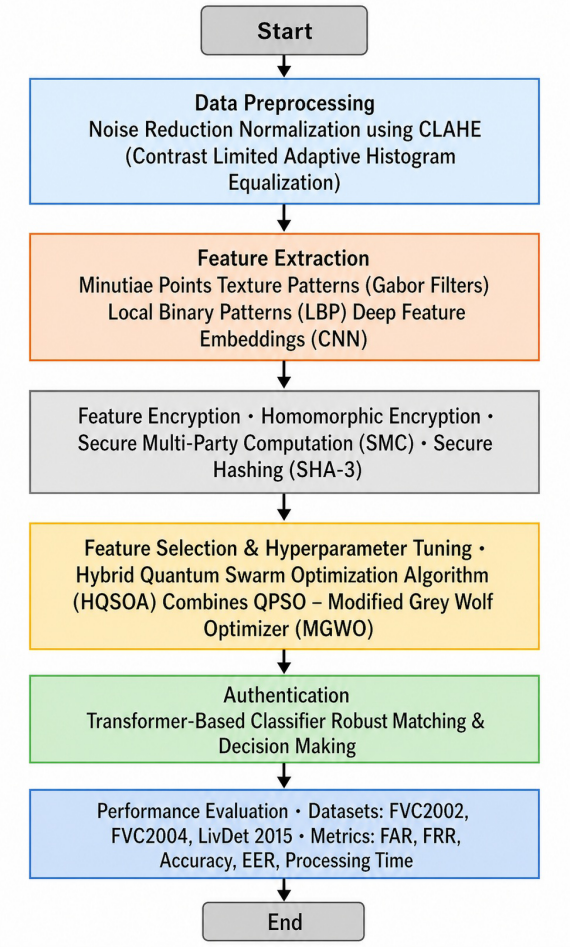


Figure 1. Overview of the proposed approach.

It consists of a sequential framework involving: (i) Data Preprocessing, including noise reduction and Contrast Limited Adaptive Histogram Equalization (CLAHE); (ii) Feature Extraction through minutiae points, Gabor filters, Local Binary Patterns (LBP), and Convolutional Neural Network (CNN) embeddings; (iii) Feature Encryption using Homomorphic Encryption, Secure Multi-Party Computation (SMPC), and Secure Hash Algorithm-3 (SHA-3); and (iv) Authentication through a Transformer-based classifier for secure fingerprint matching. The Hybrid Quantum Swarm Optimization Algorithm (HQSOA), which integrates Quantum Particle Swarm Optimization (QPSO) for global search and Modified Grey Wolf Optimization (MGWO) for rapid convergence, is utilized for feature selection and hyperparameter optimization. This integrated framework ensures robust privacy preservation, superior authentication accuracy, and efficient computational performance, making it highly suitable for secure biometric applications. Transformer models effectively perform fingerprint matching by learning long-range spatial dependencies through self-attention mechanisms, thereby enhancing robustness against noise, rotational distortions, and partial fingerprint impressions. The proposed privacy-preserving fingerprint authentication system is integrated into MCPS to provide rapid, low-latency, and secure identity verification for clinicians accessing critical medical infrastructures such as ICU devices, medication administration systems, radiology platforms, Electronic Health Records (EHRs), and telemedicine services. This integration ensures authorized access, minimizes impersonation risks, and significantly improves patient safety through encrypted biometric verification and efficient Transformer-based authentication.

3.1. **Dataset Description.** The proposed framework is evaluated on three publicly available fingerprint datasets, FVC2002, FVC2004, and LivDet 2015, with different fingerprint samples, having different qualities, distortions, and spoofing attempts. The images in FVC2002 and FVC2004, the images of the Fingerprint Verification Competitions, are composed of images captured by various sensors and synthetic generators, and have four subsets (DB1-DB4) of 800 images, with more severe distortions in FVC2004. LivDet 2015, which includes real and spoofed fingerprints made of gelatin and latex, to detect fingerprint liveness to achieve resistance to presentation attacks. These datasets can be thoroughly trained, validated and tested on the proposed framework, and this enables reproducibility and the evaluation of the reliability of the proposed framework based on standard biometric authentication metrics. (Dataset link: FVC2002 [9], FVC2004 [10], LivDet 2015 [15].)

3.2. **Data Preprocessing.** The preprocessing stage enhances the quality of the fingerprint images by eliminating noise and normalizing the size of the print. Gaussian and median filtering eliminate noise and maintains ridge information. Adaptive Histogram Equalization (CLAHE) with a clip limit of 2.0 and a grid size of 8×8 is applied to boost contrast without excessively boosting noise, making features clearer and easier to identify.

3.3. **Feature Extraction.** The fingerprint image is then passed to the feature extraction stage to generate unique fingerprint patterns, in order to ensure high authentication reliability. Fingerprint minutiae detection identifies ridge endings and bifurcations, and are essential for the uniqueness of the fingerprint. Gabor filters are employed to obtain texture based features that encode the directional ridges and local texture variations are encoded by LBP in order to be insensitive to illumination changes. Deep Feature Embeddings are also obtained using a CNN to process the fingerprint image to a feature vector that encapsulates the fingerprint images essential characteristics. The features are extracted and input into classification or verification models and can be used for precise fingerprint matching with a stored database. This multi-level feature extraction ensures that a comprehensive representation of the fingerprint is obtained is one such use of this feature extraction to allow a higher level of recognition accuracy and security as shown in Fig.1. The LBP operator works by comparing each pixel in a grayscale image (referred to as the central pixel) to its surrounding P neighbors on a circular radius R. Each neighbor is given a binary value: 1 if the intensity of the neighbor is greater than or equal to

the intensity of the central pixel and 0 otherwise. These binary values are then concatenated to form a P-bit binary code which is then translated into a decimal value which is the texture at that pixel position.

3.4. **Gabor Filters: Extraction of Directional Texture Features.** Fingerprint feature extraction relies on Gabor filters, which can capture spatial frequency, orientation and texture. They are selective for specific orientations and frequencies and making them effective for detecting ridge patterns in fingerprint analysis. A Gabor filter is a plane wave that is envelope-modulated by a Gaussian to achieve frequency selectivity and spatial localization. A 2D Gabor filter is given by the general form:

$$G(x, y; \lambda, \theta, \psi, \sigma, \gamma) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right) \cos\left(2\pi \frac{x'}{\lambda} + \psi\right). \tag{1}$$

In Eqn. (1), λ represents the wavelength of the sinusoidal component, controlling the scale of texture features. θ is the orientation of the filter, defining the direction of feature extraction. ψ is the phase offset, determining the shift of the sinusoidal wave. σ is the standard deviation of the Gaussian envelope, affecting spatial frequency bandwidth. γ is the spatial aspect ratio, influencing the elongation of the filter. x' and y' are the rotated coordinates, given in Equation (2):

$$x' = x\cos\theta + y\sin\theta, \quad y' = -x\sin\theta + y\cos\theta. \tag{2}$$

These transformed coordinates ensure that the filter responds to features aligned with the selected orientation θ. In fingerprint processing, a bank of Gabor filters with multiple orientations (e.g., $0B^\circ, 30B^\circ, 60B^\circ, 90B^\circ$) is applied to extract ridge details in different directions. The fingerprint image $I(x, y)$ is convolved with the Gabor filter $G(x, y)$ to obtain the filtered response as Eqn. (3):

$$R(x, y) = I(x, y) * G(x, y), \tag{3}$$

where * represents the convolution operation. It passes through these filtering processes to enhance ridge patterns and suppress noise and background variations so that captured features would be more robust in fingerprint matching. Multiple Gabor filters are applied at different orientations and frequencies to generate a representative of the texture, which is a critical component for a fingerprint authentication scheme which can be trusted and performed reliably.

3.5. **Local Binary Patterns (LBP): Encoding Local Texture Variations.** The LBP (given in [26]) is one of the most popular feature extraction techniques used in fingerprint authentication for texture analysis. Local texture variations are described by LBP, which compares neighboring pixels to a central pixel to encode structural patterns with high computational efficiency. The standard LBP operator has 3×3 neighborhoods, thresholding each surrounding pixel against the central pixel and converting the result into a binary number. The LBP value at (x, y) is computed mathematically as Eqn. (4):

$$LBP_P^R(x, y) = \sum_{p=0}^{P-1} s(I_p - I_c) \cdot 2^p, \tag{4}$$

where P is the number of neighbors (typically 8 for a 3×3 window), R is the radius of the circular neighborhood, I_c is the intensity of the central pixel, I_p is the intensity of the p-th neighboring pixel, $s(\cdot)$ is the thresholding function defined as Eqn. (5):

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}. \tag{5}$$

This results in an 8-bit binary number for each pixel, which is then converted into a decimal value to form the LBP-coded image. By analyzing these encoded values, fingerprint ridge and

texture patterns are effectively captured. The extracted LBP features are then used to construct a histogram representation, given by Eqn. (6):

$$H(k) = \sum_{x,y} \delta(LBP_P^R(x,y) - k), \tag{6}$$

where $H(k)$ is the frequency of occurrence of pattern k, and $\delta(x)$ is the Kronecker delta function, which returns 1 if $x = 0$ and 0 otherwise.

3.6. **Deep Feature Embeddings: CNN for Deep Feature Representation.** This is achieved by using powerful extraction of high-dimensional features and hierarchical fingerprint features from CNNs, which are powerful deep learning models. While minutiae points and LBP are handcrafted features, CNNs learn spatial and structural patterns from raw fingerprint images through multiple layers of convolution, activation, pooling, and fully connected operations.

3.7. **CNN Architecture for Fingerprint Feature Extraction.** A CNN processes and architecture is presented in Fig.2 [13, 27].

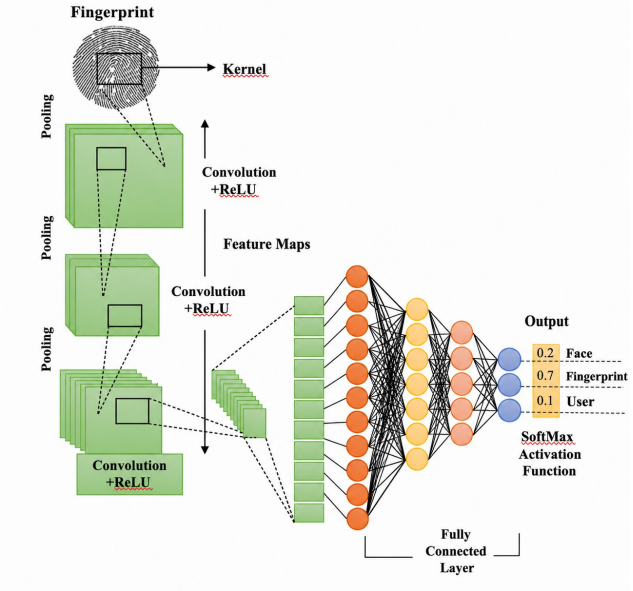


FIGURE 2. Architecture of CNNs.

Convolutional Layer: Extracts local spatial features by applying a set of trainable filters W_k, producing feature maps as Eqn. (7):

$$F_k(x,y) = \sum_{i,j} I(x-i, y-j) W_k(i,j) + b_k, \tag{7}$$

where W_k represents the convolution kernel, b_k is the bias term, and (i,j) denotes the kernel size. This operation enhances ridge structures and unique fingerprint patterns.

Activation Function: Introduces non-linearity using ReLU (Rectified Linear Unit) as Eqn. (8):

$$f(x) = \max(0, x), \tag{8}$$

ensuring that negative values are suppressed while preserving meaningful patterns.

Pooling Layer: Reduces spatial dimensions while retaining essential features through max-pooling as presented in Eqn. (9):

$$P_k(x,y) = \max_{(i,j)\in R} F_k(x+i, y+j), \tag{9}$$

where R is the pooling window. This step enhances computational efficiency and makes the model robust to minor shifts and distortions.

Fully Connected Layer: Converts extracted features into a compact deep feature vector z, representing the fingerprints unique characteristics as shown in Eqn. (10):

$$Z = W \cdot h + b, \tag{10}$$

where h is the flattened pooled feature map, W is the weight matrix, and b is the bias term.

Output Layer: The deep feature vector is used for classification or matching against stored fingerprint templates using distance metrics or classifiers such as the Transformer-based model.

3.8. **Authentication Model: Transformer-Based Classifier, Architecture and Implementation Details.** The authentication phase employs a Transformer-based classifier based on self-attention techniques to capture complex relationship between fingerprint features. The deep feature vector z is extracted using a CNN and optionally combined with texture-based features (Gabor filters, LBP), and is fed as input to the Transformer model. There are multiple self-attention layers, feed-forward networks and normalization layers that enhance feature representation and improve matching accuracy of the Transformar model [12]. The following equations are used to compute relationships between feature dimensions using the self-attention mechanism:

Key, Query, and Value Matrices: Key, query, and value matrices are mathematically represented in Eqn. (11).

$$Q = zW_Q \quad K = zW_K \quad V = zW_V, \tag{11}$$

where W_Q, W_K, W_V are learnable weight matrices that project the feature vector into different subspaces.

Scaled Dot-Product Attention: Attention based last layer of the network is mathematically represented as Eqn. (12).

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V, \tag{12}$$

where d_k is the dimension of the key vectors. This operation assigns importance to different feature elements, allowing the model to focus on key distinguishing characteristics.

Multi-Head Attention: Multiple self-attention heads process fingerprint features in parallel, ensuring robust feature representation as Eqn. (13):

$$MultiHead(Q, K, V) = Concat(head_1, \ldots, head_h)W_O, \tag{13}$$

where each attention head learns distinct feature dependencies, and W_O is an output projection matrix.

The output is passed through a feedforward network, followed by layer normalization, and then mapped to a matching decision (genuine or imposter) using a fully connected layer.

3.9. **Hybrid Quantum Swarm Optimization Algorithm (HQSOA).** The HQSOA is a new type of optimization algorithm by integrating QPSO and MGWO to achieve feature selection and hyperparameter tuning for fingerprint authentication. By combining the good global search capability of QPSO and the efficient local convergence of MGWO, HQSOA can achieve optimal feature selection and meanwhile improve the classification performance.

3.10. **Quantum Particle Swarm Optimization (QPSO): Global Search and Feature Selection.** The Quantum PSO is an improved version of QPSO, which is based on quantum mechanics principles [19] . It brings an additional global search capability by allowing particles to have probabilistic movements in a quantum potential well instead of fixed velocity updates. The Eqn. (14) is used to update each particles position:

$$x_i^{(t+1)} = P_i + \beta|M - M_{x_i}^{(t)}| \cdot \ln(1/u), \tag{14}$$

where $x_i^{(t+1)}$ is the updated position of the particle, P_i is the local attractor, defined as the average of the personal best and global best positions, M is the mean best position of all particles, β is a control parameter governing exploration, u is a random number drawn from a uniform distribution $(0, 1)$.

QPSO efficiently explores a high-dimensional search space for selecting optimal fingerprint features, reducing redundancy while retaining essential discriminative information.

3.11. **Modified Grey Wolf Optimizer (MGWO): Convergence Improvement and Fine-Tuning.** The GWO is a metaheuristic based on the hunting behavior of grey wolves [16]. An adaptive dynamic control parameter is introduced into standard GWO to enhance the local search efficiency and convergence speed, which is called MGWO. Wolves (solution candidates) update their positions with respect to the best solutions (α, β, δ) in MGWO using Eqn. (15):

$$X_i^{(t+1)} = X_\alpha - A \cdot |C \cdot X_\alpha - X_i|, \tag{15}$$

where X_α, X_β, and X_δ are the top three best solutions, A and C are adaptive coefficient vectors, controlling exploration and exploitation, X_i is the position of the current solution at iteration t.

MGWO fine-tunes the selected fingerprint features and optimizes the hyperparameters of the Transformer-based classifier to enhance matching performance.

The optimization framework employs QPSO for feature selection and MGWO for hyperparameter tuning of the Transformer classifier. QPSO, with quantum-inspired position updates, effectively balances exploration and exploitation to select discriminative features. It uses a population size of 30, 50 iterations, and $\beta = 1.0$. MGWO enhances convergence by modifying GWO's leadership hierarchy and hunting strategy. It optimizes parameters such as learning rate, batch size, and attention heads, using a population size of 20, 40 iterations, and a linearly decreasing control coefficient a (from 2 to 0). This hybrid approach improves both accuracy and error rate performance.

3.12. **Evaluation and Performance Metrics.** In order to measure the performance of the proposed model, several performance metrics that are used. Accuracy is the overall correctness of authentication taking into account the correctly classified genuine and imposter attempts. False Acceptance Rate (FAR) is the rate of unauthorized access attempts that are incorrectly accepted which reflects the security of the system, and the False Rejection Rate (FRR) is the rate of incorrect denial of access to legitimate users which affects usability. The Equal Error Rate (EER) is a metric used to provide a balanced evaluation of system reliability, where lower values correspond to better system performance. Processing time is also evaluated to ensure that the feature extraction, encryption, and matching operations can be performed in real time to satisfy the authentication needs.

3.13. **Implementation Details.** The fingerprint authentication framework is executed on an NVIDIA RTX 3090 graphics card, Intel Core i9-13900K processor, 64GB RAM, 2TB NVMe SSD, Ubuntu 22.04 LTS, Python 3.10, and CUDA 12.1 to accelerate computations. OpenCV and scikit-image are used for preprocessing and feature extraction, and depending on whether they are integrated with TensorFlow 2.11 or PyTorch 2.0 models. HQSOA optimization is implemented with the help of DEAP and SciPy, PySEAL is used for homomorphic encryption, and additional security is provided using PyCryptodome (SHA-3) and SMPC respectively. Experiments are done with FVC2002, FVC2004 and LivDet 2015 with a 80-10-10 train-validation-test with robustness ensured through data augmentation. The Transformer classifier has 6 layers, 8 attention heads, 512-dimensional embedding and a 0.1 dropout rate.

3.14. **MCPS Integration.** The system facilitates clinician authentication to access vital medical equipment and devices like ventilators, infusion pumps, and radiology equipment, and to securely access EHRs, telemedicine platforms, and the MCPS control dashboard. The framework provides privacy-preserving authentication by using encrypted fingerprint templates and secure

communication protocols, and low latency suitable for supporting high-frequency and repetitive clinical processes, such as ICU device adjustments and medication administration. This greatly minimizes impersonation threats and unauthorized access within safety critical environments. Additionally, the framework supports positive patient identification through securely connecting biometric data to patient records, thus reducing misidentification errors in wards, ICUs, and emergency departments. The architecture is designed to be deployed on device controllers, nurse workstations, hospital edge servers, and cloud platforms, with scalable and real-time authentication. Additionally, the system is extended to remote healthcare settings, as it allows secure verification of patient biometrics on their smartphones and tablets, in which encrypted templates are processed and using cloud-based mechanisms.

4. Results

4.1. **Performance Evaluation.** To assess the effectiveness of the proposed Transformer-based authentication framework optimized with HQSOA, a fair comparative evaluation was conducted on the FVC2002 dataset, ensuring that all models were trained and tested on the same dataset for consistency. Table 1 summarizes the performance of the proposed method against baseline models: CNN + GA, SVM + PSO, and RF + GWO. The proposed framework achieved the highest accuracy (97.83%) and the lowest error rates (FAR: 1.12%, FRR: 1.35%, EER: 1.24%), demonstrating its superior capability in learning discriminative fingerprint features and handling image distortions through self-attention mechanisms.

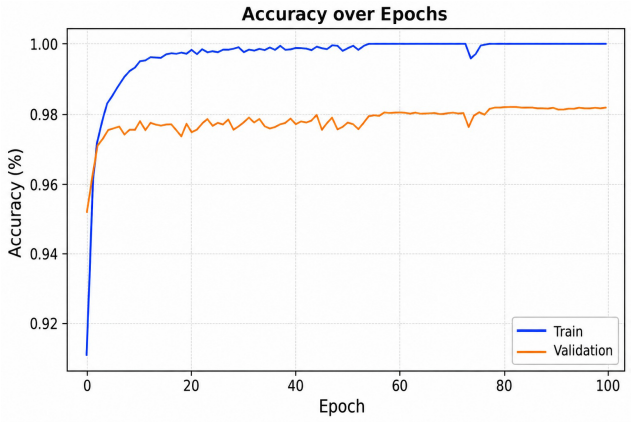


Figure 3. Accuracy over epochs.

The learning performance of a fully connected neural network is shown in Fig.3 shows an accuracy-over-epochs plot. The training accuracy (blue curve) and the validation accuracy (orange curve) keep increasing, both of which show good learning, as well as good generalization. The optimization process of a fully connected neural network is shown in Fig.4 loss over epochs plot.

Table 1. Performance comparison of authentication methods.

Model	Dataset	Accuracy (%)	FAR (%)	FRR (%)	EER (%)	Time (ms)
CNN + GA	FVC2002	94.12	2.75	3.13	2.94	45.3
SVM + PSO	FVC2002	92.30	3.10	3.40	3.25	48.0
Random Forest + GWO	FVC2002	90.85	3.50	3.75	3.60	50.1
Transformer + HQSOA	FVC2002	97.83	1.12	1.35	1.24	39.8

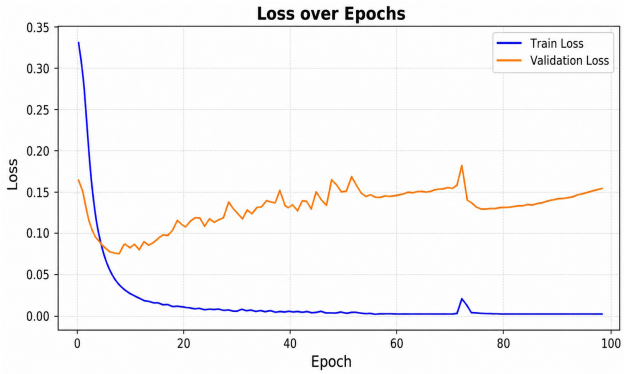


FIGURE 4. Loss over epochs.

4.2. **Feature Extraction and Encryption Effectiveness.** Fingerprint authentication benefits from feature extraction, which is required for both accuracy and speed. In the proposed framework, minutiae-based features, and texture patterns (Gabor filters, LBP and deep feature embeddings from a CNN) are integrated to capture both the local and global fingerprint characteristics. Performance comparison of the above feature extraction techniques is illustrated in Table 2. The highest accuracy (96.75%) was achieved by CNN embeddings as they are capable of extracting hierarchical features, while the widely used minutiae-based extraction was affected by small variations in fingerprint quality, resulting in a slightly higher False Acceptance Rate (FAR).

TABLE 2. Performance of feature extraction techniques.

Feature extraction method	Accuracy (%)	FAR (%)	FRR (%)	Time (ms)
Minutiae	93.21	2.85	3.12	27.5
Gabor filters	92.48	3.12	3.45	29.1
LBP	90.79	3.67	4.12	25.8
CNN embeddings	96.75	1.98	2.31	33.4

It also integrates HE, SMPC, and SHA-3 hashing simultaneously to increase data security without significant impact on authentication time. It provides privacy-preserving computations (HE), secure multi-party computation (SMPC) and integrity verification (SHA-3). However, Table 3 shows the trade-off between security and speed, where HE incurs a computational overhead of 11.4 ms, but SHA-3 hashing is computationally lightweight but does not provide encryption. The hybrid encryption strategy strikes a proper balance between security and efficiency offering good protection without slow performance.

TABLE 3. Impact of encryption methods on authentication speed.

Encryption method	Security level	Authentication overhead (ms)
Homomorphic encryption (HE)	High	+11.4
Secure multi-party computation (SMPC)	High	+9.2
SHA-3 hashing	Medium	+3.7
Proposed hybrid (HE + SMPC + SHA-3)	High	+6.8

4.3. **Impact of HQSOA.** In this way, the Hybrid Quantum Swarm Optimization Algorithm (HQSOA, QPSO and MGWO) bring tremendous improvement in feature selection and classification accuracy. HQSOA has better global search efficiency than traditional optimization algorithms, such as GA, PSO and GWO, and it can maintain convergence stability to select

optimal feature subsets and achieve better classifier performance. In feature selection for fingerprint authentication, Table 4 compares these algorithms. HQSOA achieved the highest accuracy (97.83%) with the least feature selection time (18.7 ms) since its exploration-exploitation balance was enhanced.

TABLE 4. Feature selection performance of different optimization algorithms.

Optimization algorithm	Selected features	Accuracy (%)	Selection time (ms)
GA	74	94.12	31.2
PSO	68	95.43	27.6
GWO	65	96.02	24.8
HQSOA (QPSO + MGWO)	52	97.83	18.7

The idea of QPSO introduces quantum behavior that can overcome the slow exploration of the search space as well as prevent early convergence and improve feature selection. The traditional GWO is modified by dynamically adjusting the hunting strategy to achieve improved convergence and feature subset reduction. These techniques help optimally tune hyperparameters such as the learning rate, batch size and number of attention heads of the Transformer classifier while increasing the long-term classification performance without much additional computational cost. HQSOA's advantage in achieving optimal settings using lower tuning time is as shown in Table 5, which presents hyperparameter tuning efficiency.

TABLE 5. Hyperparameter tuning efficiency of HQSOA versus traditional methods.

Optimization algorithm	Learning rate	Batch size	Tuning time (ms)
GA	0.005	64	42.3
PSO	0.003	48	35.1
GWO	0.0025	32	29.4
HQSOA (QPSO + MGWO)	0.002	24	21.6

4.4. **Authentication Accuracy and Error Rate.** Table 6 shows that the Transformer model achieved the best accuracy (97.83%) because it has a self-attention mechanism that can capture spatial dependencies in fingerprint features. Deep feature extraction performed well in CNN, which was, however, probably less robust in handling variations in fingerprint quality. SVM and RF had lower accuracy as they were not well-suited for high-dimensional feature spaces.

TABLE 6. Accuracy comparison of different classifiers.

Classifier	FVC2002 (%)	FVC2004 (%)	LivDet 2015 (%)	Average (%)
SVM	91.74	89.85	87.61	89.73
Random Forest	92.41	90.32	88.10	90.27
CNN	95.12	93.85	92.17	93.71
Transformer (proposed)	98.12	97.64	97.72	97.83

4.5. **Comparison with Existing Methods.** A comparative evaluation was performed to assess the effectiveness of the proposed framework for fingerprint authentication based on Transformers, against state-of-the-art biometric algorithms such as traditional machine learning models (SVM, RF), deep learning models (CNN, ResNet) and hybrid optimization methods (PSO, GWO, GA). Table 7 shows that the proposed method has the highest accuracy (97.83%) and low error rates (FAR: 1.12%, FRR: 1.35%, EER: 1.24%) compared to existing methods in terms of performance and security. Security and privacy enhancements were also on the cards beyond accuracy. Conventional fingerprint authentication methods store raw biometric data, which are prone to attacks. This paper proposes a framework that uses HE, SMPC and SHA-3 hashing

so that raw fingerprint data is never presented during authentication. In addition, HQSOA enhances the feature selection efficiency, which reduces the authentication time to 39.8 ms, thus making it secure and computationally efficient for real-time applications [4, 8].

TABLE 7. Comparison of proposed method with state-of-the-art techniques.

Method	Optimization	Accuracy (%)	FAR (%)	FRR (%)	EER (%)	Time (ms)	Security level
SVM + PSO	PSO	91.86	3.42	4.10	3.76	50.7	Medium
Random Forest + GWO	GWO	89.74	4.12	4.58	4.35	53.2	Medium
CNN + GA	GA	94.12	2.75	3.13	2.94	45.3	Medium
ResNet + PSO	PSO	95.67	2.21	2.45	2.33	43.6	Medium-high
Transformer + HQSOA	HQSOA	97.83	1.12	1.35	1.24	39.8	High

5. Discussion

To increase the security level of the proposed privacy-preserving biometric authentication framework, we utilize Homomorphic Encryption, Secure Multi-Party Computation, and apply SHA-3 hashing to the fingerprint data to read the input, yet remain protected. With advanced feature extraction to feature minutiae points, Gabor filters, LBP and CNN deep embeddings, fingerprint recognition as well as resilience against noise have been significantly increased. Also, the use of a transformer-based classifier optimized with the HQSOA implies that robust feature selection and good overfitting prevention have been ensured while improving the adaptability to different fingerprint databases [22, 23].

However, the study's reliance on public databases may restrict its applicability to real-world fingerprint differences at other sensor types as well as fake attempts. However, the framework proves to be quite accurate, but more varied datasets need to be tested in order to further boost its robustness.

6. Conclusion

This study presents a privacy-preserving biometric authentication framework tailored for secure deployment within MCPS. The proposed approach integrates advanced encryption techniques, hybrid deep learning-based feature extraction, and a Transformer-based classifier optimized using HQSOA to ensure reliable and efficient identity verification. By combining HE, SMPC, and SHA-3 hashing, the framework provides strong protection for fingerprint templates during storage and transmission. The fusion of handcrafted features with deep CNN embeddings enhances authentication performance, achieving superior accuracy and reduced error rates on benchmark datasets such as FVC2002, FVC2004, and LivDet 2015. The low-latency authentication mechanism supports rapid and repeated access in the ICU, medication administration, and radiology settings, while significantly reducing impersonation risks and unauthorized access. Additionally, the framework facilitates positive patient identification, thereby minimizing misidentification errors and enhancing patient safety. Its scalable architecture supports deployment across device controllers, nurse workstations, hospital edge servers, and cloud-based systems, ensuring seamless integration within modern healthcare infrastructures.

Future work will focus on extending the framework to multi-modal biometric authentication for improved robustness, developing lightweight encryption strategies for resource-constrained medical devices, and incorporating adaptive and explainable learning models to address evolving security threats in dynamic MCPS environments.

7. Acknowledgments

This work has been supported by the Hunan Provincial Natural Science Foundation (2025JJ70482) and the Excellent Youth Project of Hunan Provincial Department of Education (24B0721).

References

[1] Annappanavar, S.M, Chavan, P.V. Enabling secure authentication using fingerprint and visual cryptography, *Int. J. Biom.*, Vol.16, No.6, 2024, pp.614-639.

[2] Ametefe, D.S., Suzi S.S., Darmawaty M.A., Wan, N.W. et al. Enhancing fingerprint authentication: A systematic review of liveness detection methods against presentation attacks, *J. Inst. Eng., (India): Series B,* Vol.105, No.5, 2024, pp.1451-1467.

[3] Baghel, V.S., Surya, P. Generation of secure fingerprint template using DFT for consumer electronics devices, *IEEE Trans. Consum. Electron.*, Vol.69, No.2, 2022, pp.118-127.

[4] Barzut, S., Milosavljevic, M., Adamovic, S., Saračević, M. et al. A novel fingerprint biometric cryptosystem based on convolutional neural networks, *Mathematics*, Vol.9, No.7, 2021, Article No.730.

[5] Blanton, M., Murphy, D. Privacy Preserving Biometric Authentication for Fingerprints and Beyond, Cryptology ePrint Archive, Paper 2024/525.

[6] Crihan, G., Craciun, M., Dumitriu, L. A comparative assessment of homomorphic encryption algorithms applied to biometric information, *Inventions,* Vol.8, No.4, 2023, p.102.

[7] Datta S., Namasudra, S. Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing, *IEEE Trans. Consum. Electron.,* Vol.70, No.1, 2024, pp.4026-4036.

[8] Elsadai, A., Adamoviç, S., Earac, M., Saračević, M., Kumar Sharma, S. New approach for fingerprint recognition based on stylometric features with blockchain and cancellable biometric aspects, *Multimed. Tools Appl.* Vol.81, No.25, 2022, pp.36715-36733.

[9] FVC2002: Fingerprint Verification Competition 2002. [Online]. Available: https://bias.csr.unibo.it/fvc2002/download.asp

[10] FVC2004: Fingerprint Verification Competition 2004. [Online]. Available: https://bias.csr.unibo.it/fvc2004/download.asp

[11] Guo, Q., Shao, H., Liu, Ch., Wan, J., Zhong, D. Homomorphic encryption-based privacy protection for palmprint recognition, In *Biometric Recognition: 17th Chin. Conf.*, Lecture Notes in Computer Science, Springer, Singapore, Vol.14463, 2023, pp.363-371.

[12] Hu, M.M., Zhang, K., You, R.B., Tu, B. AuthConFormer: Sensor-based continuous authentication of smartphone users using a convolutional transformer, *Comput. Secur.,* Vol.127, No.6, 2023, Article No.103122.

[13] Kattenborn, T., Leitloff, J., Schiefer, F., Hinz, S. Review on Convolutional Neural Networks (CNN) in vegetation remote sensing, *ISPRS J. Photogramm. Remote Sens.,* Vol.173, 2021, pp.24-49.

[14] Kumar, T., Bhushan, S., Sharma, P., Garg, V. Examining the vulnerabilities of biometric systems: Privacy and security perspectives, *In: Leveraging Computer Vision to Biometric Applications,* Chapman and Hall/CRC, 2024, pp.34-67.

[15] LivDet 2015: Liveness Detection Fingerprint Dataset. [Online]. Available: https://service.tib.eu/ldmservice/dataset/livdet-2015.

[16] Mirjalili, S., Mirjalili, S.M., Lewis, A. Grey wolf optimizer, *Adv. Eng. Softw.,* Vol.69, 2014, pp.46-61.

[17] Parate, S., Josyula, H.P., Reddi, L.Th. Digital identity verification: Transforming KYC processes in banking through advanced technology and enhanced security measures, *Int. Res. J. Mod. Eng. Technol. Sci.,* Vol.5, No.9, 2023, pp.128-137.

[18] Prakasha, K.K., Sumalatha, U. Privacy-preserving techniques in biometric systems: Approaches and challenges, *IEEE Access*, Vol.13, 2025, pp.32584-32616.

[19] Qing, W., Ma, Z., Fan, J., Xu, G., Shen, Y. A feature selection method based on hybrid improved binary quantum particle swarm optimization, *IEEE Access,* Vol.7, 2019, pp.80588-80601.

[20] Qin, Y., Zhang, B. Privacy-preserving biometrics image encryption and digital signature technique using arnold and ElGamal, *Appl. Sci.,* Vol.13, No.14, 2023, Article No.8117.

[21] Ramakrishna, D., Shaik, M.A. A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges, *IEEE Access,* Vol.13, 2024, pp.11576-11593.

[22] Rajasekar, V., Predič, B., Saračević, M., Elhoseny, M., et al. Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm, *Sci. Rep.* Vol.12, No.1, 2022, Article No.622.

[23] Rajasekar, V., Saračević, M., Hassaballah, M., Karabasevic, D., et al. Efficient multimodal biometric recognition for secure authentication based on deep learning approach, *Int. J. Artif. Intell. Tools,* Vol.32, No.3, 2023, Article No.2340017.

[24] Sasikumar, K., Nagarajan, S. Enhancing cloud security: A multi-factor authentication and adaptive cryptography approach using machine learning techniques, *IEEE Open J. Comput. Soc.* Vol.6, 2025, pp.392-402.
[25] Singh, S., Igene, L., Schuckers, S. Securing biometric data: Fully homomorphic encryption in multimodal iris and face recognition, arXiv preprint arXiv:2408.14609, 2024.
[26] Song, T.C., Feng, J., Luo, L., Gao, C.Q., Li, H.l. Robust texture description using local grouped order pattern and non-local binary pattern, *IEEE Trans. Circuits Syst. Video Technol.* Vol.31, No.1, 2020, pp.189-202.
[27] Takahashi, A., Koda, y., Ito, K., Aoki, T. Fingerprint feature extraction by combining texture, minutiae, and frequency spectrum using multi-task CNN, In 2020 *IEEE Int. Jt. Conf. Biom. (IJCB),* Houston, TX, USA, IEEE, 2020, pp.1-8.
[28] Wu, C.K., Cheng, C.T., Uwate, Y., Chen, G.R., et al. State-of-the-art and research opportunities for next-generation consumer electronics, *IEEE Trans. Consum. Electron.,* Vol.69, No.4, 2023, pp.937-948.
[29] Yang, W.C., Wang, S., Cui, H., Tang, Zh.H., Li, Y. A review of homomorphic encryption for privacy-preserving biometrics, *Sensors,* Vol.23, No.7, 2023, Article No.3566.



Dezi Li - is a key teacher at Huaihua University. He received his Ph.D. degree in Engineering from Fujian Normal University in 2022. He is a member of the Youth Working Committee of the Optical Society of Hunan Province. His research interests include the polarization-sensitive optical coherence tomography technology, fingerprint identification, and optical encryption systems.



Leyu Chen - obtained his bachelor's degree in Optoelectronic Information Science and Engineering from Huaihua University from 2026. His research interests include the intelligent visual neural networks.



Yufan Zhong - obtained his bachelor's degree in Optoelectronic Information Science and Engineering from Huaihua University in 2026. She research interests include the intelligent optical detection, energy-saving applications, intelligent tracking systems, and optoelectronic sensing for modern agriculture.



Jian Lian - obtained his bachelor's degree in Optoelectronic Information Science and Engineering from Huaihua University in 2022. His research interests include physical optics, classical mechanics, quantum mechanics, celestial mechanics, electromagnetism, and thermodynamics.