International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FINGER VEIN-BASED BIOMETRIC KEY GENERATION WITH POST-QUANTUM ENCRYPTION AND OPTIMIZED MAGNETIZED HOPFIELD GLOBAL NEURAL NETWORK

[1]Arun Raj S. R, [2]Dr. G. Ramana Murthy, [3]Dr Shilpa P, [4]Naduvathezhath Nessariose Jose, [5]Shameem Ansar A, [6]P. Venkateswarlu Reddy

[1]Research Scholar
Electronics and Communication Engineering
Alliance College of Engineering and Design, Alliance University, Bengaluru
arunrajsr5@gmail.com

[2]Professor
Electronics and Communication Engineering
Alliance College of Engineering and Design, Alliance University, Bengaluru
ramana.murthy@alliance.edu.in

[3]Assistant Professor
Mathematics
Dayananda Sagar Academy of Technology and Management, Bangalore-560 082
shilpap80@gmail.com

[4]Senior IT Consultant/Architect
Regent Strategic Solutions
india
josenaduvan@gmail.com

[5]Assistant Professor
Computer Science and Engineering
TKM College Of Engineering
shameemansar@gmail.com

[6]Assistant Professor
Computer Science and Engineering
Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College (Autonomous))
venkateswarlucse@gmail.com

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Abstract

Biometric authentication, especially using finger vein patterns, offers a reliable and non-invasive method for secure identity verification. However, current systems face limitations in robustness, scalability, and post-quantum resilience. Existing methods often struggle with noisy biometric inputs, key instability, and vulnerability to quantum attacks. This motivates the development of a lightweight, secure, and stable key generation system. This paper introduces a new biometric key generation framework based on the combination of several state-of-the-art techniques. It starts with Adaptive and Propagated Mesh Filtering (APMF) for improved preprocessing, followed by Spike-Driven Transformer (SDT) for spatiotemporal feature extraction. Min–Max Normalization (M2N) normalizes feature vectors, which are then mapped to binary strings for robust key representation. A fuzzy extractor produces helper data, and Dynamic Lightweight Symmetric Encryption (DLSE) provides post-quantum secure binding. Authentication and key recovery are carried out through a Magnetized Hopfield Global Neural Network (MHGNN), the weight parameters of which are optimized by the White Shark Optimizer (WSO). The model attains 99.7% accuracy with an Equal Error Rate of 0.08, which is higher compared to traditional methods with regard to accuracy and security. This paradigm provides secure authentication with minimal computational expense, and future extensions will be explored to extend it to multimodal biometrics and real-time deployment on edge devices.

Keywords— Adaptive and Propagated Mesh Filtering, Dynamic Lightweight Symmetric Encryption, Min–Max Normalization, Spike-Driven Transformer, White Shark Optimizer.

I. INTRODUCTION

Advantages of biometric authentication, such as portability, simple usage as well and having no memory requirements, are some of the reasons that it has become a competitive identity identification technology within the past few years [1]. An advanced one is the fingerprint identification system, which involves storing the user's fingerprint template to use in comparing and authenticating them [2]. The template of the fingerprint is normally stored on a local security domain or server [3]. The fact is that it is difficult to tamper with once it has been generated because the biometrics of a human fingerprint are compromised [4]. Moreover, any approach to fingerprint authentication involves storing a fingerprint feature template on a local computer or a server so that the fingerprint comparison can be completed [5-6]. Hackers, however, can easily target the template. Privacy leaking is therefore a danger associated with the technical approach for keeping fingerprint feature templates [7]. The main techniques for protecting fingerprint information currently in use are fuzzy vaults, biological keys, fingerprint feature template protection, and biological keys [8]. When the template protection approach is used, fingerprint identification accuracy has dropped, and the protection impact is subpar [9]. When using fuzzy vault technology, there is a chance that a malicious party might compare many template databases with identical biometric features and discover the user's fingerprint characteristics [10].

Received: July 16, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Traditional biometric authentication systems face challenges in ensuring robust security, particularly against emerging quantum threats, while maintaining efficiency in real-time and resource-constrained environments. Existing methods often suffer from vulnerabilities such as key instability, susceptibility to spoofing, and high computational demands. This research is motivated by the need for a secure, lightweight, and reliable biometric key generation approach that can resist quantum-level attacks. By leveraging finger vein patterns unique and difficult to replicate and integrating advanced neural models with post-quantum encryption, the proposed system addresses the critical need for enhanced security, accuracy, and adaptability in authentication frameworks. The contributions are listed below,

- Introduced Adaptive and Propagated Mesh Filtering (APMF) to enhance finger vein image quality by removing noise and preserving vein structure for better feature extraction.
- Employed a Spike-Driven Transformer (SDT) to extract robust, biologically inspired temporal features from finger vein patterns.
- Designed a binary vector conversion scheme integrated with fuzzy extractor logic to enable stable and repeatable key generation from biometric features.
- Integrated Dynamic Lightweight Symmetric Encryption (DLSE) for secure key binding, ensuring quantum-resistant data protection.
- Proposed MHGNN optimized by White Shark Optimizer (WSO) to enhance accuracy and convergence in biometric key reconstruction and authentication.

The literature is reviewed in Section 2, a technique is suggested in Section 3, the results and comments are presented in Section 4, and future work is discussed in Section 5.

II. Literature Survey

Some of the existing articles based on Biometric Key Generation using DL are discussed here.

In 2025, Hammad, et al., [11] presented deep learning-based multidimensional scaling, cancelable finger vein authentication. This approach combined MDS with a lightweight convolutional neural network (LCNN) model for feature extraction, thereby addressing the shortcomings of earlier biometric identification systems. The outcomes showed how well the suggested approach worked, as it produced excellent results in the diversity and irreversibility tests, along with high accuracy and low mistake rates.

In 2022, Chai, et al., [12] employed LCNN with shape-driven technology for finger vein biometrics. First, vein images were obtained from the benchmark dataset. This is followed by preprocessing to improve vein visibility and consistency in the suggested methodology for finger vein recognition. Deep networks include drawbacks, including excessive memory use and poor training efficiency, which were addressed by using a Lightweight Semi-pretrained Model (LSPM) to strike a balance between performance and computational efficiency.

Received: July 16, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In 2025, Hammad, et al., [13] suggested a new structure that integrates a shallow deep learning model with Cancelable Random Masking (CRM) to make safe and understandable finger vein authentication. Based on cryptography, random masks, the CRM method manipulates the template of biometrics to ensure privacy, revocability, and cancelability. These altered templates were then fed through convolutional neural networks (CNNs) that were supposed to learn discriminative features directly on masked inputs instead of having to manually develop feature extraction.

In 2022, Wu, et al., [14] presented fingerprint image capture and preprocessing were the first steps in the fingerprint bio-key generation procedure for post-quantum security. To extract stable, discriminative features while lowering intra-user variability, the processed images are sent to a deep learning-based FPBK_Stabilizer, which carries out feature selection and multilayer convolutional projection. After the feature vector was binarized, it was sent into a fuzzy extractor, which generates public helper data and a repeatable cryptographic key. Using a quantum-resistant method like McEliece, the key was bound to provide post-quantum security.

A. Research Gap

Recent approaches in finger vein and fingerprint biometrics have explored lightweight deep learning models, cancelable template protection, and improved recognition accuracy. However, a notable gap remains in integrating these systems with post-quantum cryptographic mechanisms. Most existing works focus either on efficient feature extraction or template security, lacking an end-to-end framework that combines deep learning-based feature stabilization, reproducible biometric key generation, and quantum-resistant binding. Additionally, challenges such as intra-user variability, environmental noise, and the need for interpretability are not fully addressed. There is a need for a unified, secure, and efficient biometric system that ensures both high accuracy and post-quantum resilience.

III. Proposed Methodology

The proposed MHGNN-WSO system begins with finger vein image acquisition, which is enhanced using APMF to improve vein clarity. Feature extraction is performed using an SDT, and the resulting vector is normalized with M2N. This normalized feature vector is converted into a binary format and passed through a fuzzy extractor to generate a secure cryptographic key along with helper data. For post-quantum protection, DLSE is applied. During authentication, the MHGNN, optimized by the WSO, reconstructs the original key. The block diagram of the proposed approach is displayed in Figure 1.

A. Input Acquisition

Finger vein recognition is a highly secure biometric modality due to its internal, unique, and forgery-resistant nature. It has also become a widespread application in authentication systems for personal and institutional purposes. Finger vein images are utilized in this study as the main biometric input. The dataset, obtained from Kaggle, consists of 425 images with

Received: July 16, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

85 classes, giving a strong and varied sample set to be used for training and testing the system [15]. The images are captured via near-infrared (NIR) imaging, which emphasizes the patterns of subcutaneous veins needed to extract features accurately and generate secure cryptographic keys.

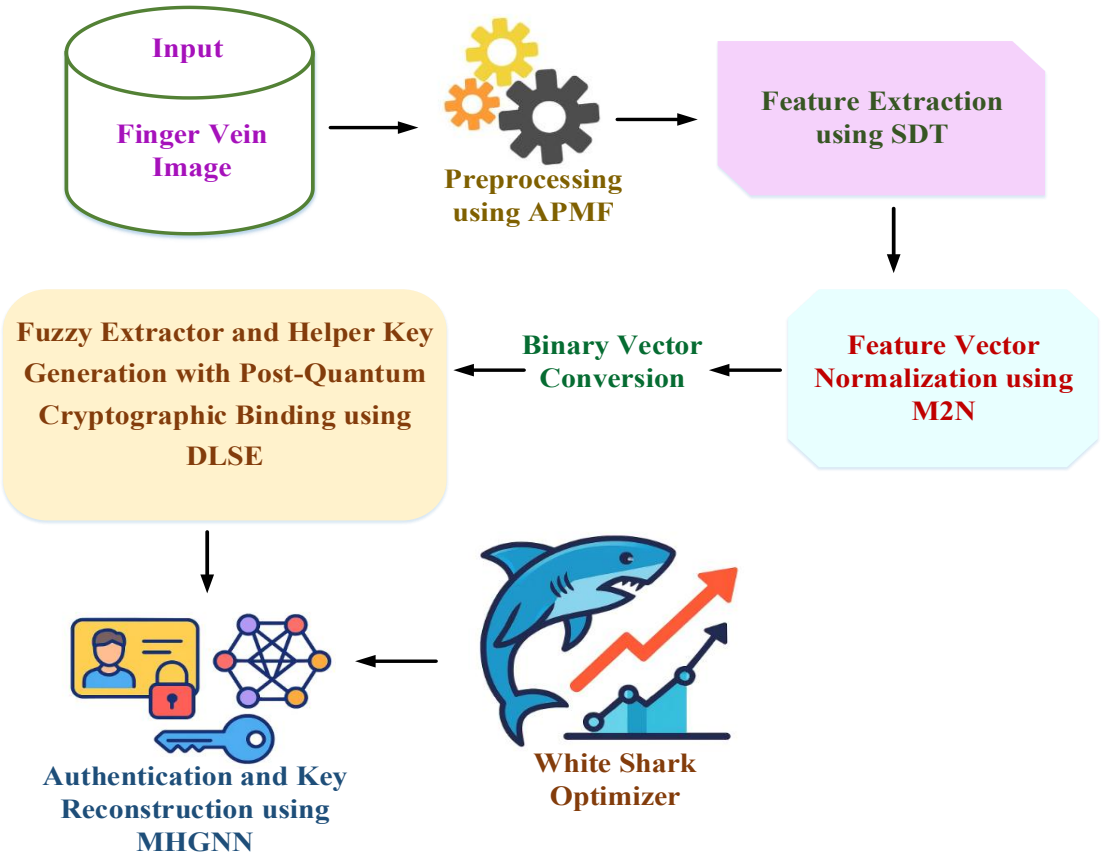

Fig.1. Block diagram of proposed methodology

B. Preprocessing using Adaptive and Propagated Mesh Filtering

Adaptive and Propagated Mesh Filtering (APMF) is employed as a preprocessing technique to enhance finger vein images by reducing noise and improving the visibility of vein structures for accurate feature extraction [16]. Its flexibility enables the reduction of noise on a local basis and does not cause significant biometric features to fail. This preprocessing process yields clean images and more uniform images, which is very important in ensuring accurate results in terms of extracting the features.

Pretreatment preprocessing involves Duplicate mesh construction of the finger vein image, such that in the construction, each segmented area is treated as a node, with the edges drawn to link neighboring areas so as to make the spatial relation. A bilateral filtering method is used to smooth region normals based on both spatial proximity and angular similarity, as expressed in Equation (1):

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$\bar{Z}_i = \frac{1}{G_i} \sum_{j_l \in M_i} C_{k_i}(I(k_i,k_l)) C_{a_i}(I(Z_i,Z_l)) Z_l \quad (1).$$

where, $\bar{Z}_i$ represents Filtered normal at vertex i, Z_l is the Normal at neighboring vertex l, M_i represents Neighboring vertices within the patch around i, $I(k_i,k_l)$ Geodesic distance between centroids k_i and k_l, $I(Z_i,Z_l)$ represents Difference between the normals Z_i and Z_l, G_i represents Normalizing weight for the patch. The final update of each pixel's position is computed by blending curvature-driven adjustment with normal direction correction, as shown in Equation (2):

$$\bar{p}_i = p_i + S.\frac{\psi_i}{\|\psi_i\|^2}.w_i + (1-S).w_i \quad (2).$$

where, S is the balance parameter. This comprehensive APMF-based preprocessing pipeline ensures that finger vein inputs are noise-free, contrast-enhanced, and structure-preserving, laying a strong foundation for reliable feature extraction and biometric key generation.

C. Spike-Driven Transformer-based Feature Extraction

Spike-Driven Transformer (SDT) is employed for feature extraction to efficiently capture temporal and spatial patterns in finger vein images through biologically inspired spike-based encoding and attention mechanisms [17]. It is capable of information encoding via transient measurements (spikes), its energy consumption is low, and its utility is more computationally efficient since it is inspired by and fundamentally works by modeling the physical mechanisms of the brain. It is also resistant to noise and distortion as its spike-based architecture enables it to generate sparse, compact representations of feature representations, which can be effectively converted into binary or secure keys.

The proposed biometric system would require the involvement of DT as it extracts spatiotemporal features that make sense out of the finger vein photos. Fundamentally, the SDT consists of spiking neuron models that represent biological neurons in a time-dependent, yet computationally efficient way by assuming a Leaky Integrate-and-Fire (LIF) neuron model. The membrane potential of each neuron is changed at each time step depending on the accumulation of historical signal and the existing spatially encoded signal, as written in Equation (3):

$$Q[t] = K[t-1] + R[t] \quad (3).$$

where, $Q[t]$ represents the membrane potential at time step t, $K[t-1]$ is the historical state propagated from the previous time step, $R[t]$ represents the incoming feature from the input layer, such as convolutional attention-based embeddings derived from a finger vein image. Once the potential is computed, spike activation is triggered when the potential exceeds a predefined firing threshold, governed by Equation (4):

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$B[t] = Hea(Q[t] - q_{th}) \quad (4).$$

where, binary output $B[t]$ is generated through the Heaviside step function, where the neuron emits a spike (1) only if the membrane potential exceeds the threshold q_{th} ; otherwise, it remains inactive (0). To model global dependencies within the spatial domain of the vein structure, the architecture employs Spike-Driven Self-Attention (SDSA), a spiking alternative to conventional softmax-based attention, as defined in Equation (5):

$$SDSA(A,H,L) = SN(SUM_1(A_B \otimes H_B)) \otimes L_B \quad (5).$$

where, A_B , H_B and L_B re the spike-encoded representations of the query, key, and value tensors, respectively. The attention map is generated using a Hadamard product and column-wise summation, followed by spike neuron activation $SN(.)$. This attention mechanism emphasizes critical regions within the vein image, enabling precise and sparse feature representation essential for secure biometric key generation.

D. Feature Vector Normalization using Min–Max Normalization

Min–Max Normalization (M2N) is used to scale the extracted feature vectors into a uniform range, enabling consistent, stable, and efficient processing in the subsequent stages of the biometric key generation system [18]. This normalization enhances numerical stability, accelerates the convergence of learning models like MHGNN, and maintains the relative structure of the original data.

To ensure uniformity and consistency in feature scales, M2N is applied to the extracted feature vectors. This technique scales each feature to a predefined range, typically between 0 and 1, which helps in eliminating bias caused by differing feature magnitudes and enhances the performance of subsequent processing stages like binary conversion and neural network-based authentication. The normalization is performed using equation (6)

$$b'_{o.m} = \frac{b_{o,m} - \min(b_o)}{\max(b_o) - \min(b_o)} \times (new\_\max - new\_\min) + new\_\min \quad (6).$$

where, $b'_{o.m}$ represents the normalized feature value, $b_{o,m}$ is the original input, $\min(b_o)$ and $\max(b_o)$ represents the minimum and maximum values of the feature o respectively. The range $(new\_\max - new\_\min)$ is set to [0,1] in this context. This normalization step ensures consistent feature scaling, enhances model stability and convergence, and prepares the data effectively for binary vector conversion in the secure biometric key generation process.

E. Binary Vector Conversion

In order to facilitate safe cryptographic key creation, the constant real-valued feature vector achieved with the help of the finger vein image is reduced to binary with the help of a threshold rule. This will be necessary in the process of linking the biometric data to fuzzy extraction units and encryption formulae. Every component of the feature vector is matched

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

with an a priori threshold that is usually zero or the average of the feature vector. The value is replaced by 1, in case it is big enough or equal to the threshold, or replaced by 0 otherwise. This binary coding simplifies the level of features and maintains critical differences in key reconstruction. The procedure of binarization is described in equation (7)

$$J_j = \begin{cases} 1 & if\ z_j \geq d_j \\ 0 & if\ z_j < d_j \end{cases} \quad (7).$$

where, J_j is the j^{th} binary output, z_j is the j^{th} feature value, d_j represents the corresponding threshold. This binary conversion ensures that the extracted features are transformed into a stable and compact representation, enabling consistent and secure biometric key generation suitable for post-quantum cryptographic applications.

F. Fuzzy Extractor and Helper Key Generation with Post-Quantum Cryptographic Binding using DLSE

As biometric key generation in the proposed noticeable biometric key generation indicates, a Fuzzy Extractor is employed to produce a consistent and secure cryptographic key that is based on the binarized biometric feature vector. The fuzzy extractor is vital because of the intra-user variability of biometric data samples in re-reconstructing an identical key upon every authentication session in the event that there is a modest modification of the input. It produces two elements: the secure key and an attached helper, which aids in the regeneration of keys without showing any sensitive data regarding biometrics.

In order to achieve security in the post-quantum era, a Dynamic Lightweight Symmetric Encryption (DLSE) [19] is incorporated to allow the helper data and these generated keys to be bound and to encrypt them. To fulfill its purpose specifically, DLSE is made to perform effectively in resource-limited settings, like embedded biometric gadgets, with low-latency decryption and encryption with high-security standards.

a. Session Key Generation

The DLSE process commences with the initiation of a dynamic Session Symmetric Key (SSK). An ASCII-compatible number (between 33 and 126) is selected at random, converted into an 8-bit binary, and duplicated until it reaches 64 bits of the base key. The key is rotated 10 times to the left, with the number of bits rotated in each round being provided by the timestamp and metadata of the biometric that is input. The key is then divided through rotation into two 32-bit halfs known as left session key (LSK) and right session key (RSK). The final 64-bit SSK, which should be of high randomness and session uniqueness, is generated by a bitwise XOR of LSK and RSK.

b. Master Key Creation and Encryption

During the encryption portion, the biometric key that accompanies the fuzzy extractor is stuffed up to 64 64-bit margins and divided into Left and Right halves. They are XORed with

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

session keys (LSK and RSK) and then permuted and substituted many times. The processed halves are then XORed with a session symmetric key (SSK) and merged. The final 64-bit binary is converted to printable ASCII characters (33–126), with a flag array recording adjustments. A Master Secret Key (MSK), formed from the flag array and original random number, ensures secure decryption and unique, resilient encryption tightly linked to the biometric input.

c. Key Regeneration and Decryption

During authentication, the received MSK is parsed to extract the random number and the flag array. Using this information, the DLSE session key generation steps are re-executed to regenerate LSK, RSK, and SSK. The encrypted biometric key is then converted back to binary form. Based on the flag array, inverse arithmetic operations are performed to revert the ASCII normalization. The binary string is split into two halves, XORed with the regenerated SSK, and then processed through inverse substitution and permutation rounds. A final XOR with LSK and RSK fully restores the original biometric key, enabling secure and accurate authentication. The process of DLSE is given in Algorithm 1.

Algorithm 1: Dynamic Lightweight Symmetric Encryption

Input

Biometric Key (from fuzzy extractor)

Random number x (between 33–126)

Metadata value J

Output

Encrypted Biometric Key (cipher_text)

Master Secret Key (MSK)

Reconstructed Biometric Key (during decryption)

Step 1: Session Key Generation

Generate a random number x between 33–126.

Convert x to 8-bit binary and repeat it 8 times → 64-bit key.

Rotate the key left 10 times by p bits (p starts at 5, increases by 2 each time).

Split the key into:

LSK: left 32 bits

RSK: right 32 bits

$SSK = LSK \oplus RSK$

Step 2: Encryption and MSK Generation

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Convert biometric key to binary → pt_bin. Pad to 64 bits if needed.

Split into two halves: left and right.

XOR:

left = left ⊕ LSK

right = right ⊕ RSK

Apply 4 rounds of:

Substitution (S-box)

Permutation (P-box) to both halves.

XOR both with SSK:

n_left = left ⊕ SSK

n_right = right ⊕ SSK

Merge into m_ct (64-bit).

Convert m_ct into decimal values and adjust:

If < 33 → add 33 → flag = "1"

If > 126 → subtract 126 → flag = "2"

Else → flag = "0"

Convert to characters → cipher_text.

Create MSK by combining x and the flag_string.

Step 3: Decryption and Key Regeneration

Extract x and flag_string from MSK.

Repeat ***Session Key Generation*** *to get LSK, RSK, and SSK.*

Convert cipher_text to decimal values.

Reverse ASCII adjustments using flag_string.

Convert back to binary → ct_bin, then split into left and right.

XOR:

left = left ⊕ SSK

Right = right ⊕ SSK

Apply 4 rounds of ***inverse****:*

S-box substitution

P-box permutation

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Final XOR:

$left = left \oplus LSK$

$right = right \oplus RSK$

Merge both → original pt_bin.

Convert pt_bin to recover the ***biometric key****.*

G. Authentication and Key Reconstruction using Magnetized Hopfield Global Neural Network

MHGNN is employed in the proposed framework to reliably reconstruct biometric keys during authentication by leveraging its powerful associative memory and noise-resilient pattern retrieval capabilities [20-21]. MHGNN enhances the classical Hopfield network by integrating magnetization-inspired global dynamics, allowing it to accurately retrieve stored binary biometric keys even when partial or noisy inputs are presented.

The dynamic behavior of MHGNN can be described using an energy-based model, where each state represents a potential biometric key pattern, and stable states correspond to valid, learned keys. The system evolution is governed by the following differential equation (8)

$$\frac{dc_e}{dt} = -c_e + \sum_{g=1}^{n} h_{ef} \cdot \tan y(c_g) + V_e(t) \quad (8).$$

where, c_e is the state variable representing the predicted or stored energy usage level for feature e, h_{ef} represents synaptic weight capturing learned interaction from neuron g to e, $\tan y(.)$ is the nonlinear activation function ensuring bounded outputs and modeling real-world saturation effects, $V_e(t)$ external input reflecting contextual variables such as weather conditions or pricing data at time t. To enhance the temporal sensitivity and feature discrimination capabilities of MHGNN, a GAN is integrated, enabling the model to dynamically prioritize the most relevant temporal segments and feature patterns within the biometric input. This combination enhances the accuracy and stability of key reconstruction when the network is able to adaptively interfere with important variations in biometric data, realizing greater resilience to noise, a higher level of interpretability, and reliable authentication in secure biometric systems. To obtain convergence and prevent unstable oscillations, the network is put into a principle of energy minimization, which can be written in equation (9)

$$\hat{k} = D_s r_{final} + x_s \quad (9).$$

where, D_s denotes the output weight matrix, x_s is the output bias. During authentication, the noisy binary vector obtained from the fuzzy extractor is fed as input, and the MHGNN evolves toward the closest stable state. This enables accurate reconstruction even in the

Received: July 16, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

presence of biometric variation or corruption. Furthermore, MHGNN supports parallel pattern matching, low-latency inference, and high fault tolerance, making it an ideal mechanism for secure, real-time key recovery in biometric-based post-quantum cryptographic systems.

a. Optimization using White Shark Optimizer

The weight parameters h_{ef} and D_s are optimized using WSO [22].WSO is inspired by the swift and strategic predatory behavior of white sharks, which efficiently balances exploration and exploitation. In the proposed biometric framework, WSO optimizes MHGNN weight parameters, enhancing key reconstruction by avoiding local minima, accelerating convergence, and ensuring robust performance even with noisy biometric input data. The stepwise procedure is described below,

Step 1: Initialization

In the proposed framework, WSO is used to optimize the weight parameters of the MHGNN. Initially, a population of candidate solutions representing different parameter sets is randomly generated within a multi-dimensional search space, where each dimension corresponds to a trainable weight of the MHGNN model.

Step 2: Fitness Function

To guide WSO in optimizing MHGNN for biometric key reconstruction, a fitness function is defined to minimize reconstruction error. This function evaluates how accurately the network retrieves the original key from noisy input, penalizing deviations and ensuring robust, precise authentication by steering WSO toward optimal weight configurations. The mathematical expression of the fitness function is given in equation (10)

$$Fitness\ \ function = optimizing\left(h_{ef}\ and\ D_s\right) \tag{10}$$

where, h_{ef} is for increase accuracy and D_s is for decrease loss.

Step 3: Exploration-Exploitation Strategy of White Sharks

In the proposed biometric key reconstruction system, WSO simulates the exploratory movement of white sharks within the high-dimensional weight space of MHGNN. Each white shark adjusts its position by considering both its personal best solution and the globally best-known position discovered by the swarm. This balance between global exploration and local exploitation is achieved through adaptive velocity updates, formulated in equation (11)

$$E_u^{i+1} = Y\left[E_u^i + F_1.P_1.\left(r_{gbest}^i - p_u^i\right) + F_2.P_2.\left(r_{uv}^{best} - r_u^i\right)\right] \tag{11}$$

where, E_u^i represents the current velocity vector of the u^{th} shark at iteration i, p_u^i represents the current position of the u^{th} shark, r_{gbest}^i is the global best position found so far, r_{uv}^{best} is the Best-known position.

Received: July 16, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Step 4: Termination Condition

The WSO optimization halts upon reaching a predefined iteration limit or achieving a target fitness threshold, ensuring efficient convergence and reliable parameter tuning for accurate biometric key reconstruction using MHGNN.

IV. Results and Discussion

This section of the study presents the MHGNN-WSO method's outcomes. The proposed framework was implemented using Python 3.10 with TensorFlow and PyTorch libraries. All experiments were conducted on a system with an Intel Core i9 processor, 32 GB RAM, and an NVIDIA RTX 3080 GPU.

A. Performance measures

Several performance metrics have been analysed for the comparison of the proposed methodology. The performance of the proposed technique with reference to other existing methods [11-14] is provided in Table 1.

Table I. Comparative Performance Analysis of the Proposed Model Against Existing Methods

Methods	Accuracy (%)	FAR	FRR	EER
LCNN [11]	94.2	0.12	0.11	0.115
LCNN-LSPM [12]	95.6	0.09	0.10	0.095
CNN-CRM [13]	96.3	0.08	0.09	0.085
MCP-FP [14]	97.2	0.07	0.08	0.075
Proposed	99.7	0.08	0.08	0.08

Table 1 compares the performance of various biometric authentication methods using key metrics: Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). The proposed method outperforms others with 99.7% accuracy and the lowest balanced error rate (EER = 0.08), indicating superior security and reliability.

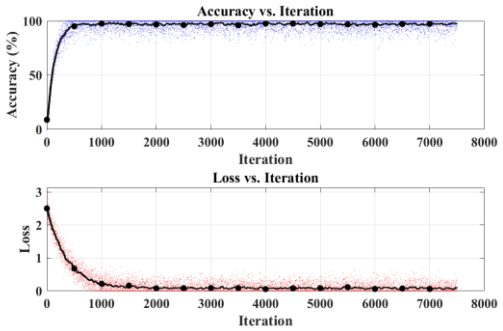

Fig.2. Accuracy and Loss trends over training iterations showing convergence behavior

Figure 2 plots demonstrate the learning behavior of the proposed model. Accuracy improves rapidly within the first 1000 iterations, stabilizing near 98–100%, indicating

Received: July 16, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

effective learning and minimal overfitting. Simultaneously, the loss decreases sharply early on and gradually plateaus, confirming stable convergence and efficient model optimization throughout training.

V. Conclusion

This study proposed a secure biometric key generation framework using finger vein images with APMF preprocessing, SDT-based feature extraction, and MHGNN-WSO for key reconstruction. DLSE ensures post-quantum security through dynamic encryption. The system achieved high accuracy (99.7%) and low EER (0.08), outperforming existing methods. However, limitations include computational complexity and sensitivity to image quality. Future work will focus on optimizing performance for real-time and edge applications, enhancing robustness to noisy inputs, and extending the framework to support multimodal biometric data for broader authentication scenarios in healthcare and IoT environments.

References

[1] O. Kuznetsov, D. Zakharov, and E. Frontoni, "Deep learning-based biometric cryptographic key generation with post-quantum security," Multimedia Tools Appl., vol. 83, no. 19, pp. 56909–56938, 2024. DOI: 10.1007/s11042-023-17714-7

[2] R. Arjona, P. López-González, R. Román, and I. Baturone, "Post-quantum biometric authentication based on homomorphic encryption and classic McEliece," Appl. Sci. (Basel), vol. 13, no. 2, p. 757, 2023. DOI: 10.3390/app13020757

[3] B. Bera, S. Nandi, A. K. Das, and B. Sikdar, "Healthcare Security: Post-Quantum Continuous Authentication With Behavioral Biometrics Using Vector Similarity Search," IEEE Trans. Inf. Forensics Security, vol. 20, pp. 1597–1612, 2025. DOI: 10.1109/TIFS.2025.3531197

[4] M. Alam, J. Hoffstein, and B. Cambou, "Privately generated key pairs for post quantum cryptography in a distributed network," Appl. Sci. (Basel), vol. 14, no. 19, p. 8863, 2024. DOI: 10.3390/app14198863

[5] K. Pursharthi and D. Mishra, "Post-quantum framework for authorized and secure communication in multi-server networking," Telecomm. Syst., vol. 87, no. 2, pp. 403–418, 2024. DOI: 10.1007/s11235-024-01190-x

[6] A. Braeken, "Flexible hybrid post-quantum bidirectional multi-factor authentication and key agreement framework using ECC and KEM," Future Gener. Comput. Syst., vol. 166, p. 107634, 2025. DOI: 10.1016/j.future.2024.107634

[7] K. Mansoor, M. Afzal, W. Iqbal, Y. Abbas, S. Mussiraliyeva, and A. Chehri, "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems," Internet Things (Amst.), vol. 27, p. 101228, 2024. DOI: 10.1016/j.iot.2024.101228

[8] D. Chaudhary, U. Kumar, and K. Saleem, "A construction of three party post quantum secure authenticated key exchange using ring learning with errors and ECC cryptography," IEEE Access, vol. 11,136947–136957, 2023. DOI: 10.1109/ACCESS.2023.3325886

Received: July 16, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[9] A. Ahmad and S. Jagatheswari, "Quantum safe multi-factor user authentication protocol for cloud assisted medical iot," IEEE Access, 2024.

[10] Ahmed, S. and Anisi, M.H., 2025. A Post-Quantum Secure Federated Learning Framework for Cross-Domain V2G Authentication. IEEE Transactions on Consumer Electronics.

[11] M. Hammad, M. ElAffendi, and A. A. Abd El-Latif, "Cancelable finger vein authentication using multidimensional scaling based on deep learning," Egyptian Informatics Journal, vol. 30, p. 100708, 2025. DOI: 10.1016/j.eij.2025.100708

[12] T. Chai, J. Li, S. Prasad, Q. Lu, and Z. Zhang, "Shape-driven lightweight CNN for finger-vein biometrics," J. Inf. Secur. Appl., vol. 67, p. 103211, 2022. DOI: 10.1016/j.jisa.2022.103211

[13] M. Hammad, A. A. Ateya, M. ElAffendi, and A. A. Abd El-Latif, "Cancelable random masking with deep learning for secure and interpretable finger vein authentication," Intell. Syst. Appl., vol. 27, p. 200552, 2025. DOI: 10.1016/j.iswa.2025.200552

[14] Z. Wu, Z. Lv, J. Kang, W. Ding, and J. Zhang, "Fingerprint bio-key generation based on a deep neural network," Int. J. Intell. Syst., vol. 37, no. 7, pp. 4329–4358, 2022. DOI: 10.1002/int.22782

[15] https://www.kaggle.com/code/kerneler/starter-finger-vein-304d4660-1

[16] B. Liu, B. Li, J. Cao, W. Wang, and X. Liu, "Adaptive and propagated mesh filtering," Comput. Aided Des., vol. 154, p. 103422, 2023. DOI: 10.1016/j.cad.2022.103422

[17] M. Yao, J. Hu, T. Hu, Y. Xu, Z. Zhou, Y. Tian, et al., 2024. Spike-driven transformer v2: Meta spiking neural network architecture inspiring the design of next-generation neuromorphic chips. arXiv preprint arXiv:.

[18] M. Shantal, Z. Othman, and A. A. Bakar, "A novel approach for data feature weighting using correlation coefficients and min–max normalization," Symmetry (Basel), vol. 15, no. 12, p. 2185, 2023. DOI: 10.3390/sym15122185

[19] Saif, S., Halder, S. and Biswas, S., 2024. DLSEA-64: dynamic lightweight symmetric encryption algorithm for secure data transmission in IoT based pervasive sensing applications. Journal of Cyber Security Technology, pp.1-27.

[20] H. Lin, C. Wang, Y. Sun, and T. Wang, "Generating n-scroll chaotic attractors from a memristor-based magnetized hopfield neural network," IEEE Trans. Circuits Syst. II Express Briefs, vol. 70, no. 1, pp. 311–315, 2022. DOI: 10.1109/TCSII.2022.3212394

[21] F. Zhang, S. Lin, X. Xiao, Y. Wang, and Y. Zhao, "Global attention network with multiscale feature fusion for infrared small target detection," Opt. Laser Technol., vol. 168, p. 110012, 2024. DOI: 10.1016/j.optlastec.2023.110012

[22] M. Braik, A. Hammouri, J. Atwan, M. A. Al-Betar, and M. A. Awadallah, "White Shark Optimizer: A novel bio-inspired meta-heuristic algorithm for global optimization problems," Knowl. Base. Syst., vol. 243, p. 108457, 2022. DOI: 10.1016/j.knosys.2022.10845

Received: July 16, 2025