

Enhanced Elman Spike Neural Network optimized with Glowworm Swarm Optimization for Authentication of Multiple Transaction using Finger Vein

S. Mary Joans (✉ profsmaryjoans1472@gmail.com)

Velammal Engineering College

J.S. Leena Jasmine

Velammal Engineering College

P. Ponsudha

Anna University Chennai

Research Article

Keywords: Authentication Of Multiple Transaction, contrast limited adaptive histogram equalization filtering, Enhanced Elman Spike Neural Network, Finger Vein, Glowworm Swarm Optimization, visual geometry group network

Posted Date: June 29th, 2022

DOI: <https://doi.org/10.21203/rs.3.rs-1775418/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Enhanced Elman Spike Neural Network optimized with Glowworm Swarm Optimization for Authentication of Multiple Transaction using Finger Vein

Dr. S. Mary Joans, ^{1*}Dr. J.S. Leena Jasmine, ² Dr. P. Ponsudha³

^{1}Professor and Head, Department of Electronics and Communication Engineering,*

Velammal Engineering College, Chennai

^{1}Email: profsmaryjoans1472@gmail.com*

²Professor, Department of Electronics and Communication Engineering, Velammal

Engineering College, Chennai

³Research Scholar, Department of Electronics and Communication Engineering, Anna

University, Chennai, Tamil Nadu, India.

Abstract

Nowadays, Automated Teller Machines (ATM) are broadly used every one. Hence, the security is some more need to improve the bank sector. Due to increase in the count of criminals and their activities, ATMs have become unsafe. The access card and PIN are used in the ATM system for identity verification. Recent advances in biometric detection techniques, like fingerprinting, retinal scanning, face recognition, have made great strides in recovering the insecure environment at ATMs. In this manuscript, an Enhanced Elman Spike Neural Network Optimized with Glowworm Swarm Optimization is proposed for Authentication of Multiple Transaction Using Finger Vein (EESNN-GWO-AMT-FV). Here finger vein authentication, images are collected from the SDUMLA-HMT dataset. Then the images are pre-processed to improve the quality of the images using contrast limited adaptive histogram equalization filtering (CLAHEF). The features are extracted by using the visual geometry group network (VGG16). By using VGG16 model, various features are extracted,

such as Vein Patterns, Local Binary Patterns, Dimensionality Reduction and Image Transformations. The extracted features are transferred to EESNN classifier for classifying the authorized person and unauthorized person. Then the weight parameters of the EESNN are optimized using the Glowworm swarm optimization Algorithm (GWO). The proposed method is implemented and the efficiency of the proposed EESNN-GWO-AMT-FV is examined under performance metrics, viz accuracy, specificity, sensitivity, precision, Error rate, AUC. The performance of the proposed method provides higher accuracy 99.01%, 98.34%, and 97.45%, and higher precision 87.12%, 94.12% and 91.78% compared with existing methods, like CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV respectively.

Keywords: *Authentication Of Multiple Transaction, contrast limited adaptive histogram equalization filtering, Enhanced Elman Spike Neural Network, Finger Vein, Glowworm Swarm Optimization, visual geometry group network.*

1. Introduction

Finger Vein authentication schemes commonly utilized in various applications for authentication purposes [1, 2]. Unlike conventional authentication tools, like PIN, password always at risk of being forgotten or stolen, but the biometric authentication provides the best convenience for the user [3, 4]. Privacy is an important concern in finger vein authentication systems [5]. If the biometric template is compromised, it cannot be changed. Several biometric template protection (BTP) schemes are presented to deal this challenge [6, 7]. Even though BTP offers privacy for the finger vein authentication system, they suffer the performance of authentication [8, 9]. Authentication depends on the vascular patterns formed by the blood vessels of the human finger in finger vein biometric systems. Because these forms have sufficient characteristics, they are utilized for automatic personal recognition [10]. Most of these methods extract the structure of binary vessel, and then compare the

extracted templates utilizing algorithms [11]. Besides these methods, some other methods use deep neural networks [12]. However, many works try to improve the finger vein recognition (FVR) systems secure. Index-of-Maximum (IoM) hashing technique has been used to present an alignment-free template protection scheme [13, 14]. Conversely, in extracted biometric features, the user-specific random scheme is used to decrease the dimension of the features and create protected templates [15]. A deep neural network is applied secured templates.

Nowadays, crime in ATMs has become a matter of concern. There is no guarantee behind the security for the customer's account. Many who are unaware about PIN are not likely to memorize and recognize it, for eg, if they have lost their card, their account may be accessed by others and they may lose their money. To overcome this problem, some solutions need to be put forward to fix this problem. The existing methods did not provide sufficient accuracy for authentication of multiple transactions using finger vein, which are motivated to do this research work.

For account transaction instead of ATM/Debit card using finger Vein Authentication. User can integrate all his accounts in other banks can be integrated in this single account with unique double digits PIN numbers. User finger vein authentication is used for the verification part. For this purpose Enhanced Elman Spike Neural Network Optimized with Glowworm Swarm Optimization for Authentication of Multiple Transaction Using Finger Vein (EESNN-GWO-AMT-FV) is proposed.

The main contribution of this manuscript are summarized below,

- In this manuscript, Enhanced Elman Spike Neural Network Optimized with Glowworm Swarm Optimization is proposed For Authentication of Multiple Transaction Using Finger Vein (EESNN-GWO-AMT-FV).
- Here, finger vein authentication, imageries are collected from SDUMLA-HMT dataset [16].

- Then the imageries are pre-processed to improve the quality of the images using contrast limited adaptive histogram equalization filtering (CLAHEF) [17].
- Then features is extracted by using the visual geometry group network (VGG16) [18].
- By using VGG16 model, various features are extracted such as Vein Patterns, Local Binary Patterns, Dimensionality Reduction and Image Transformations.
- Then, the extracted features are transferred to enhanced Elman spike neural network (EESNN) [19] classifier for classifying the authorized person and unauthorized person. Then the weight parameters of the EESNN are optimized using the Glowworm swarm optimization Algorithm (GWO) [20].
- The proposed method is implemented and the efficiency of the proposed EESNN-GWO-AMT-FV is examined under performance metrics, like accuracy, specificity, sensitivity, precision, Error rate, AUC.
- Then, the performance of the proposed method is analyzed with existing methods, like CNN-AOA-MBR-FV [21], CNN-MBR-FKP-FV [22], DCNN-MBR-FV [23] respectively.

Remaining manuscript is organized as: section 2 portrays recent studies, section 3 describes about the proposed method, section 4 shows the results with discussion, and section 5 concludes the manuscript.

2. Literature Survey

Among the several research works related to authentication of multiple transactions using finger vein, some of the latest investigations are reviewed here,

In 2020, Alay, et.al., [21] have presented deep learning approach for multimodal biometric recognition system based on fusion of iris, face, finger vein traits. The presented scheme was depending on CNNs that extract the features as well as classify the imageries through softmax classifier. To build the convolutional neural networks model, VGG-16,

Adam optimization was deemed, also categorical cross-entropy was employed into loss function. It provides lower accuracy with minimum error rate.

In 2020, Daas, et.al., [22] have presented multimodal biometric identification schemes utilizing deep learning depending on finger vein and finger knuckle print fusion. The features extraction for finger knuckle print and finger vein were performed by transfer learning CNN architectures, viz AlexNet, VGG16, ResNet50. It provides higher accuracy conversely with higher error rate.

In 2022, Boucetta, et.al., [23] have presented biometric authentication utilizing finger-vein patterns along deep-learning, discriminant correlation analysis. Where, finger-vein identification system uses Squeeze net pre-trained Deep-CNN as feature extractor from left and right finger vein patterns. Then combine such deep-based features through feature-level Discriminant Correlation Analysis to lessen the feature dimensions. It provides high mean accuracy with higher error rate.

In 2020, Shaheed, et.al., [24] have presented finger-vein presentation attack detection using depth wise separable convolution neural network. A depthwise separable convolution neural network (DSC) with residual connection and a linear support vector machine (LSVM) for automatic identification of finger vein presentation attacks. DSC was extract robust features from FV images. Then LSVM classifier was classify the images as bonafide and fake images. It provides low error rate with low accuracy.

In 2020, Yang, et.al., [25] have presented an embedded finger-vein recognition along antispooofing utilizing unified convolutional neural network. The finger-vein recognition and antispooofing network (FVRAS-Net) incorporates the recognition task and the antispooofing task into a unified CNN model utilizing multiple task learning model and attains higher security. A multiple intensity illumination was suggested into the embedded biometric system to automated select the most informative image for finger-vein identification, which enhances

the recognition performance of the real system. It provides lower matching rate with higher specificity.

In 2021, Shahreza, et.al., [26] have presented protecting and enhancing vascular biometric recognition methods via biohashing and deep neural networks. Where, considered raw and pre-processed finger vein imageries and presented a deep-learning-base model for securing biometric templates as well as upgrade recognition performance. A deep convolutional auto-encoder structure was used to lessen the feature space dimension, then secure templates in term of Biohashing approach. It provides lower error rate with lower precision.

In 2022, Heidari, et.al., [27] have presented deep learning based biometric authentication depending on different level fusion of finger knuckle print and fingernail. A multimodal biometric was considered to enhance the performance of authentication and make it resistant for spoofing attacks. A deep learning-based method with the help of convolutional neural network along AlexNet as a pre-trained model was applied. Various features were extracted from hand imageries, were consolidated normalization and fusion methods. It provides higher sensitivity with higher error rate.

3. Proposed Methodology

Cardholder can be verified by using fingerprint authentication as a tool to authenticate users at ATMs. ATM login process based on finger vein, which equipped with finger vein recognition technology can identify human finger vein during transaction. ATMs automatically remind the cardholder to be alert when there are "shoulder surfers" who try to peak over the cardholder's shoulder when the cardholder enters the PIN. The use of finger vein authentication enables to offer advanced transactions at its ATMs because finger vein authentication provides additional security to the cardholder and the bank. Bank customers are not limited to the accounts associated with their ATM card; they can access their accounts at the ATM using their debit / credit card. With finger vein authorization, the Bank can assure

the most stringent security with the convenience of open banking service to its customers. This procedure utilized by the bank is to capture the customers face imagery at the branch of bank, then save the images in a secured biometric database. The deep finger vein activates the biometric software provided by the deep learning model when the customer taps his ID card or inserts his bank card in the ATM. The system captures multi finger vein imageries as well as find out the best image to be utilized for recognition. If nothing is deemed appropriate, the customer will be motivated to approach closer, or do whatever is necessary to capture the appropriate image. Figure 1 shows the Block diagram for EESNN-GWO-AMT-FV method.

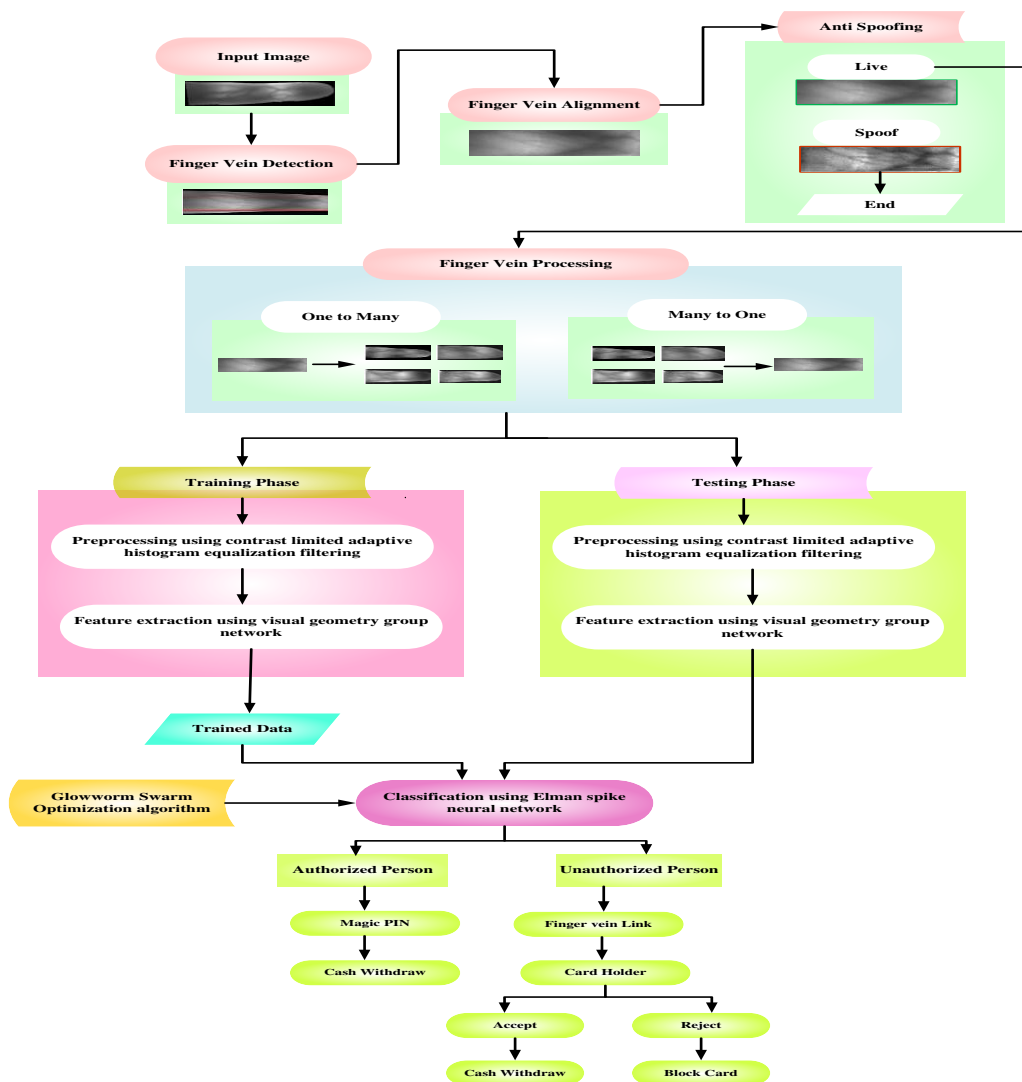


Figure 1: Block diagram for EESNN-GWO-AMT-FV method

3.1 Image acquisition

Here, the datas are gathered via SDUMLA-HMT dataset. This dataset comprise 3816 finger vein imageries that are captured via the device. This is generated by Intelligent Computing and Intelligent Systems of Wuhan University.

3.2. Pre-processing using contrast limited adaptive histogram equalization filtering (CLAHEF)

CLAHEF technique is utilized for improving the image quality and remove noise from input finger vein imageries. It has the ability to filter the small areas of the images and provides good outcome by removing noises. By using CLAHE technique, the images are pre-processed using equation (1),

$$CLAHEF_{Preprocessing} = \frac{Processed_{image}}{Original_{image}} \quad (1)$$

Where $Processed_{image}$ and $Original_{image}$ are represented as the contrast values images that are pre-processed and the original image for removing the noises from finger vein images. The contrasts in the noise removed images and improve the image quality are enhanced using equation (2),

$$contrast = \frac{graylevel_{value\ of\ image}}{background_{value\ of\ image}} \quad (2)$$

In this way, the input image noises are removed and the contrasts of the images are enhanced.

3.3.Feature extraction using visual geometry group network (VGG16) method

In feature extraction stage, pre-processed images are extracted using Visual geometry group network (VGG16). Visual geometry group network (VGG16) is one of the types of CNN model. To attain the feature map, convolutional layers are utilized for convolving the

preprocessed image by means of kernel weight. The kernel weight is connected with the feature map units of preceding layer. VGG16 contains twenty three layers with weights. The initial layer is convolutional layer used for pre-processing and it reduces the preprocessed image size by removing soft tissues. Next, the pre-processed image size is decreased to $227 \times 227 \times 3$. Thus, the feature extraction using convolution layer equation is given in equation (3).

$$Conv_{MRI\ database}(MD) = \{X_i; 1 \leq i \leq L\} \quad (3)$$

Here, X_i specifies the i^{th} vein image from database MD , $Conv$ is represented as the convolutional layer, L specifies the count of vein present in the database. Then, the pre-processed images are given to the trainable VGG16 for extracting the image features for detecting the finger vein images. The next layers in VGG16 are utilized to extract image features for detecting the vein region. Also, the Next layers are 2 convolutional layer, 2 ReLU, 2 cross channel normalization (Norm), and 2 max-pooling layers. Layer two and six are convolutional layer with $11 \times 11 \times 3$ and $5 \times 5 \times 48$ convolution. In this, the input pre-processed image is represented as a , weight is represented as W and the integer variables are represented as y . Thus, the output of 2D discrete convolution equation is specified in equation (4).

$$h(j,i) = a(j,i) * W(j,i) = \sum_f \sum_d a(f,d) W(j-f, i-d) \quad (4)$$

Where, h is represented as the output of convolution layer, W, a are represented as preprocessed inputs from the previous layer with weights, f, d are represented as the size of the convolution matrix, j, i are represented as i^{th} and j^{th} finger vein image from database MD , $*$ is represented as the activation function. Then, the output of this layer that is layers 2 and 6 apply activation function from attained convolutional output h . The next layer is ReLU

layer, that is, layer 3 and layer 7 is linear activation function to the neuron output is expressed in equation (5),

$$s(h) = \frac{1}{1 + e^{-h}} \quad (5)$$

Next, the layer four and eight are the cross-channel Norm layer with five channels. Layer five and layer nine contains 3×3 max-pooling layer. Here, max-pooling layer is utilized for down sampling process that lessens the over fitting problem through the classification method. By this process, features are extracted, number of finger vein images by detecting the unauthorized person is represented as $L \times L$ and then the output is represented as the $\frac{M}{L} \times \frac{M}{L}$, then layer 9 gives the extracted features in 1×43264 dimension. By using this, finger vein image features are extracted, such as Vein Patterns, Local Binary Patterns, Dimensionality Reduction and Image Transformations.

Vein Patterns are extracted through these images categories. In several cases, topological or curvature information of the veins on the basis of preprocessing steps for higher degree, because the veins are in the binary image and better performance of every method. The feature extracted from vein patterns are given in equation (6)

$$V_{Pattern} = \min_{\{h(L(h))=0\}} f(j, i) \quad j, i \in \beta \quad (6)$$

Where f represents the normalization of finger vein image and β denotes the image thinning. Texture features are used to extract Local Binary Patterns, Dimensionality Reduction and Image Transformations features from the input preprocessed finger vein image to detect the spoofing attacks in fingerprint recognition.

Local Binary Patterns (LBP) extracting the region of interest for finger vein, and extract the LBP images. As an alternative, the histogram image is considered for matching process at certain cases. LBP is calculated by utilizing the pixel intensity along neighbor's input pre-processed image and it is expressed in equation (7).

$$LB_{pattern} = \sum_{i=0}^{f-1} \sum_{j=0}^{d-1} (i-j)^2 f(i-j) \quad (7)$$

Where, i, j specifies the input pre-processed image, $f(i-j)$ specifies the image of feature extraction.

Dimensionality Reduction decreases the feature vector to any desired length resulting this type of feature extraction acquire better outcomes. Generally, these methods combined with the matching function for classification and obtaining adequate outcomes. Moreover, dimensionality reductions are deployed with other types of feature extraction methods. This expressed in equation (8).

$$DR = \sqrt{\sum_{i=0}^{j-1} \sum_{j=0}^{i-1} f^2(i, j)} \quad (8)$$

Image Transformations after extracting the region of interest of finger vein utilizing image transformation filters and classifier-base prediction model. Hence, it is expressed in equation (9).

$$IT = \frac{\sum_{i=0}^{f-1} \sum_{j=0}^{d-1} (i-j)^2 f(i-j) - M_i M_j}{\sigma_i \sigma_j} \quad (9)$$

Where $M_i M_j$ represents the rotation or scaling factors and $\sigma_i \sigma_j$ denotes the chosen transformations function. After feature extraction, trained data is applied to EESNN classifier for accurately classifying the authorized person and unauthorized person.

3.4 Classification using Enhanced Elman Spike Neural Network (EESNN)

Here, Enhanced Elman Spike Neural Network (EESNN) is utilized for classifying authorized and unauthorized person. The EESNN is modified by basic Elman NN and this is one kind of partial recurrent spike neural network model. This EESNN has 4 layers, such as input, context, invisible, output. The modified structure contains self-feedback variable that gain in the context layer and the neural network is fed with the input $f_i^{(1)}$, where $f_i^{(1)} = \omega_i^* - \omega_s$ is

considered. The input layer and hidden layer contain neurons and the control function as i_o^* .

The basic function and propagation of every layer is given to authentication purpose. The input layer with node layer is shown in equation (10),

$$a_i^{(1)}(m) = a_i^{(1)}(nt_i^{(1)}(m)) \quad i = 1 \quad (10)$$

Where $nt_i^{(1)}(m) = f_i^{(n)}(m)$ and m denotes the m^{th} iteration of spoofing attacks. $f_i^{(1)}(m)$ represents input and $a_i^{(1)}$ is represented as output of input layer. Then, hidden layer and nodes in the layer is expressed in equation (11),

$$a_j^{(2)}(m) = R(nt_j^{(2)}(m)), \quad l = 1, 2, \dots, 9 \quad (11)$$

$$nt_j^{(2)}(m) = \sum_i T_{ij} \times a_i^{(1)}(m) + \sum_l T_{lj} \times a_l^{(3)}(m) \quad j = 1, 2, \dots, 9 \quad (12)$$

Where $R(a)$ is denoted as the sigmoid function of authentication and it is shown in $R(a) = 1/(1 + e^{-a})$. Therefore, $a_i^{(1)}(m)$ and $a_l^{(3)}(m)$ are the input and $a_j^{(2)}(m)$ is the output of hidden layer. Additional T_{ij} and T_{lj} represents the neurons connecting weights from input layer to hidden layer and neurons connecting weights from context layer to hidden layer. Then, the context layer is shown in equation (13)

$$a_l^{(3)}(m) = \beta a_l^{(3)}(m-1) + a_j^{(2)}(m-1) \quad (13)$$

Where, β represents self-connecting feedback gain contains $0 \leq \beta \leq 1$. Then, the output layer is shown in equation (14) as given below,

$$b_k^{(4)}(m) = e_k^{(4)}(nt_k^{(4)}(m)) \quad (14)$$

Where, $nt_k^{(4)}(m) = i_o^*$ then i_o^* represents the control function and $nt_k^{(4)}(m)$ is shown in equation (15)

$$nt_k^{(4)}(m) = \sum_j T_{jk} \times a_j^{(2)}(m) \quad (15)$$

$b_k^{(4)}(m)$ is represented as output and control parameter of multiple transaction controller, then,

T_{jk} denotes connecting weights of neurons in hidden layer to the output layer.

The parameters of EESNN utilizing the chain rule of its learning mode. Firstly, every layer is computed and applied by chain rule. The purpose of training process is to lessen the overall authentication is denoted as F . Hence, it is shown in equation (16)

$$F = \frac{1}{2}(\omega_s^* - \omega_s)^2 = \frac{1}{2}f^2 \quad (16)$$

Where, f represents the error rate, ω_s^* and ω_s denotes the detection speed. The chain rule of EESNN is delineated below, Updates the weight parameters of output layer on T_{jk} then the error term are calculated and it classify authorized person and unauthorized person as equation (17),

$$\delta_1 = -\frac{\partial F}{\partial nt_k^{(4)}} = \left[-\frac{\partial F}{\partial b_k^{(4)}} \frac{\partial b_k^{(4)}}{\partial nt_k^{(4)}} \right] \quad (17)$$

Then, the weight T_{jk} is adjusted by equation (18),

$$\nabla T_{jk} = -\frac{\partial F}{\partial T_{jk}} = \left[-\frac{\partial F}{\partial b_k^{(4)}} \frac{\partial b_k^{(4)}}{\partial nt_k^{(4)}} \right] \left(\frac{\partial nt_k^{(4)}}{\partial T_{jk}} \right) = \delta_1 T_{jk} a_j^{(2)} [1 - a_j^{(2)}] a_l^{(3)} \quad (18)$$

Where δ_1 represents the detection layer and it is updated using equation (19),

$$T_{jk}(m+1) = T_{jk}(m) + \xi_1 \nabla T_{jk} \quad (19)$$

Where ξ_1 represents the training rate of layer four. Update the weight parameters of invisible layer in T_{lj} , then the training pattern of weight T_{lj} is adjusted using equation (20)

$$\nabla T_{lj} = -\frac{\partial F}{\partial T_{lj}} = \left[-\frac{\partial F}{\partial b_k^{(4)}} \frac{\partial b_k^{(4)}}{\partial nt_k^{(4)}} \right] \left(\frac{\partial nt_k^{(4)}}{\partial a_j^{(2)}} \frac{\partial a_j^{(2)}}{\partial T_{lj}} \right) = \delta_1 T_{jk} a_j^{(2)} [1 - a_j^{(2)}] a_l^{(1)} \quad (20)$$

Next, the connecting weight T_{lj} is updated using equation (21)

$$T_{lj}(m+1) = T_{lj}(m) + \xi_3 \nabla T_{lj} \quad (21)$$

Where, ξ_3 denotes the training rate of the context layer. EESNN layer related to accuracy as well as count of assessed flows per sec. Several cells are included with EESNN layer for greater classification result. EESNN attains balanced tradeoff amid the accuracy and flow throughput. By this, the enhanced Elman spike neural network is used to classify the authorized person and unauthorized person. To get more accurate evaluation of authentication, weight parameters ∂F , T_{jk} and ω_s^* are optimized using Glowworm Swarm Optimization Algorithm (GWO). The Glowworm Swarm Optimization Algorithm are explained below,

3.5 Step by step procedure of Glowworm Swarm Optimization Algorithm for optimizing EESNN

Glowworm Swarm Optimization Algorithm (GWO) is employed to optimize the parameters of enhanced Elman spike neural network (EESNN) for obtaining optimum parameters. These parameters have optimized for computing the optimal parameters for assuring accurate classification of authentication in multiple transactions. GWO is determined as the swarm cognizance in the fact of illustrating and conducting the glowworms. It is totally dependent on the prospects of variation intensity associated with the glowworms, and in this manner the glows are explored at various levels. In Glowworm Swarm Optimization, the glowworm clustering is being approximated seeded over the space of search. Luciferin is determined as the quantity of luminescence instructed by the glowworms. The maximal peak luciferin value converses with the peak values of fitness functions and the better state are its current area. The attraction of glowworm is made by its sparkling neighbor within its vector space. The step-by-step process of GWO are described below,

Step 1: Initialization

Initially, all the glowworms carry an equal luciferin level randomly based on the lower and upper bounds of the production power of glowworm and control parameters. The initial population of glowworm is expressed in equation (22),

$$I = \frac{Q_s}{4\pi d^2} \quad (22)$$

Where, Q_s and d denotes the lower and upper bound of the parameter.

Step 2: Random Generation

After the process of initialization, the input parameters are generated randomly. Here, the highest fitness values are selected depends on accurate hyper-parameter context. Generate randomly the population of procedure value for the accurate prediction of authentication in multiple transactions.

Step 3: Fitness Function

This is assessed to reach the objective function that is accurate prediction of authentication in multiple transactions as well as reach the optimum value. The weight parameters of EESNN classifier ∂F , T_{jk} and ω_s^* have been optimized by Glowworm Swarm Optimization (GWO) approach. It is expressed mathematically in equation (23),

$$Fitness = optimization[\partial F, T_{jk} \text{ and } \omega_s^*] \quad (23)$$

Step 4: Update luciferin value to optimize the weight parameter ∂F

In GWO, each glowworm may update its position by improved via predetermined count of trials, specified by the user of GWO algorithm. Hence the position updation of glowworm is expressed in equation (24),

$$\gamma_i^g = d * Tansig\left(1 - \frac{g}{g_{\max}}\right) \eta_i \quad (24)$$

Where, d is a random number of a normal distribution in $[0,3]$, $Tansig$ represents the tangent sigmoid functions, g indicates the number of the current iteration and $g_{\max}$ is the maximum number of iteration.

Step 6: Update luciferin volume to optimize the weight parameter T_{jk}

The luciferin volume is updated to optimize the weight parameter T_{jk} . Exploration of glowworm for better solutions are obtained by equation (25),

$$\beta = \frac{1}{1 + NI_j^i} \quad (25)$$

Where, β denotes the randomly selected position j for glowworm i and NI_j^i represents the new source. Figure 2 shows the flowchart for Glowworm Swarm Optimization Algorithm for optimizing EESNN.

Step 7: Perform mutation operation to optimize the weight parameter ω_s^*

In GWO, the mutation operation performed is with respect to probability values using the fitness values provided by glowworm. To this intention, a fitness based selection technique is used. It is obtained using equation (26),

$$N(M) = \left\{ R \left(\frac{S}{2} * \left(1 - \frac{g}{g_{\max}} \right) \right) + 1 \right\} \quad (26)$$

Where, the training data of EESNN for classifying the authorized and unauthorized person expressed as $N(M)$, g expresses the current iteration number, moreover $g_{\max}$ denotes the best optimal locations, S indicates the maximum number of iterations and R denotes the round.

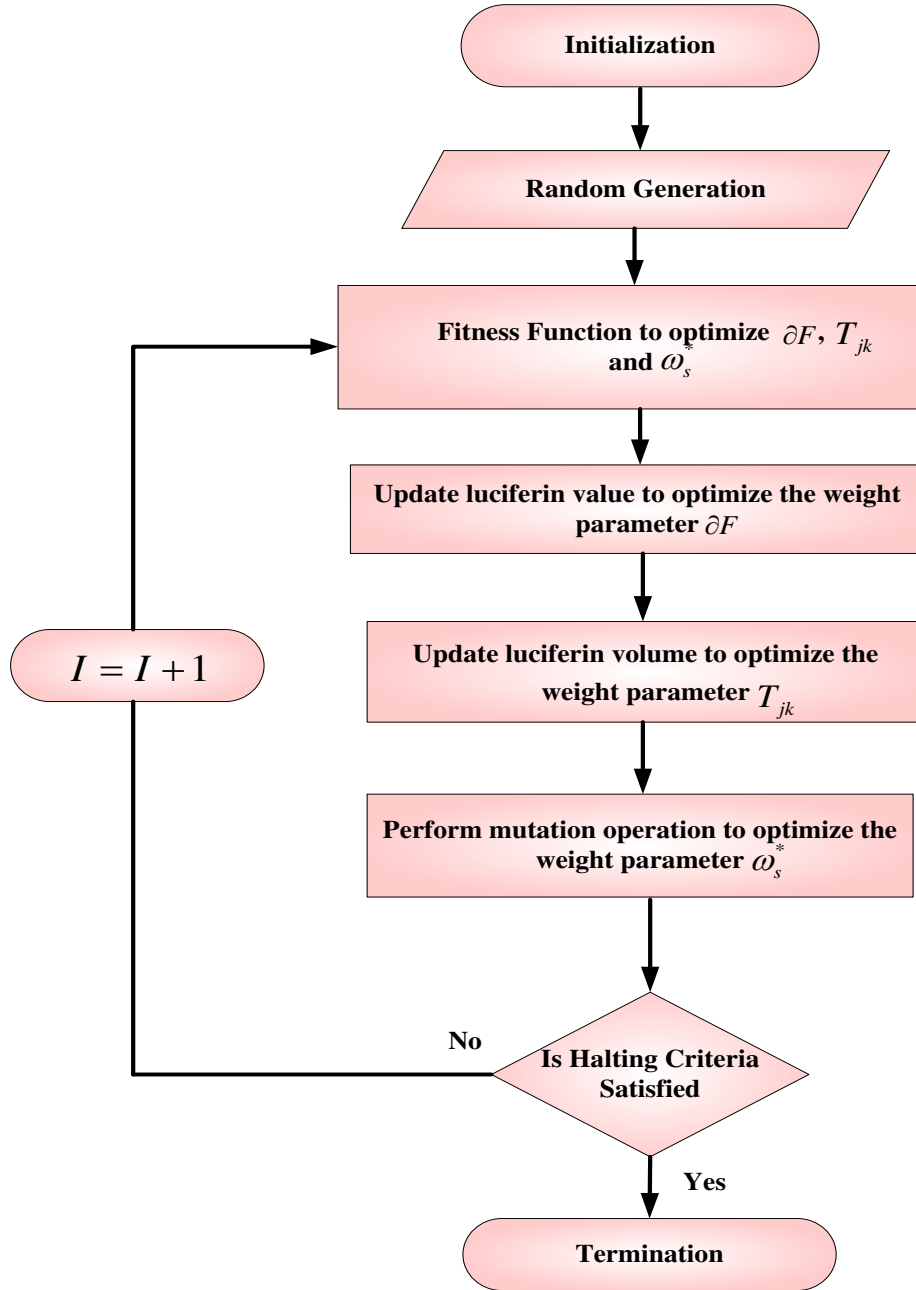


Figure 2: Flowchart for Glowworm Swarm Optimization Algorithm for optimizing EESNN

Step 8: Termination Condition

Here, the optimum hyper-parameter ∂F , T_{jk} and ω_s^* are chosen in enhanced Elman spike neural network with the help of Glowworm Swarm Optimization Algorithm (GWO), will iteratively repeat the step 3 until the halting criteria $I = I + 1$ is met. Then finally EESNN predicts the authentication purpose with higher accuracy by lessening the error by using Glowworm Swarm Optimization Algorithm.

The capturing image is forward to the biometric processing scheme, then it is likened to the customer's image saved in bank's ID database. The customer can access their accounts and make authorized transactions once verified. If it is not verified, the ATM camera captures the user's face image. The bank account holder needs an internet friendly mobile communication device that can be accessed 24/7 sites to handle remote certification. Certification and authentication processes for multimedia messaging services (MMS) require robust Internet and GSM networks. Many anti-fraud measures are structured to add to its security in the system. The infrared lens is to capture additional facial details to prevent fraudulent attempts.

4. Result and Discussion

In this section, the experimental result is discussed for Enhanced Elman Spike Neural Network Optimized with Glowworm Swarm Optimization for authentication of multiple transactions using finger vein. The setup for authentication of multiple transactions using finger vein consists of a PIC microcontroller, Power supply, Personal computer with MATLAB software, Keypad, Finger vein Detection module and an LCD display. The proposed EESNN-GWO-AMT-FV method is simulated with MATLAB utilizing SDUMLA-HMT dataset. The performance metrics, such as, accuracy, specificity, sensitivity, precision, Error rate and AUC are analyzed. The proposed EESNN-GWO-AMT-FV method is compared with the existing methods, like deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits (CNN-AOA-MBR-FV) [21], multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion (CNN-MBR-FKP-FV) [22] and biometric authentication using finger-vein patterns with deep-learning and discriminant correlation analysis (DCNN-MBR-FV) [23] respectively.

4.1 Dataset description

Here, the data are gathered via SDUMLA-HMT dataset. This is a multimode biometrics dataset, developed by a set of deep learning as well as applications in Shandong University. It saves a range of biometric data through 106 people. Wherein, 61 males and 45 females among 17 and 31 age. The dataset has five biometric traits for each subject. Also, it contains 3816 finger vein imageries are captured through the device developed by Intelligent Computing and Intelligent Systems. At the process of capturing, various imageries of index, middle and ring fingers of both hands are taken for each subject. Each subject provide images and the collection for each of the 6 fingers is repeated for 6 times to obtain 6 finger vein images. Every image is stored in “bmp” format with 320×240 pixels in size. The total size of finger vein database is around 0.85G Bytes.

4.2 Performance measures

This section describes the performance measures needed for experiment. The performance metrics is a significant role for the authentication of multiple transactions using finger vein. To authenticate the performance, the most common performance measures, like accuracy, specificity, sensitivity, precision, Error rate and AUC are analyzed. For estimating the performance metrics, the confusion matrix is required. For measuring the confusion matrix, True Positive, True Negative, False Positive, False Negative values are considered.

- True Positive (TP): Unauthorized person is properly recognized into unauthorized person.
- True Negative (TN): Authorized person is properly recognized into Authorized person.
- False Positive (FP): Authorized person is properly recognized into unauthorized person.
- False Negative (FN): unauthorized person is properly recognized into authorized person.

4.2.1 Accuracy

This is computed by,

$$Accuracy = \frac{(TP + TN)}{(TP + FP + TN + FN)} \quad (27)$$

4.2.2 Specificity

This is computed by,

$$Specificity = \frac{TN}{(FP + TN)} \quad (28)$$

4.2.3 Sensitivity

This is nothing but recall or detection rate, it is computed utilizing the given equation,

$$Sensitivity = \frac{TP}{(TP + FN)} \quad (29)$$

4.2.4 Precision

This is determined by,

$$Precision = \frac{TP}{(TP + FP)} \quad (30)$$

4.2.5 AUC

This is determined by,

$$AUC = 0.5 \times \left(\frac{TP}{TP + FN} + \frac{TN}{TN + FP} \right) \quad (31)$$

4.3 Performance Analysis

Figure 3-7 shows the simulation results of the Enhanced Elman Spike Neural Network Optimized with Glowworm Swarm Optimization for authentication of multiple transactions using finger vein. The performance metrics, like accuracy, specificity, sensitivity, precision, error rate and AUC are examined. The performance of proposed EESNN-GWO-AMT-FV method is analyzed with the existing methods, like CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV respectively.

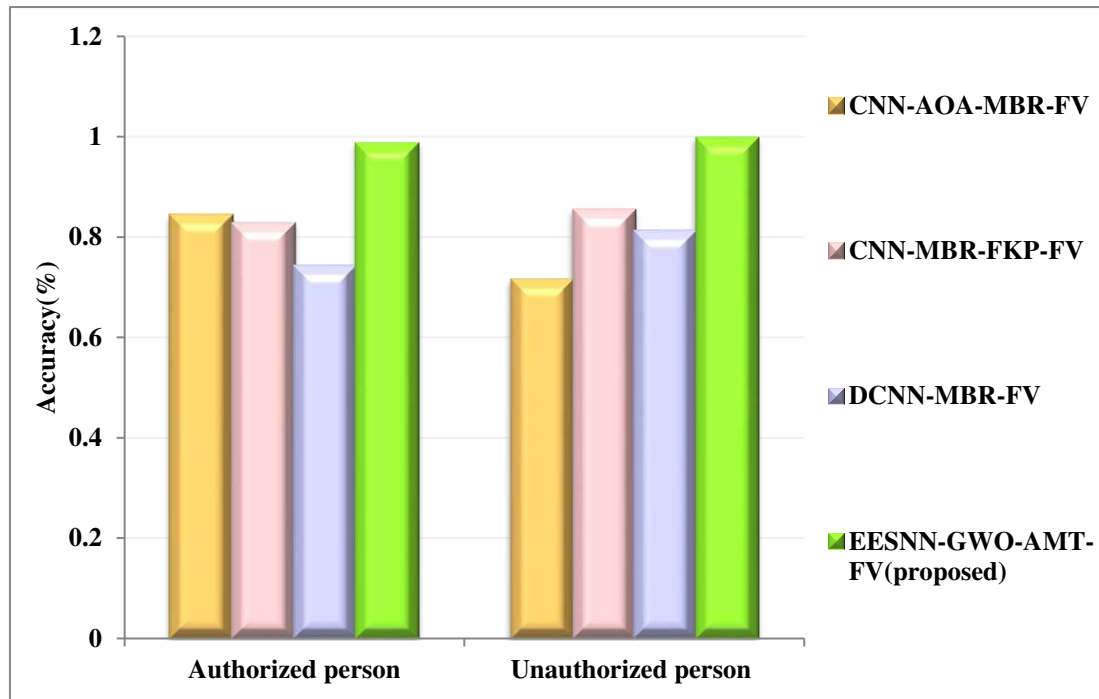


Figure 3: Performance analysis of Accuracy with various methods

In Figure 3, the performance of the proposed EESNN-GWO-AMT-FV method is compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively. For authorized person, the proposed EESNN-GWO-AMT-FV method provides 16.66%, 19.51% and 21.03% better accuracy compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively. For unauthorized person, the proposed EESNN-GWO-AMT-FV method provides 15.988%, 14.542% and 12.478% better accuracy compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively.

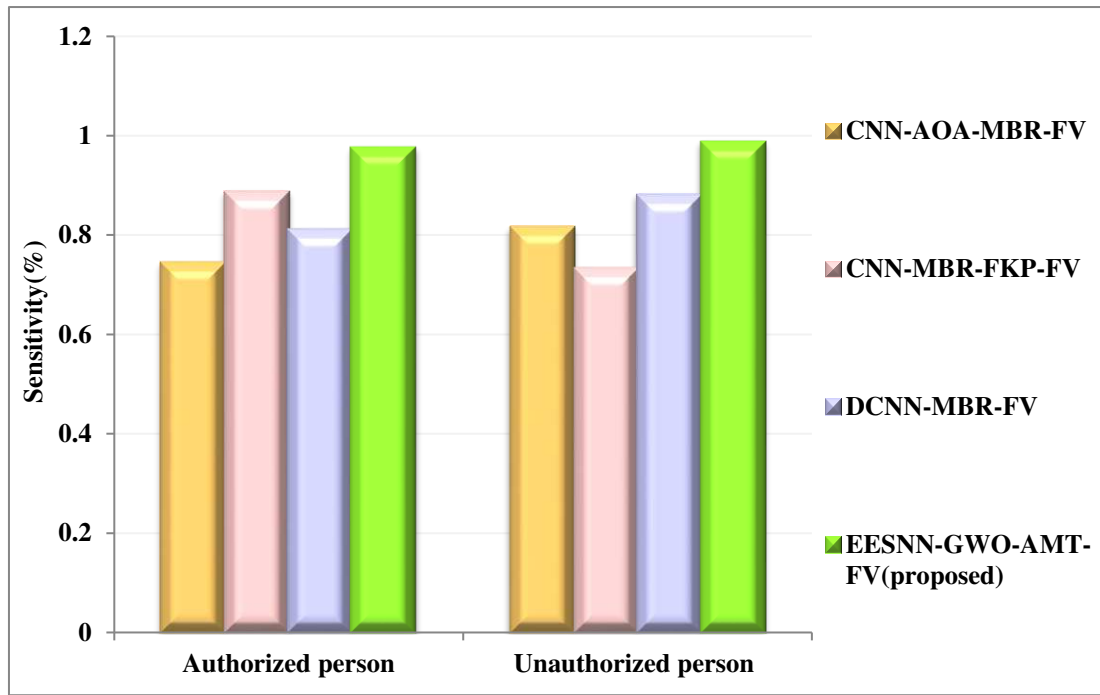


Figure 4: Performance analysis of Sensitivity with various methods

In Figure 4, the performance of the proposed EESNN-GWO-AMT-FV model is compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods. For authorized person, the proposed EESNN-GWO-AMT-FV method provides 14.913%, 16.056% and 15.812% better sensitivity compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively. For unauthorized person, the proposed EESNN-GWO-AMT-FV method provides 18.22%, 10.3% and 14.84% better sensitivity compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively.

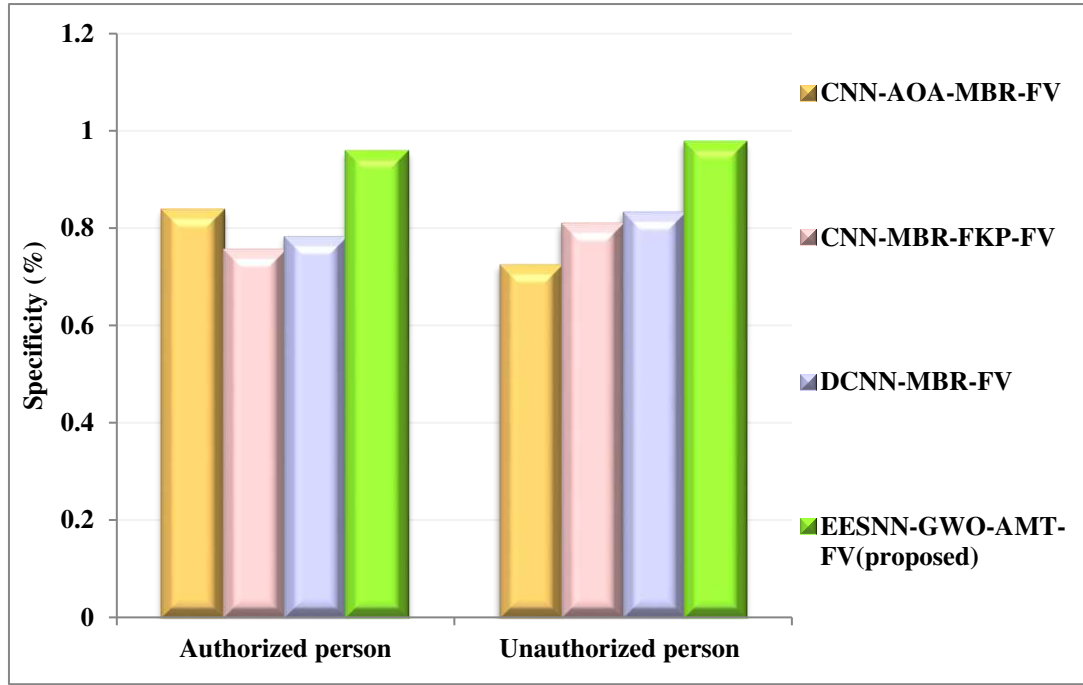


Figure 5: Performance analysis of Specificity with various methods

In Figure 5, the performance of the proposed EESNN-GWO-AMT-FV model is compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods. For authorized person, the proposed EESNN-GWO-AMT-FV method provides 14.26%, 13.47% and 20.31% better specificity compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively. For unauthorized person, the proposed EESNN-GWO-AMT-FV method provides 16.3%, 11.37% and 15.29% better specificity compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively.

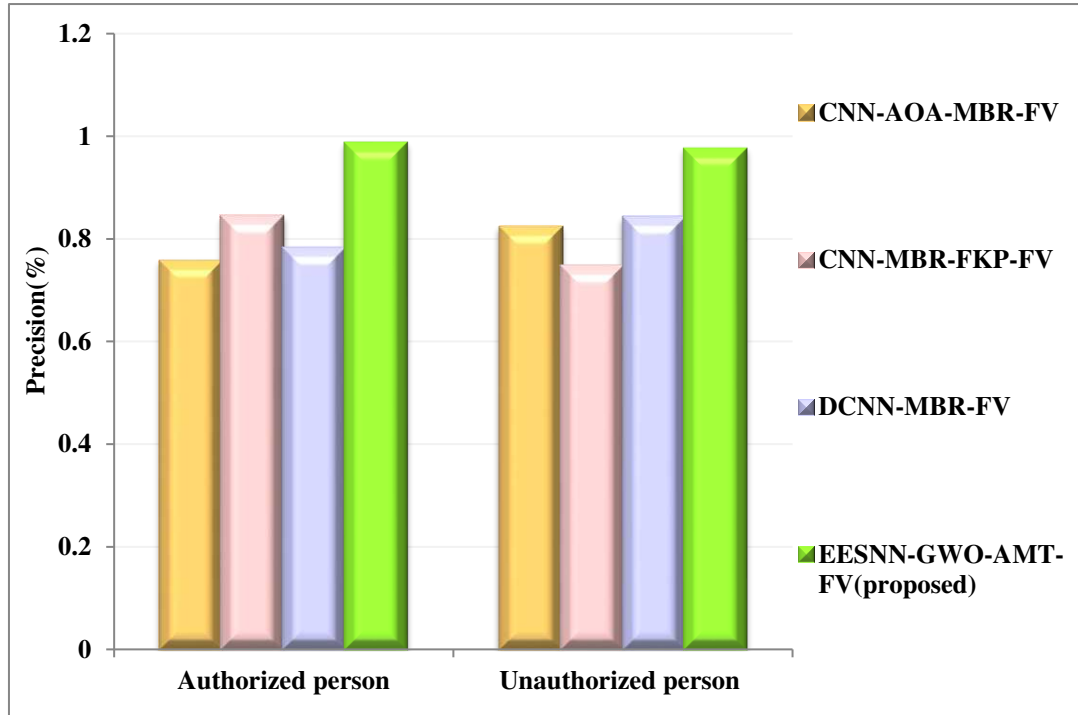


Figure 6: Performance analysis of Precision with various methods

In Figure 6, the performance of proposed EESNN-GWO-AMT-FV method is compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods. For authorized person, the proposed EESNN-GWO-AMT-FV method provides 9.36%, 11.75% and 22.13% better precision compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively. For unauthorized person, the proposed EESNN-GWO-AMT-FV method provides 16.02%, 10.84%, 11.6% better precision compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods.

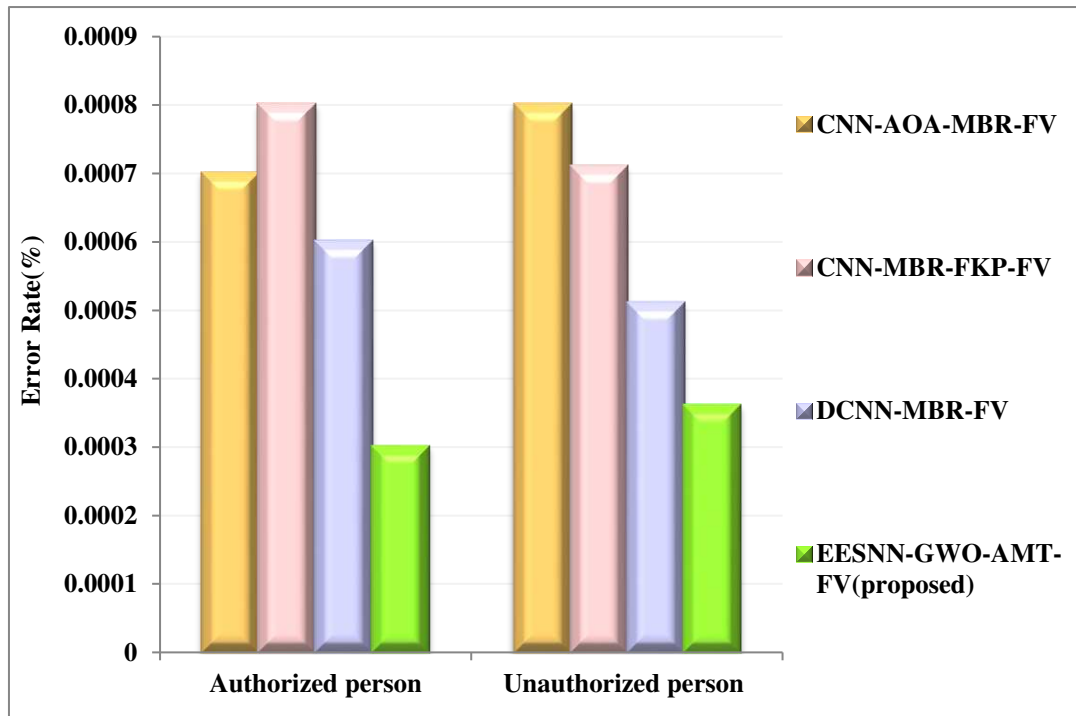


Figure 7: Performance analysis of Error Rate with various methods

In Figure 7, the performance of proposed EESNN-GWO-AMT-FV model is compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods. For authorized person, the proposed EESNN-GWO-AMT-FV method provides 33.33%, 60.32% and 63.66% lower error rate compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively. For unauthorized person, the proposed EESNN-GWO-AMT-FV method provides 44.41%, 50.03% and 54.55% lower error rate compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively.

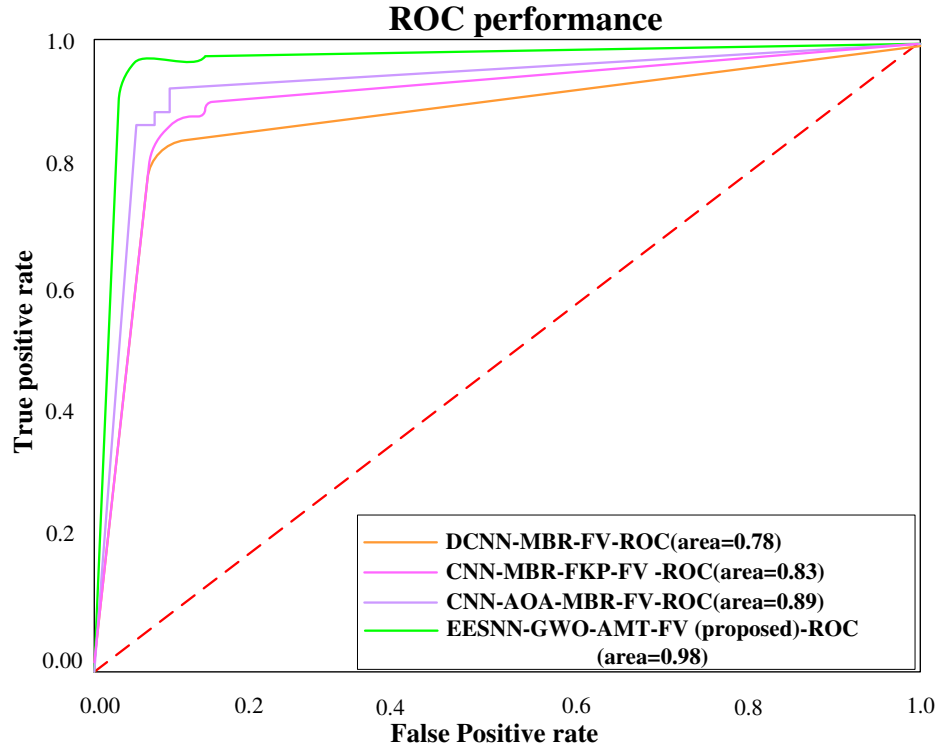


Figure 8: ROC curve for multiple transaction authentications

Figure 8 depicts ROC curve for multiple transaction authentication. Then, ROC of proposed EESNN-GWO-AMT-FV method provides 2.89%, 6.59%, and 6.34% greater AUC than the existing methods, CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV respectively. Figure 9 depicts Screen for getting input from user.

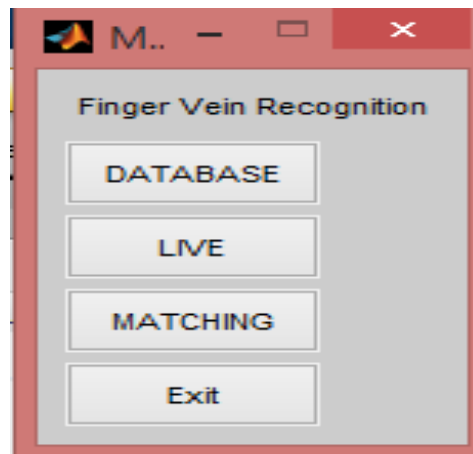


Figure 9: Screen for getting input from user

After entering the vein, it processed and a message box will be displayed, which intimate that the authentication is passed. Figure 10 depicts Screen displaying whether the authentication is passed or not.

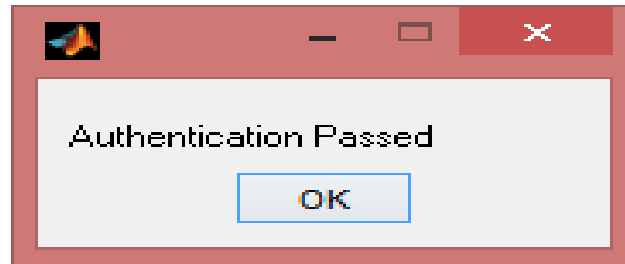


Figure 10: Screen displaying whether the authentication is passed or not

Then the finger vein is compared with the matching unit for authentication and recognition of the user for further accessing process. The matching process is done by comparing it with the finger vein which is already stored in the database during the time of account initiation. If it matches, then the user is identified as an authorized user. Figure 11 depicts (a) Image of the Vein Stored in database, (b) image of the vein when entered during accessing.



Figure 11: (a) Image of the Vein Stored in database, (b) image of the vein when entered during accessing

Then the user is allowed to access his/her multiple account by entering the two digit pin number using the keypad. Otherwise, message box with an authorized user is displayed, if the user's vein is not matched.

5. Conclusion

An Enhanced Elman Spike Neural Network Optimized with Glowworm Swarm Optimization is successfully implemented in this manuscript for Authentication of Multiple Transaction Using Finger Vein. The simulation process is done in MATLAB environment and the performance is examined under performance metrics. Therefore, the performance of the proposed EESNN-GWO-AMT-FV method attains higher sensitivity 93.76%, 92.82% and 95.87%, higher specificity 96.87%, 95.08% and 97.98% compared to the existing CNN-AOA-MBR-FV, CNN-MBR-FKP-FV and DCNN-MBR-FV methods respectively.

Compliance with Ethical Standards

Data availability statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Funding Information:

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Ethical approval:

This article does not contain any studies with human participants performed by any of the authors.

Declaration of interest Statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

Materials and Methods: Not applicable

Conflicts of interest: Authors declare that they have no conflict of interest.

Code availability: Not applicable

Consent to participate: Not applicable

Availability of data and material: Not Applicable

Acknowledgement: None

References

- [1] Wagh, D.P., Fadewar, H.S. & Shinde, G.N., (2020). Biometric finger vein recognition methods for authentication. *In Computing in engineering and technology* (pp. 45-53). Springer, Singapore.
- [2] Mohsin, A.H., Zaidan, A.A., Zaidan, B.B., Albahri, O.S., Ariffin, S.A.B., Alemran, A., Enaizan, O., Shareef, A.H., Jasim, A.N., Jalood, N.S. & Baqer, M.J., (2020). Finger vein biometrics: taxonomy analysis, open challenges, future directions, and recommended solution for decentralised network architectures. *Ieee Access*, 8, pp.9821-9845.
- [3] Kirchgasser, S., Kauba, C., Lai, Y.L., Zhe, J. & Uhl, A., (2020). Finger vein template protection based on alignment-robust feature description and index-of-maximum hashing. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2(4), pp.337-349.
- [4] Huang, J., Tu, M., Yang, W. & Kang, W., (2021). Joint Attention Network for Finger Vein Authentication. *IEEE Transactions on Instrumentation and Measurement*, 70, pp.1-11.
- [5] Shaheed, K., Mao, A., Qureshi, I., Kumar, M., Hussain, S. & Zhang, X., (2022). Recent advancements in finger vein recognition technology: Methodology, challenges and opportunities. *Information Fusion*, 79, pp.84-109.

- [6] Sidiropoulos, G.K., Kiratsa, P., Chatzipetrou, P. & Papakostas, G.A., (2021). Feature Extraction for Finger-Vein-Based Identity Recognition. *Journal of Imaging*, 7(5), p.89.
- [7] Shaheed, K. & Qureshi, I., (2022). A hybrid proposed image quality assessment and enhancement framework for finger vein recognition. *Multimedia Tools and Applications*, pp.1-26.
- [8] Boucherit, I., Zmirli, M.O., Hentabli, H. & Rosdi, B.A., (2020). Finger vein identification using deeply-fused Convolutional Neural Network. *Journal of King Saud University-Computer and Information Sciences*.
- [9] Huang, J., Luo, W., Yang, W., Zheng, A., Lian, F. & Kang, W., (2022). FVT: Finger Vein Transformer for Authentication. *IEEE Transactions on Instrumentation and Measurement*.
- [10] Khodadoust, J., Medina-Pérez, M.A., Monroy, R., Khodadoust, A.M. & Mirkamali, S.S., (2021). A multibiometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print. *Expert Systems with Applications*, 176, p.114687.
- [11] Zhan, Y., Rathore, A.S., Milione, G., Wang, Y., Zheng, W., Xu, W. & Xia, J., (2020). 3D finger vein biometric authentication with photoacoustic tomography. *Applied Optics*, 59(28), pp.8751-8758.
- [12] El-Rahiem, B.A., El-Samie, F.E.A. & Amin, M., (2021). Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. *Multimedia Systems*, pp.1-13.
- [13] Hu, N., Ma, H. & Zhan, T., (2020). Finger vein biometric verification using block multi-scale uniform local binary pattern features and block two-directional two-dimension principal component analysis. *Optik*, 208, p.163664.

- [14] Sujatha, E., SathiyajebaSundar, J., Deivendran, P. & Indumathi, G., (2021). Multimodal Biometric Algorithm Using IRIS, Finger Vein, Finger Print with Hybrid GA, PSO for Authentication. *In Data Analytics and Management* (pp. 267-283). Springer, Singapore.
- [15] Muthusamy, D. & Rakkimuthu, P., (2022). Steepest deep bipolar Cascade correlation for finger-vein verification. *Applied Intelligence*, 52(4), pp.3825-3845.
- [16] <https://wavelab.at/sources/Prommegger19c/>
- [17] Pour, A.M., Seyedarabi, H., Jahromi, S.H.A. & Javadzadeh, A., (2020). Automatic detection and monitoring of diabetic retinopathy using efficient convolutional neural networks and contrast limited adaptive histogram equalization. *IEEE Access*, 8, pp.136668-136673.
- [18] Jangra, M., Dhull, S.K. & Singh, K.K., (2020). ECG arrhythmia classification using modified visual geometry group network (mVGGNet). *Journal of Intelligent & Fuzzy Systems*, 38(3), pp.3151-3165.
- [19] Al-Jamali, N.A.S. & Al-Raweshidy, H.S., (2020). Modified Elman spike neural network for identification and control of dynamic system. *IEEE Access*, 8, pp.61246-61254.
- [20] Chowdhury, A. & De, D., (2020). MSLG-RGWO: Movement score based limited grid-mobility approach using reverse glowworm swarm optimization algorithm for mobile wireless sensor networks. *Ad Hoc Networks*, 106, p.102191.
- [21] Alay, N. & Al-Baity, H.H., (2020). Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. *Sensors*, 20(19), p.5523.
- [22] Daas, S., Yahi, A., Bakir, T., Sedhane, M., Boughazi, M. & Bourennane, E.B., (2020). Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion. *IET Image Processing*, 14(15), pp.3859-3868.

- [23] Boucetta, A. & Boussaad, L., (2022). Biometric authentication using finger-vein patterns with deep-learning and discriminant correlation analysis. *International Journal of Image and Graphics*, 22(01), p.2250013.
- [24] Shaheed, K., Mao, A., Qureshi, I., Abbas, Q., Kumar, M. & Zhang, X., (2022). Finger-vein presentation attack detection using depthwise separable convolution neural network. *Expert Systems with Applications*, 198, p.116786.
- [25] Yang, W., Luo, W., Kang, W., Huang, Z. & Wu, Q., (2020). Fvras-net: An embedded finger-vein recognition and antispoofing system using a unified cnn. *IEEE Transactions on Instrumentation and Measurement*, 69(11), pp.8690-8701.-
- [26] Shahreza, H.O. & Marcel, S., (2021). Towards protecting and enhancing vascular biometric recognition methods via biohashing and deep neural networks. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 3(3), pp.394-404.
- [27] Heidari, H. & Chalechale, A., (2022). Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail. *Expert Systems with Applications*, 191, p.116278