An Intelligent System for Fingerprint Recognition and Verification Using Dilated Convolutional Neural Network and Extreme Learning Machine

N.Suresh Babu[1], Dr.M.Elamparithi[2], Dr.V.Anuratha[2]

[1] Research Scholar, Department of Computer Science, Kamalam College of Arts and Science, Anthiyur, Bharathiar University, Coimbatore, Tamilnadu, India

[2]Associate Professor, Department of Computer Science, Kamalam College of Arts and Science, Anthiyur, Bharathiar University, Coimbatore, Tamilnadu, India

Abstract: Several applications currently utilize fingerprint-based user recognition and authentication, but obtaining complete accuracy (eliminating false matches) is still challenging. Prior to feature extraction, improper image alignment was one of the causes of this problem. This paper proposes a novel fingerprint recognition and verification system using a dilated convolutional neural network (DICNN) and a weighted and bias-optimized extreme learning machine (WBELM). Image preprocessing, feature extraction, and fingerprint recognition are the main phases of the proposed work. To begin, image preprocessing is performed using bilateral filtering to suppress the noise in the gathered images. After that, the proposed system uses DICNN to extract features from the preprocessed images. From the extracted features, fingerprint recognition is done using WBELM. This study conducted experiments on the publicly available FVC 2004 dataset. The proposed model achieves 98.54 percent recognition accuracy with an elapsed time of 584 ms.

Keywords: Fingerprint Recognition, Verification, Noise Removal, Feature Extraction, Fingerprint Matching, Deep Learning, and Machine Learning.

1. INTRODUCTION

Modern human civilization is expanding quickly, which has increased the need for innovative and effective technology to support it. Using highly trustworthy and widely available individual authentication and identity mechanisms became essential as security and privacy concerns surfaced [1]. The most common type of authentication relies on knowledge-based procedures, such as usernames and passwords, personal identification numbers that contain digits, and pattern locks. However, these authentication mechanisms are insecure because they are vulnerable to brute force, shoulder-surfing, and password-guessing attacks. It has been demonstrated that fingerprint feature-based user authentication overcomes the drawbacks of knowledge-based systems [2]. Due to their uniqueness and immutability, fingerprints are primarily used and recognized for personal identification [3]. This technology, in the form of a password, is used by smartphones and laptops to unlock the screen. It is employed in residential systems for timekeeping and attendance. However, the fingerprint-based biometric technology is only partially secure. An issue with biometric security makes recognizing people incorrectly or not at all possible. The vulnerability notion covers strategies for mistakenly accepting a person's influence on a system's performance or attacking another system using leaked data [4]. Therefore, attackers' top priority is accurately recognizing fingerprints [5]. The fingerprint authentication system aims to achieve rapid and accurate detection [6].

Machine learning (ML) and deep learning (DL) methods are widely used to recognize fingerprints. K-nearest neighbour (KNN), decision trees (DT), and multiclass support vector machines (SVM) are a few ML techniques that are used because they can give classification results with high accuracy. Additionally, several computer vision, audio recognition, and natural language processing tasks have seen state-of-the-art results in recent years thanks to DL-based models [7]. These models are a logical fit for the ever-expanding range of fingerprint or biometric identification concerns, from mobile authentication to airport security systems [8]. The ability of DL to extract local and global structures from images is very significant. As a result, it might offer improved prediction performance [9, 10] since it gives a greater level of feature abstraction. This study combines DL and ML for feature extraction from

fingerprint images and fingerprint image recognition based on the benefits of ML and DL. The following is a list of the paper's main contributions:

- The proposed system uses bilateral filtering to remove the noise from the collected images.
- The proposed system uses DICNN to extract the features from the pre-processed image. Dilated convolution can shift the receptive field to collect more distinct information.
- Also, the proposed system uses WBELM to recognize the fingerprint image, in which WOA optimizes the weight and bias to improve the recognition rate.

The remaining part of the paper is organized accordingly. The related work is summarized in Section 2. Section 3 presents a brief explanation of the proposed methodology. Section 4 investigates the performance of the proposed work with existing methods, and Section 5 provides a conclusion and future research.

2. RELATED WORK

Pradeep N. R. and Ravi J [11] presented a dual-tree complex wavelet transformation (DTCWT) for fingerprint recognition. The image binarization task was initially performed as a preprocessing step, and then DTCWT was utilized to extract the features from the fingerprint images. Finally, the system applied Euclidean distance to match the images stored in the database with the final vectors of the test image. When tested on FVC 2004 DB 3_A with 32s of less processing time, the system attained better outcomes than the existing schemes. **Long the Nguyen *et al.* [12]** presented an ML model for automatic fingerprint recognition. The noise filtering of the collected data was performed initially using the Weiner filter. Then, the system carried out histogram equalization and normalization on the filtered data to reduce the non-uniform intensity effect of the images. Afterwards, the move expansion technique was utilized for segmenting the fingerprint area. The features from the segmented fingerprint were extracted manually, and finally, the features were matched with the templates in the database. The system achieved an accuracy of 97.75% for both high- and low-quality databases.

Uttam U. Deshpande *et al.* [13] suggested a scale- and rotation-invariant miniature features-based automatic latent fingerprint authentication system. The images were initially pre-processed by performing image normalization and noise removal using a Gabor filter. Then, the system utilized latent minutiae similarity and a clustered latent minutiae pattern algorithm for extracting scale and rotation-invariant minutiae features. The system achieved a maximum accuracy of 97.5% and 93.80% for the FVC2004 and NIST SD27 fingerprint databases, respectively. **Samy Bakheet *et al.* [14]** proffered a scale-invariant feature transform (SIFT) based fingerprint minutiae extraction and matching model. The system initially applied contextual filtering for image quality enhancement. Then, an adaptive version of SIFT was utilized to extract robust minutiae feature points from the enhanced fingerprint image. Finally, the system performed matching based on the Euclidean distance metric. The evaluations showed that the system attained an average equal error rate of 2.01% on FVC2004 fingerprint datasets, which was better than previous state-of-the-art methods. **Quang Nhat Tran *et al.* [15]** suggested a binary classification system for biometric authentication with a zero-knowledge proof protocol. The features of the fingerprint data were represented in a binary form initially. Following retrieving a query's features in binary format, the model used ECC to confirm the validity of the query. After the complete verification process, the support vector machine and multilayer perceptron algorithms performed the fingerprint recognition. The system achieved an average false reduction rate of 1.17% when tested on UBIRISv1, FVC2002-DB1, DB2, and DB3.

2.1 PROBLEM STATEMENT

The surveys above had their shortcomings while also producing significant findings. The design of effective feature extractors that can extract valuable information from the data is crucial for accurately detecting fingerprint data. Conventional feature extractors used to describe fingerprint data and aid in identification processes were manual or trial-and-error based. However, manual feature extraction and hand-crafted features take longer to process, resulting in slower recognition times. The suggested approach in this work uses neural networks, which have been shown to accurately and efficiently extract important characteristics and information from data. In order to successfully recognize the fingerprint, the proposed system combines ML classifiers like ELM. The system is effective and scalable since it combines DL and ML.

3. PROPOSED METHODOLOGY

Figure 1 shows the workflow of the proposed methodology. This paper proposes an intelligent fingerprint recognition and verification system using a dilated convolutional neural network and an extreme learning machine. The proposed system has three stages: preprocessing, feature extraction, and fingerprint recognition. Initially, the collected fingerprint images from the FVC 2004 database are preprocessed by Bilateral filtering. After that, the local and global fingerprint features are extracted via DICNN. Finally, the fingerprint recognition is carried out with the help of WBELM, in which WOA optimally chooses the weights and bias.

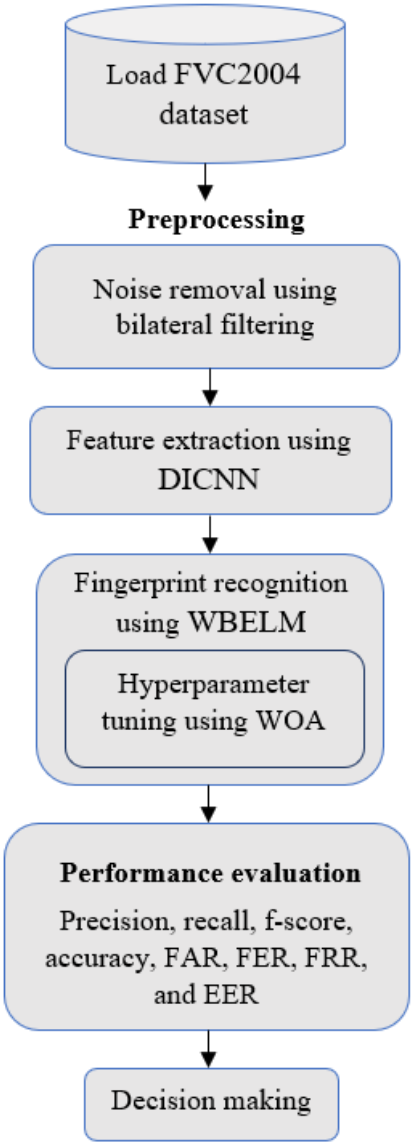

Figure 1: Workflow of the proposed methodology

3.1 Preprocessing

The input fingerprint images are initially collected from the openly available FVC2004 dataset. After that, the image preprocessing was carried out on the collected images. Developing an effective recognition or authentication system relies on preprocessing fingerprint images. The challenge is brought on by unimportant noise generated when the fingerprint is obtained online from the biometric sensor. The fingerprint images have much noise that makes the classification system challenging. So, to reduce the image's noise, this research suggests a bilateral

filtering. A non-linear, edge-preserving, and noise-reduction smoothing filter for images is known as a bilateral filter. It replaces each pixel's intensity value with the nearby pixel's weighted average of intensity values. It is mathematically described as follows:

$$\overline{\overline{NF}}_{filtered}(i) = \frac{1}{T_N} \sum_{i_a \in \Omega} \overline{\overline{NF}}(i_a) \hat{K}\hat{R}\left(\left\| \overline{\overline{NF}}(i_a) - \overline{\overline{NF}}(i) \right\| \right) \hat{G}\hat{T}\left(\|i_a - i\| \right) \quad (1)$$

$$T_N = \sum_{i_a \in \Omega} \hat{K}\hat{R}\left(\left\| \overline{\overline{NF}}(i_a) - \overline{\overline{NF}}(i) \right\| \right) \hat{G}\hat{T}\left(\|i_a - i\| \right) \quad (2)$$

Where, $\overline{\overline{NF}}_{filtered}$ indicates the noise filtered image, $\overline{\overline{NF}}$ denotes the original input fingerprint image, i refers to the current pixel's coordinates to be filtered, Ω signifies the window centered in i, so $i_a \in \Omega$ is another pixel, $\hat{K}\hat{R}$ refers to the kernel range for smoothing intensity differences (Gaussian function), $\hat{G}\hat{T}$ denotes the spatial kernel for smoothing coordinates differences, and T_N indicates the normalization term.

3.2 Feature Extraction

Once preprocessing is completed on the collected images, the feature extraction process is done in this phase. The main features used in fingerprint preprocessing are subdivided into local and global features. The local features use information that is specific to the local area. However, the secondary features use more general information that does not change due to global alteration. The type, number, and location of the singularities and the geometrical and spatial relationships of their size, ridgelines, and shape are examples of global features. The proposed work uses the preprocessed data to extract these local and global properties using a DICNN. Instead of manually extracting the precise features, as with older methods, CNN may automatically learn high-level, robust characteristics from the original image. However, some discriminant information may be lost because of the original CNN's narrower receptive field, and the data from the little item cannot be recovered and reconstructed. To enhance the performance of the low complexity network, the convolutional is proposed in the conventional CNN by replacing the convolution layers in traditional CNN with the dilated convolution layers. This technique expands the receptive field without increasing parameters. Thus, the dilated convolutional-based CNN is termed DICNN. The layers of the DICNN are explained as follows;

a) Dilated convolutional layer

The dilated convolutional layer receives the preprocessed image first. The dilated convolution, which is substantially the same as the classic convolution, was devised by raising the dilation rate to control the receptive field of convolution on the traditional convolution of CNN. In contrast to traditional convolution, dilated convolution's parameter count does not rise as the receptive field widens. The dilated convolutional layer is mathematically expressed as follows:

$$D''(x,y) = \sum_{u}^{X} \sum_{v}^{Y} \hat{P}\left(x + Rt \times u, y + Rt \times v\right) \hat{W}(u,v) \quad (3)$$

Where, $D''(x,y)$ indicates the output of dilated convolution from input $\hat{p}(x,y)$ and a filter $\hat{W}(u,v)$ with the length and the width of $\hat{W}(u,v)$ and $\hat{W}(u,v)$ respectively. The parameter Rt denotes the dilation rate. If $Rt = 1$, a dilated convolution turns into a normal convolution. Then, the obtained features from the dilated convolutional layer are passed to the max-pooling layer.

b) Max-Pooling layer

After that, the output from the dilated convolutional layers is subjected to the Max-pooling process. The term "max pooling" refers to a pooling process that chooses the most significant element from the feature map area that the

filter covers. The output of the max-pooling layer would be a feature map that included the most noticeable features from the prior feature map. Max-pooling generates the feature maps with 2*2 kernels and a stride of 2.

c) Fully connected layer

The fully connected layer finally receives the output from the max-pooling layer, which contains all the features and fuses them in a long tube for additional processing, i.e., it passes the fused features into the classifier.

3.3 Fingerprint Recognition

Finally, the fingerprint recognition is done by using the WBELM. With an input, hidden, and output layer, ELM is a three-layer classification architecture. Each layer's neurons in this architecture are fully coupled to the neurons of the layer below it, for example, input to hidden and hidden to output layers. Weights (between inputs to hidden layer), biases, and data samples are used to estimate weights between hidden and output neurons. ELM requires diminished calculation time, and its transcendent properties produce effective outcomes. However, because the neural network training process is frequently performed to improve learning performance, learning progress is plodding, and local optima are straightforward to establish due to random weights and bias. To mitigate these issues, this paper proposes a WOA to select the weights and bias of the ELM optimally. Thus, the optimal selection of weight and bias in conventional ELM is termed WBELM. The structure of the ELM is shown in Figure 2.

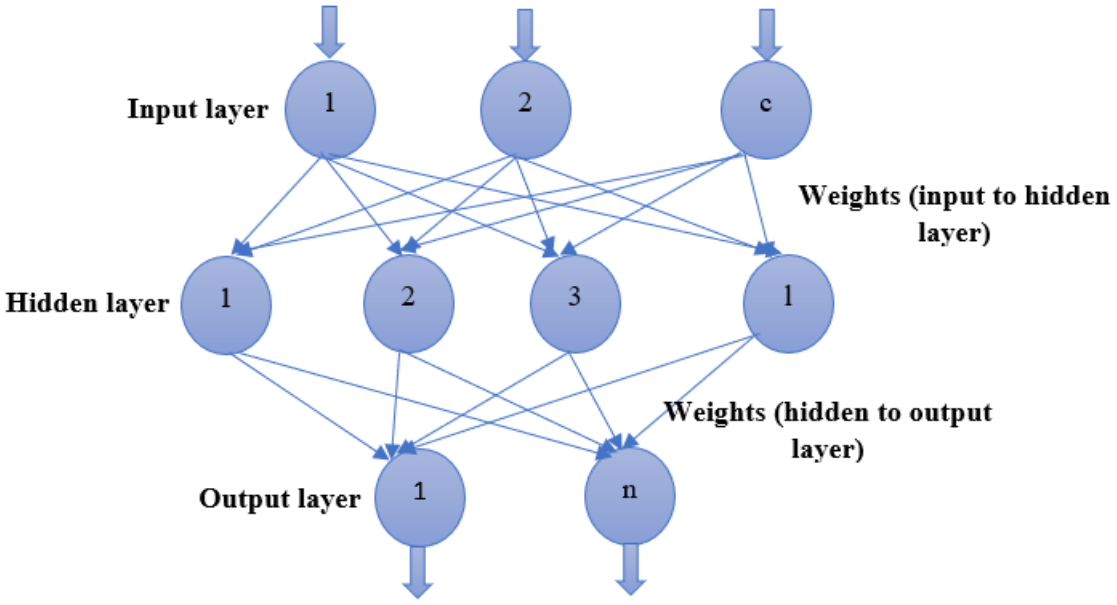

Figure 2: Architecture of ELM

Step 1: Choose the input weights and hidden layer biases using the whale optimization algorithm (WOA). A recently created meta-heuristic optimization method called the WOA is based on how humpback whales' hunt. The whales employ two different techniques to both attack and locate their prey. The prey is enclosed in the first, while bubble nets are made in the second. In terms of optimization, whales search for prey by exploring their environment and using it during an attack. The mathematical model of the three strategies is as follows:

$$\tilde{H}_n^m(\tau+1) = \tilde{H}_n^*(\tau) - \alpha . \tilde{D}_{m,n} \quad (4)$$

$$\tilde{H}_n^m(\tau+1) = \tilde{H}_n^*(\tau) + e^{\kappa j} . \cos(2\pi j) . \tilde{D}_{m,n} \quad (5)$$

$$\tilde{H}_n^m(\tau+1) = \tilde{H}_n^{rand}(\tau) - \alpha . \tilde{D}_{m,n} \quad (6)$$

Where τ indicates the current iteration, $\widetilde{H}^{*}$ denotes the global best solution, κ indicates a constant that determines the shape of solenoid; j refers to a random number in [-1, 1], $\widetilde{H}^{rand}$ represents randomly selecting a whale from the current population. When $p < 0.5$ and $\alpha \le 1$, whales update their position via equation (4), else if $\alpha > 1$, whales update their position via equation (6), $\widetilde{D}_{m,n} = \left| 2.rand\,.\,\widetilde{H}_{n}^{*}(\tau) - \widetilde{H}_{n}^{m}(\tau) \right|$, $rand$ indicates a random number in [0, 1]. Else, whales update their position via equation (5). This process continues until we obtain the optimum solution (i.e., optimal weights and bias).

Step 2: Next, compute the hidden layer $\left(\vec{\vec{h}}_{l}\right)$ output matrix as in equation (7).

$$\vec{\vec{h}}_{l} = \sum_{c=1}^{K} \ddot{B}_{c}^{*} * \mu\left(\ddot{\varpi}_{c}^{*} * \widetilde{\widetilde{F}}_{c} + \ddot{L}_{c}\right) \tag{7}$$

Where, $\ddot{B}_{c}^{*}$, $\ddot{\varpi}_{c}^{*}$, and $\ddot{L}_{c}$ refers to the weight vector connecting to c^{-th} hidden neuron to output neurons, weight vector connecting to c^{-th} hidden neurons to the input neurons, and bias at c^{-th} hidden neuron and these are optimally selected via WOA, $\widetilde{\widetilde{F}}_{c}$ indicates the input feature vector, and μ refers to the ReLU activation function.

Step 3: After that, compute the output weight $\left(\underline{\underline{OM}}\right)$ matrix using the equation (8).

$$\underline{\underline{OM}} = \vec{\vec{h}}_{l}^{+}\; T_{L} \tag{8}$$

Where, $\vec{\vec{h}}_{l}^{+}$ refers to the Moore-Penrose generalized inverse matrix of $\vec{\vec{h}}_{l}$ and T_{L} indicates the target or class label. It produces fingerprint images as true or fake. This result is given to the Matcher, who uses the up-sampled results to determine the hamming distance. The obtained hamming distance will be used to determine whether the two vectors originated from the same user if it is less than a predetermined threshold. The user is validated if the true/fake detection unit recognizes the biometric data as live data and the hamming distance exceeds the threshold.

4. RESULTS AND DISCUSSION

This section discusses the experimental outcomes obtained by the proposed and existing models for fingerprint recognition. On an Intel Core i5-4570 3.20 GHz, RAM 8 GB, Windows 10 Professional 64-bit computer, all tests and computations in this work were performed using MATLAB (R2016a) software. The descriptions of the dataset and performance analysis of the proposed system are given in sections 4.1 and 4.2.

4.1 Dataset Descriptions

The public databases, specifically the FVC 2004 from the Fingerprint Verification Competition, are used for testing and evaluation studies. The chosen dataset often takes the following four forms: Each dataset in DB1, DB2, DB3, and DB4 has 110 distinct fingerprint images, with eight finger impressions per image (for a total of 110 x 8 = 880 fingerprints). Two distinct subsets (A and B) are further separated for each component database, allowing the subset. In contrast to set B, which is made available to allow parameter tuning prior to the submission of the algorithms, set A contains the first 100 fingers and eight impressions per finger (i.e., 800 impressions total), which is typically used for the performance evaluation of fingerprint verification systems. Set B only has the last ten fingers (80 impressions). Through http://bias.csr.unibo.it/fvc2004/download.asp, it is simple to access.

4.2 Performance Analysis

This section investigates the outcomes of the proposed WBELM against the classical approaches of ELM, SVM, RF, and naïve bayes (NB) classifiers. The evaluation is carried out with the help of recognition accuracy, precision, recall, f-measure, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Elapsed time, respectively. These analyses are shown in the following figure and table.

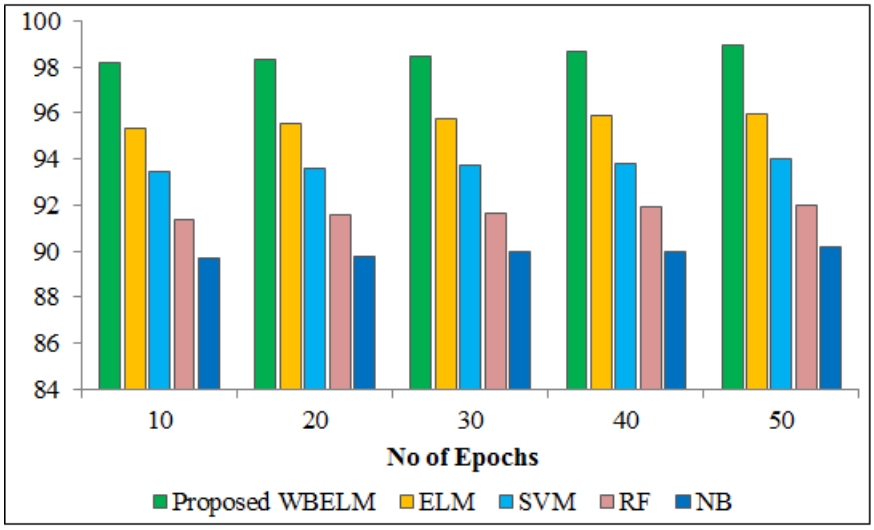

Figure 3: Recognition accuracy analysis

Figure 3 demonstrates the efficiency of the proposed WBELM, which is analyzed with the conventional ELM, SVM, RF, and NB classifiers in terms of recognition accuracy metric for the different epochs, varying from 10 to 50. The recognition accuracy returned an overall measurement of the correct prediction of individual classes among the total number of classes. For epoch 10, the existing ELM, SVM, RF, and NB achieve recognition accuracy of 95.34%, 93.47%, 91.35%, and 89.67%, which is less than the proposed methods, because the proposed one achieves high recognition accuracy of 98.23%. Likewise, for the remaining no of epochs (20-50), the proposed one achieves maximum accuracy of 98.37%, 98.49%, 98.67%, and 98.96%, which are also better outcomes than the existing methods. Thus, figure 3 concludes that the proposed one achieves superior outcomes than the existing methods. Next, the following table shows the performance of the proposed WBELM with the existing ELM, SVM, RF, and NB classifiers in terms of precision, recall, f-measure, FAR, FRR, EER, and elapsed time.

Table 1: Performance analysis of the propose model

Metrics	**Proposed WBELM**	**ELM**	**SVM**	**RF**	**NB**
Precision (%)	98.63	95.78	93.83	91.81	89.99
Recall (%)	98.47	95.58	93.63	91.57	89.85
F-Measure (%)	98.55	95.68	93.73	91.67	89.92
FAR (%)	0	0.62	0.98	1.46	1.98
FRR (%)	0.118	0.236	0.398	0.512	0.785
EER (%)	0.521	1.256	1.358	1.364	1.452
Elapsed time (ms)	584	665	957	1075	1149

Table 1 compares the proposed outcomes with existing methods. Evidently, the proposed approach outperformed the other classification techniques for all metrics. For example, the precision obtained by the proposed WBELM approach was improved by 2.85%, 4.8%, 6.82%, and 8.64 compared to ELM, SVM, RF, and NB, respectively. Regarding the same metric, the ELM is the second best compared to the other techniques. Similarly, the proposed one achieves better outcomes for the remaining metrics than the existing methods. For example, the proposed one achieves maximum outcomes of 98.47% recall, 98.55% f-measure, 0% FAR, 0.118% FRR, 0.521% EER, and less elapsed time of 584ms, respectively. The reason is that the proposed one initially utilized Bilateral filtering to

remove the noise from the image, efficiently removing the noise from the image. It also utilized the DICNN approach to extract features from the image efficiently, and it improved the prediction rate and decreased the elapsed time. Also, the WOA included in the proposed work optimally selects the weight and bias and increases the recognition rate of the proposed work.

5. CONCLUSION

This paper proposes a novel fingerprint recognition system using a dilated convolutional neural network and an extreme learning machine. The proposed system mainly comprises '3' phases: preprocessing, feature extraction, and fingerprint recognition. The proposed work uses the FVC 2004 database to analyze its effectiveness over others. The outcomes of the proposed WBELM are investigated against the existing ELM, SVM, RF, and NB classifiers regarding recognition accuracy, precision, recall, f-measure, FAR, FRR, EER, and elapsed time. Herein, the proposed work achieves a maximum accuracy of 98.54%, a better outcome than the existing methods—likewise, the proposed one archives outstanding outcomes for all the remaining metrics than all the existing approaches. In future work, this work will be prolonged by segmenting the fingerprint accurately from the preprocessed image to improve the overall recognition rate.

REFERENCES

[1] Trabelsi, S., Samai, D., Dornaika, F., Benlamoudi, A., Bensid, K., & Taleb-Ahmed, A. (2022). Efficient palmprint biometric identification systems using deep learning and feature selection methods. *Neural Computing and Applications*, *34*(14), 12119-12141.

[2] Peng, C., Chen, M., & Jiang, X. (2021). Under-display ultrasonic fingerprint recognition with finger vessel imaging. *IEEE Sensors Journal*, *21*(6), 7412-7419.

[3] Alrashidi, A., Alotaibi, A., Hussain, M., AlShehri, H., AboAlSamh, H. A., & Bebis, G. (2021). Cross-sensor fingerprint matching using siamese network and adversarial learning. *Sensors*, *21*(11), 3657.

[4] Militello, C., Rundo, L., Vitabile, S., & Conti, V. (2021). Fingerprint classification based on deep learning approaches: experimental findings and comparisons. *Symmetry*, *13*(5), 750.

[5] Popli, A., Tandon, S., Engelsma, J. J., & Namboodiri, A. (2023). A unified model for fingerprint authentication and presentation attack detection. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment* (pp. 77-99). Singapore: Springer Nature Singapore.

[6] Rim, B., Kim, J., & Hong, M. (2021). Fingerprint classification using deep learning approach. *Multimedia Tools and Applications*, *80*, 35809-35825.

[7] Garcia-Martin, R., & Sanchez-Reillo, R. (2021). Deep learning for vein biometric recognition on a smartphone. *Ieee Access*, *9*, 98812-98832.

[8] Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. *Artificial Intelligence Review*, 1-49.

[9] Tchito Tchapga, C., Mih, T. A., Tchagna Kouanou, A., Fozin Fonzin, T., Kuetche Fogang, P., Mezatio, B. A., & Tchiotsop, D. (2021). Biomedical image classification in a big data architecture using machine learning algorithms. *Journal of Healthcare Engineering*, *2021*, 1-11.

[10] Shaheed, K., Mao, A., Qureshi, I., Kumar, M., Abbas, Q., Ullah, I., & Zhang, X. (2021). A systematic review on physiological-based biometric recognition systems: current and future trends. *Archives of Computational Methods in Engineering*, 1-44.

[11] NR, P. (2021). Fingerprint recognition model using DTCWT algorithm. *International Journal of Information Technology*, *13*(4), 1581-1588.

[12] Nguyen, L. T., Nguyen, H. T., Afanasiev, A. D., & Nguyen, T. V. (2022). Automatic identification fingerprint based on machine learning method. *Journal of the Operations Research Society of China*, *10*(4), 849-860.

[13] Deshpande, U. U., Malemath, V. S., Patil, S. M., & Chaugule, S. V. (2022). Automatic latent fingerprint identification system using scale and rotation invariant minutiae features. *International Journal of Information Technology*, *14*(2), 1025-1039.

[14] Bakheet, S., Alsubai, S., Alqahtani, A., & Binbusayyis, A. (2022). Robust Fingerprint Minutiae Extraction and Matching Based on Improved SIFT Features. *Applied Sciences*, *12*(12), 6122.

[15] Tran, Q. N., Turnbull, B. P., Wang, M., & Hu, J. (2021). A Privacy-Preserving Biometric Authentication System with Binary Classification in a Zero Knowledge Proof Protocol. *IEEE Open Journal of the Computer Society*, *3*, 1-10.

DOI: https://doi.org/10.15379/ijmst.v10i2.2957