DOI: 10.6977/IJoSI.202508_9(4).0007
R. Sreemol, M. B. Santosh Kumar, etc./Int. J. Systematic Innovation, 9(4), 84-105 (2025)

# Fusion Net-3: Denoising-based secure biometric authentication using fingerprints

R. Sreemol[1]*, M. B. Santosh Kumar[2], A. Sreekumar[1]

[1]Department of Computer Applications, Faculty of Technology, Cochin University of Science and Technology, Kochi, Kerala, India

[2]Department of Information Technology, School of Engineering, Faculty of Engineering, Cochin University of Science and Technology, Kochi, Kerala, India

*Corresponding author E-mail: sreemolr@cusat.ac.in

(Received 3 October, 2024; Final version received 24 June, 2025; Accepted 9 July, 2025)

## Abstract

Fingerprint-based authentication is a critical biometric approach for ensuring security and accuracy. Traditional methods often face challenges such as noise and suboptimal feature extraction. To address the challenges, Fusion Net-3, an extensive model, is proposed to improve the speed, precision, and security level of fingerprint-based authentication systems. Fusion Net-3 operates through two separate stages: enrollment and authentication. During the enrollment phase, advanced pre-processing of fingerprint images was performed, incorporating an enhanced bilateral filter optimized with the seagull optimization algorithm. After pre-processing, features were obtained using a two-phase method: Zernike moments for shape-based features and local binary patterns for texture-based features. This helped ensure that fingerprint features were considered comprehensive for representation. For feature selection optimization, the falcon-inspired jackal optimization algorithm was proposed, a hybrid method combining the strengths of the golden jackal optimization and falcon optimization algorithm. Then, the selected features were combined using a combination of the geometric mean and the Fisher score to facilitate classification for a balanced and novel representation. During authentication, fingerprints were processed using similar techniques for consistency. Each fingerprint was labeled as genuine or fraudulent with the aid of the Fusion Net-3 model, which leverages the combined strengths of convolutional neural networks, ResNet-50, and U-Net. The model achieved an accuracy of 98.956% and a mean squared error of 0.0234 when implemented on a Python platform. Overall, the Fusion Net-3 model demonstrated superior performance compared to existing methods, effectively enhancing authentication accuracy and security.

*Keywords:* Authentication, Bilateral Filtering, Enrollment, Falcon Optimization, Fusion Net-3, Golden Jackal Optimization, Seagull Optimization.

## 1. Introduction

Biometric authentication has become the backbone of today's security systems, using unique biological characteristics to verify identity and control access. Among the modalities, fingerprint authentication has emerged as one of the most robust, reliable, and widely adopted methods in diverse applications, ranging from unlocking mobile devices to national identification programs (Adiga & Sivaswamy, 2019; Akter et al., 2024). As a unique biometric characteristic, fingerprints offer non-intrusive, high-accuracy authentication based on the uniqueness of the minutiae patterns. To provide access, fingerprint identification systems first collect a person's fingerprints, create a customized fingerprint template, and then compare it to a database of previously approved users (Ali et al., 2020; Balsiger et al., 2020). Even though fingerprint recognition is a useful biometric authentication technique, several issues need to be resolved. The security of the system is among the important elements. Since fingerprint data are private information, it must be shielded from online

dangers. Fingerprint data can be stolen and exploited by hackers for financial benefit. Therefore, designing a safe fingerprint authentication system is necessary. Efficiency is another challenge fingerprint recognition systems face. Large-scale deployments, such as those in government or corporate settings, require the system to promptly and reliably authenticate a vast number of users (Santos et al., 2024).

To address these challenges, researchers and developers have considered cutting-edge techniques and algorithms to enhance the efficacy of fingerprint recognition technologies (Zhang et al., 2019). For example, eye-tracking data, such as pupil dilation and fixation time, can be used to accurately predict cognitive load through machine learning models, including random forest (RF) and multi-layer perceptron (Dhiman & Kumar, 2019; Ding et al., 2020; Nasri et al., 2024). In addition, using an authentication system based on reconstruction is one innovative method. Reconstructing the original fingerprint picture acquired from the minute spots is how the reconstruction-based authentication system operates (Ephin & Vasanthi, 2013; Galbally et al., 2020). The distinctive qualities of a fingerprint, known as minutiae points, are the foundation of a fingerprint template. The technology can authenticate fingerprints and thwart fraudulent assaults by reconstructing the original image. However, to overcome new difficulties, traditional encryption or detection-based protection paradigms are insufficient. Traffic reshaping-based solutions, such as traffic morphing and frame quantization, provide a partial defense against specific threats but lack verifiable assurances (Abolfathi et al., 2022). Compared to conventional fingerprint recognition techniques, the reconstruction-based approach offers several benefits. First, it improves security by guarding against deceptive tactics, such as spoofing, in which a hacker fabricates a false fingerprint using synthetic materials (Gao et al., 2020; Gavaskar & Chaudhury, 2018). It is harder for fraudulent methods to deceive the system because the system authenticates fingerprints by reconstructing the original image. Second, compared to conventional fingerprint recognition methods, the reconstruction-based approach is more efficient (Gupta et al., 2020).

A reconstruction-based system can process the authentication request considerably faster because it does not need to process the entire fingerprint image. In addition, it reduces the amount of storage space needed to store fingerprint data, facilitating extensive system deployments. More research and instructional initiatives are required to enhance privacy-aware software development, while role-dependent solutions are needed to address privacy concerns in software development (Prybylo et al., 2024). The advent of hostile attacks has led to an ongoing interaction between the development of advanced attack methods and the application of strong countermeasures. This has encouraged the development of a wide range of attack techniques, each specifically designed to provide a challenge to neural networks (NNs) in different contexts. Moreover, there are critical challenges in the security and efficiency of fingerprint-based systems, including vulnerability to cyberattacks, susceptibility to spoofing, and a need for rapid and accurate performance in large-scale implementations. These challenges must be addressed to enhance the reliability of biometric systems, particularly in sensitive domains, such as financial transactions and border control (Banitaba et al., 2024; Wong & Lai, 2020). The super-learner attack, a new attack model targeting fingerprinting of HTTPS websites, has led to the development of the HTTPS obfuscation defender as a protection tactic. This defense mechanism uses adversarial example algorithms and introduces fictitious packets to interfere with categorization processes (Abolfathi et al., 2024). In parallel, reconstruction-based authentication methods have shown promise in enhancing fingerprint recognition systems' effectiveness. These approaches can stop fraudulent attacks and promptly and accurately process authentication requests (Husson et al., 2018; Xu et.al, 2019). As biometric authentication grows in popularity, designing secure and effective authentication techniques is crucial to mitigate potential cyberattacks. The main objectives of the research are as follows:

(i) Improved denoising: Enhanced bilateral filtering optimized through the seagull optimization algorithm (SOA) to preserve edge features while effectively removing noise
(ii) Robust feature extraction: Combined use of Zernike moments (shape features) and local binary pattern (LBP; texture features) for comprehensive fingerprint representation
(iii) Optimal feature selection: A novel falcon-inspired jackal optimization (FIJO) algorithm, hybridizing golden jackal optimization (GJO) and falcon optimization algorithm (FOA), was proposed to select the most discriminative features
(iv) Secure and accurate classification: Integration of convolutional NNs (CNNs), ResNet-50, and U-Net, into Fusion Net-3 to classify genuine versus fraudulent fingerprints
(v) Secure transmission: Incorporation of blockchain technology to safeguard fingerprint data integrity and confidentiality during authentication.

The remaining parts of the research include Related Works in Section 2, Proposed Model in Section 3, Results and Discussion in Section 4, and Conclusions in Section 5.

## 2. Related Works

The research conducted by various researchers on secure biometric authentication using fingerprints is provided in this section (Table 1).

Jia et al. (2019) proposed a highly secure biometric authentication system that can be created using a robust 3D fingerprint template to ensure the uniqueness of users' identities. This was achieved by computing minutiae triplets from the fingerprints' minutiae points, which were then used to generate the secured user template.

Kareem & Okur (2021) explored how a compressed sensing-based compression reconstruction method was developed to improve heart signal biometric recognition using portable remote bioelectric signal recognition equipment. This approach utilizes bioelectric signals to effectively enhance the limited resources of the equipment, resulting in more accurate recognition.

Khodadoust et al. (2020) proposed a mathematical model to examine the effects of transient-state excitation and k-space undersampling on magnetic resonance fingerprinting reconstructions. The model establishes a direct relationship across time-varying RF excitation, k-space sampling, and reconstruction errors, all of which are dependent on spatial variations.

Koonce & Koonce (2021) used an autoencoder network to detect presentation attacks on fingerprints. A one-class approach was used to improve detection accuracy in the study. The proposed method aims to detect fingerprint presentation attacks using only one class of data.

Lee et al. (2022) developed an FPD-M-net, which is an end-to-end CNN architecture for fingerprint image denoising and inpainting. By treating a problem as a segmentation task and incorporating a structure similarity loss function, the architecture can effectively extract fingerprints from a noisy background. The network is based on the M-net and is fully trainable.

Li et al. (2018) used an adaptive sampling strategy that utilizes an approximate volume sampling method to enhance the accuracy of radio maps for fingerprint-based indoor localization. This scheme employs a low-tubal-rank tensor to model all reference points' Wi-Fi fingerprints, aiming to reduce the expenditure required for reconstruction. The proposed approach is effective in enhancing the accuracy of indoor localization.

Li et al. (2022) introduced CRISLoc, the first localization prototype system that used channel-state information (CSI) fingerprinting based on ubiquitous smartphones. This system can passively overhear packets in real-time for its own CSI acquisition, eliminating the need for active user participation. With its innovative approach, CRISLoc demonstrates the feasibility of using smartphones for accurate and efficient localization.

Lin & Kumar (2018) used a new method for enhancing latent fingerprints, based on Finger Net, a CNN inspired by recent advancements in CNN development. The Finger Net architecture comprises a shared common convolution component and two separate deconvolution components, consisting of the enhancement and orientation branches. This

**Table 1.** Comparison of existing literature

| Authors | Method | Advantage | Disadvantage |
|---|---|---|---|
| Jia et al. (2019) | 3D fingerprint via minutiae triplets | High security | Needs 3D sensors |
| Kareem & Okur (2021) | Compressed sensing on heart signals | Efficient, accurate | Sensitive to signal noise |
| Khodadoust et al. (2020) | Magnetic resonance fingerprinting model | Explains error causes | Complex to apply |
| Koonce & Koonce (2021) | One-class autoencoder for presentation attack detection (PAD) | Works with one-class data | May miss unseen attacks |
| Lee et al. (2022) | FPD-M-net for denoising | Accurate, end-to-end | Needs a large training set |
| Li et al. (2018) | Adaptive sampling for radio maps | Lower cost | Sampling-dependent |
| Li et al. (2022) | CRISLoc (channel-state information via smartphones) | Passive, no user input | Varies by environment |
| Lin & Kumar (2018) | Finger Net convolutional neural network | Enhanced latent prints | Limited to poor prints |
| Liu et al. (2020a) | Contactless 3D with Siamese nets | No touch needed | Complex setup |
| Liu et al. (2021) | Cahn–Hilliard for restoration | Simple, effective | Narrow scope |
| Liu et al. (2022) | CFD-PAD with presentation attack-adaptation loss | Better spoof detection | High training cost |
| Liang & Liang (2023) | Res-WCAE for denoising | Lightweight, detailed | Limited global view |
| Rahman et al. (2022) | Minutiae and chaffs for security | High privacy | Complex template |
| Algarni (2024) | Multi-fingerprint (BioPass) | More secure login | Needs user effort |

Abbreviations: CFD: Channel-wise feature denoising; Res-WCAE: Residual wavelet-conditioned convolutional autoencoder.

approach is effective in improving the quality of latent fingerprints for better identification.

Liu et al. (2020a) proposed a contactless 3D fingerprint representation learning model, utilizing a CNN. The model incorporates a fully convolutional network for fingerprint segmentation and three Siamese networks to learn a multi-view 3D fingerprint feature representation. This approach successfully produced precise 3D fingerprint representations without requiring physical contact.

Liu et al. (2021) presented a reliable and efficient fingerprint image restoration technique, utilizing a non-local Cahn–Hilliard equation designed for modeling microphase separation of di-block copolymers. The method employs a Gauss–Seidel-type iterative approach, resulting in a straightforward implementation process that enhances the quality of fingerprint images with effectiveness and efficiency.

Liu et al. (2022) proposed a new channel-wise feature denoising fingerprint presentation attack detection technique that addresses the redundant noise data that were overlooked in earlier research. The suggested approach determines discriminative and "noise" channels by evaluating the significance of each channel to learn significant fingerprint picture features. To reduce interference, "noise" channel propagation is then muted in the feature map. To make the feature distribution of spoof fingerprints more dispersed and that of live fingerprints more aggregate, a presentation attack-adaptation loss is specifically introduced to restrict the feature distribution.

Liang & Liang (2023) presented the residual wavelet-conditioned convolutional autoencoder (Res-WCAE), a lightweight and reliable deep learning architecture with the Kullback–Leibler divergence regularization that is specifically designed for fingerprint image denoising. Res-WCAE consists of one decoder and two encoders: a wavelet encoder and an image encoder. The bottleneck layer is conditioned on the compressed representation of features derived from the wavelet encoder, which processes both approximation and detail sub-images in the wavelet-transform domain. Residual connections between the image encoder and decoder are employed to preserve fine-grained spatial features.

Rahman et al. (2022) proposed a strategy based on minutiae to defend fingerprint templates against security breaches. Even though the database provides an attacker with these safe minutiae templates, it is difficult to access the actual minutiae features of a user fingerprint. Minutiae-based techniques have been applied in the study, and the fingerprint minutiae characteristics and their associated parameters have been investigated. This technique creates a secure template by altering the actual minutiae information and adding additional chaffs (fake minutiae) to safeguard the minutiae features. It is nearly impossible to obtain fingerprint features or vault information using this method because the template pattern is completely different for each new fingerprint, even if the parameters are the same for the same fingerprint.

Algarni (2024) presented the novel idea of a multi-fingerprint sequence authentication procedure for user verification. For improved convenience and security, this multifactor methodology combines the use of several fingerprints with a sequence pattern, as opposed to the conventional, single-fingerprint methods. In addition, as an alternative to biometric usernames and text passwords, this study offers a thorough assessment of BioPass, a novel authentication mechanism that uses a multi-fingerprint sequence pattern.

New biometric systems utilizing optimal-effort fingerprint templates demonstrate improved verification security, accuracy, and efficiency. However, these systems face limitations, such as model and hardware complications, data training requirements, and potential issues with compromised signals and noise. A unification of systems integrating multimodal has not been synthesized, and computational value overstated cases. This literature review highlights the potential of emerging approaches that maintain optimal-effort security, optimize user experience, minimize hardware dependency, and mitigate potential exploitation risks, all without compromising user choice or agency. The proposed Fusion Net-3 model, optimized using SOA, incorporates enhanced bilateral filtering, hybrid feature extraction, a novel FIJO-based feature selection method, and an integrated CNN–ResNet-50–U-Net model for classification.

## 3. Fusion Net-3

The proposed model, Fusion Net-3, comprises two stages, enrollment and authentication. Using enhanced bilateral filtering, noises are removed from the images. Filter parameters are optimized using an SOA, and the images are enhanced using a contrast enhancement technique. The pre-processed output is then used to extract features based on shapes and textures. Ultimately, a unique FIJO, a combination of the GJO and FOA, is used for feature selection. The features are combined using geometric mean and Fisher score. The fingerprint images are given as input into the second phase, where pre-processing, feature extraction, feature selection, and feature fusion are conducted using similar approaches. Finally, the efficient (correct or incorrect) fingerprints are detected using the Fusion Net-3 model, which combines CNN, ResNet-50, and U-Net models. Fig. 1 illustrates the proposed model.

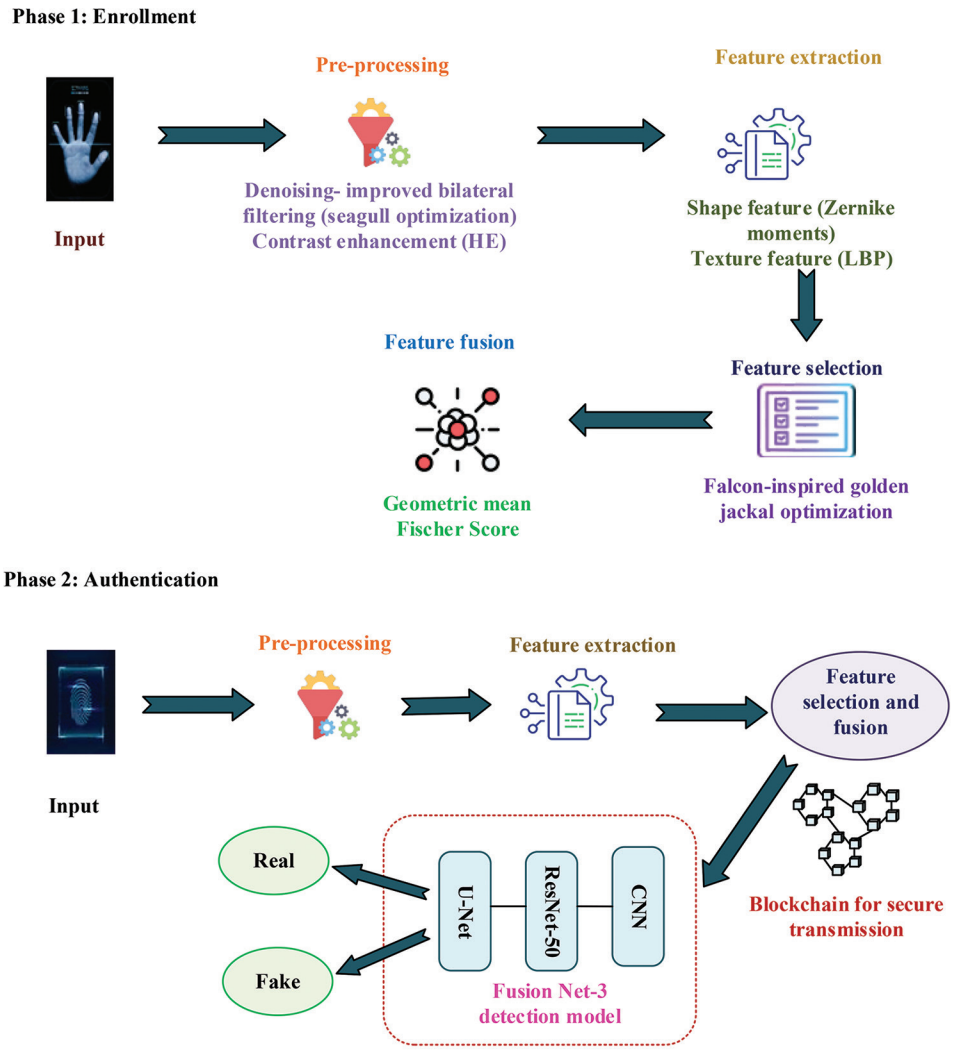


**Fig. 1.** Architecture for the proposed authentication system

### 3.1. Enrollment

Enrollment is the first phase of the model, which collects the information of scanned hands. The following steps provide a detailed explanation of this phase.

#### 3.1.1. Pre-processing

Pre-processing is a necessary step that transforms raw datasets into a desired format, ensuring the accuracy and applicability of the data. This study employed two methodologies, improved bilateral filtering (Liu et al., 2020b; Mahum et al., 2023) and histogram equalization (HE) (Narodytska & Kasiviswanathan, 2017; Paris et al., 2009).

(a) Noise Reduction Using Improved Bilateral Filtering

A non-linear filter–the bilateral filter–preserves edges while removing noise. It considers the geometric proximity of adjacent pixels and the similarity of their gray levels (Afshari et al., 2017). The filter computes the local neighborhood's weighted sum of pixels. These pixels are replaced with the weighted average of their neighbors (Gavaskar and Chaudhury, 2018). Both the intensity difference and the spatial distance of the pixel relative to its neighborhood can be used to determine the weights. It is formulated as:

$$O(p,q) = M\left(\frac{1}{A(p,q)} \sum_{(i,j)\in N(p,q)} f_b\begin{pmatrix} I(x,y) \\ -I(i,j) \end{pmatrix} .f_c\left((p,q)-(i,j)\right) I(i,j)\right) \quad (1)$$

Where $O(p, q)$ is the filtered output image at pixel $(p, q)$, $M$ is the input data, $A(p, q)$ is the normalization factor, $N(p, q)$ is the spatial neighborhood of $I(p, q)$, and $f_b$ is the intensity kernel, which is the difference

in intensities between the center pixel ($p$, $q$) and the surrounding pixels ($i$, $j$), $f_c$ is the spatial kernel, which is the spatial proximity between ($p$, $q$) and (i, j). $f_b$ and $f_c$ can be defined as:

$$f_b(d) = e^{-\frac{d^2}{2\sigma_b^2}} \tag{2}$$

Where $d$ is the intensity difference between pixels, $\sigma_b$ controls the intensity kernel's standard deviation;

$$f_c(d) = e^{-\frac{d^2}{2\sigma_c^2}} \tag{3}$$

Where $d$ is the Euclidean distance between pixels, $\sigma_c$ controls the spatial kernel's standard deviation.

$$O(x,y) = \frac{1}{A(p,q)} \sum_{(i,j)\in N(p,q)} e^{\frac{-|I(i,j)-I(p,q)|^2}{2\sigma_b^2}} . e^{\frac{-(p,q)-(i,j)}{2\sigma_c^2}}, I(i,j) = O \tag{4}$$

As a result, edge preservation and noise reduction can be accomplished using bilateral filter (BF). The improved bilateral filtering strategy was utilized in previous studies, involving the application of an SOA (Praseetha et al., 2019) to tune the filter's parameters, including the spatial kernel ($\sigma_s$) and intensity kernel ($\sigma_r$), to increase denoising efficiency. The main purpose of the SOA is to mimic the migratory and predatory behaviors of seagulls in their native environment, achieving optimal denoising performance. For example, the pursuit of food is a defining characteristic of gull migratory behavior. The manner in which seagulls hunt migratory birds at sea is referred to as "attack behaviors." The system replicates the gulls' migratory patterns from one area to another. To locate the search agent, $L$ (mobile behavior) is considered to avoid collisions among seagulls:

$$\overrightarrow{N_q} = L \times \overrightarrow{S_q}(p) \tag{5}$$

Where $\overrightarrow{N_q}$ and $\overrightarrow{S_q}$ are the search agent's position and present positionrespectively.

$$L = f_c - \left( p \times \left( \frac{f_c}{\max iter} \right) \right); p = 0,1,\ldots,\max iter \tag{6}$$

Where $f_c$ is the parameter's frequency. When the search agent avoids collisions with seagulls, it moves in the optimal nearby direction:

$$\overrightarrow{M_q} = B \times \left( \overrightarrow{S_{bq}}(p) - \overrightarrow{S_q}(p) \right) \tag{7}$$

Where $\overrightarrow{M_q}$ indicates the search agent's location, $\overrightarrow{S_q}$ is the direction of the optimum search agent $\overrightarrow{S_{bq}}$, and $B$ balances between exploration and exploitation behavior, which is stochastic and is defined as:

$$B = 2 \times L^2 \times rdm \tag{8}$$

Where $rdm$ is a random number within [0,1].

Furthermore, the search agent may adjust its ranking concerning the most prominent search agent:

$$\overrightarrow{D_q} = \left| \overrightarrow{N_q} + \overrightarrow{M_q} \right| \tag{9}$$

Where $\overrightarrow{D_q}$ shows a distinction between the search agent and the most suitable search agent (i.e., the optimal seagull with a lower fitness value).

Seagulls exhibit a spiral movement while attacking their prey. The behavior in the $x$, $y$, and $z$ planes can be stated as follows:

$$x' = r \times cos(l) \tag{10}$$

$$y' = r \times sin(l) \tag{11}$$

$$z' = r \times l \tag{12}$$

$$r = g \times e^{lh} \tag{13}$$

The updated position of the search agent is given as:

$$\overrightarrow{S_q}(p) = \left( \overrightarrow{D_q} \times x' \times y' \times z' \right) + \overrightarrow{S_{bq}}(p) \tag{14}$$

Configurations for reproducibility include a 512 × 512 pixel input image size, a 5 × 5 filter window, and optimized parameter values of $\sigma_s = 1.5$ and $\sigma_r = 0.8$.

(b) Contrast Enhancement using Histogram Equalization

Dynamic range, or the ratio of the brightest to darkest pixel intensities, determines image contrast. There are various applications for contrast enhancement techniques to improve low-contrast images. HE is a commonly employed technique. The probability distribution of input gray levels is used to map the gray levels. The histogram of the image is stretched and flattened to increase contrast. The probability density function $S(I_y)$ for image $I$ is provided as follows:

$$S(I_y) = \frac{n_y}{n} \tag{15}$$

Where $y = 0, 1,\ldots,L\text{-}1$, $y$ is the series of time of the level $I_y$ in input images, and $n$ indicates samples.

The cumulative density function is defined as:

$$c(i) = \sum_{i=0}^{y} S(I_i) \tag{16}$$

Where $I_y = i$, $y = 0,1\ldots,L\text{-}1$, and $c(I_{L-1}) = 1$ (default).

The transform function $f(i)$, based on the above equation, is given as:

$$f(i) = I_0 + (I_{L-1}-I_0)\, c(i) \tag{17}$$

The HE results, $V$, which is the function of $\{S(q, r)\}$, is given as:

$$V = f(I) = \{f(I(k,i)) | \forall I(k,i) \in I\} \tag{18}$$

As a result, the contrast of the images is enhanced.

### 3.1.2. Feature extraction

Feature extraction is the process of extracting a set of features from the pre-processed data. The shape and texture features are extracted using the Zernike moments (Shadab et al., 2022) and LBP (Shehu et al., 2018; Vogel, 2022) techniques.

(a) Shape Feature Extraction Using Zernike Moments

The low-level feature that Zernike moments yield is significant. Zernike moments provide rotationally invariant descriptors based on the order $n$ and repetition $m$ of Zernike polynomials, computed from radial polynomials which capture the finer details of shape. Since it is rotationally invariant, recognition is based on the magnitude of these moments. The following are the Zernike radial polynomials:

$$R_{nm}(p,q) = \sum_{s=0}^{(n-|m|)/2} (-1)^s \times \frac{\left(p^2+q^2\right)^{\frac{n-2s}{2}} (n-s)!}{s!\left(\left(n+\frac{|m|}{2}-s\right)!\right)\left(\left(\left(n-\frac{|m|}{2}-s\right)!\right)\right)} \tag{19}$$

Where $n$ is a non-negative integer, $m$ is a non-zero integer, $n$-$|m|$ is even, and $|m| \leq n$.

The $(n, m)$ order of the Zernike bias function is given as:

$$V_{nm}(p,q) = R_{nm}(p,q)\, e^{jm\theta} \tag{20}$$

Where $j$ is $\sqrt{-1}$, and $\theta$ is $tan^{-1}\left(\frac{y}{x}\right)$.

The Zernike moments of order $n$ and repetition $m$ of a function $f(p, q)$ are defined as:

$$Z_{nm} = \frac{n+1}{\pi}\int_0^{2\pi}\int_0^1 f(p,q) V_{nm}^*(p,q)\, dpdq \tag{21}$$

Where $V_{nm}^*$ is a complex conjugate of $V_{nm}$.

(b) Texture Feature Extraction Using Local Binary Pattern

Color features use individual pixels, whereas texture features use groups of pixels. In the feature maps, an LBP is computed for every pixel. After comparing the data, the results are binary encoded. A collection of binary characteristics is produced, capturing certain local texture patterns. It derives texture information from the surface features, patterns, and edges. The $(p_c, q_c)$ gray value of a center pixel is compared to the pixels of its eight neighbors to create an ordered binary set, or LBP. As a result, the LBP code is expressed as a decimal octet value.

$$z = LBP(p_c, q_c) = M\left(\sum_{n=0}^{7} S(i_n - i_c) 2^n\right) \tag{22}$$

Where $i_c$ is the gray value of the center pixel $(p_c, q)$ and $i_n$ is the gray value of the pixels of its eight neighbors. After transformation, the result obtained is given as:

$$S(i_n - i_c) = \begin{cases} 1 & ;(i_n - i_c) \geq 0 \\ 0 & ;(i_n - i_c) < 0 \end{cases} \tag{23}$$

The LBP is a texture representation method where the intensity difference between a central pixel and its neighbors is encoded. LBP involves parameters, such as radius ($R$) and neighbors ($P$), for generating binary patterns. Configurations include a radius of 1–3 pixels, 8–16 neighbors, and uniform pattern mapping. This two-phase approach will thus ensure full representation of features since it captures both the geometric structure and surface details of the fingerprint images.

### 3.1.3. Feature fusion

By utilizing the geometric mean and Fisher score, the fusion of selected features is achieved. This methodology ensures that every feature carries equal weight, while simultaneously maximizing the distinction between genuine and imposter fingerprints.

(a) Geometric Mean

The geometric mean is a widely used mathematical concept in finance, science, and engineering, providing a measure of central tendency for a set of numbers. Unlike the arithmetic mean, the geometric mean multiplies the values and takes the $n^{th}$ root of the product, making it more sensitive to changes in smaller values. It is particularly useful in datasets with extreme values or outliers. The geometric mean is commonly used to calculate rates of change, such as growth or inflation rates. It is given as:

$$Gm = \sqrt[m]{a_1 \times a_2 \times .... a_m} \tag{24}$$

Where $a_1, a_2 ..., a_m$ are the observations.

(b) Fisher Score

Fisher score is an effective method for reducing data feature dimension. Its major goal is to discover a feature subset that maximizes the selected features in a data space. Techniques such as clustering and dimensionality reduction are utilized to decrease distances between data points within a class and increase distances between data points in different classes. The Fisher score of the $j^{th}$ feature is calculated as:

$$FS1\left(f_j\right)=\frac{L_y(f_j)}{\sum_{K=1}^{E} L_T^{(K)}(f_j)} \tag{25}$$

Where $L_y(f_j)$ is the between-class scatter, which measures the spread of data points between different classes in a selected feature space, and $L_T^{(K)}\left(f_j\right)$ is the within-class scatter, which measures the spread of data points within each class for a particular feature. The between-class scatter of the $j^{th}$ feature is calculated by taking the sum of the squared differences across the mean $\mu_j$ of the $j^{th}$ feature in each class and the overall mean $\mu_j^{(K)}$ of the $j^{th}$ feature, multiplied by the number of samples $m_K$ in each class:

$$L_y\left(f_j\right)=\sum_{K=1}^{E} m_K(\mu_j^{(K)}-\mu_j)^2 \tag{26}$$

The within-class scatter matrix of the $j^{th}$ feature calculates the variance of that feature in the $K^{th}$ class by summing the squared differences between each data point and the mean of $j^{th}$ feature in the same class:

$$L_T^{(K)}\left(f_j\right)=\sum_{i=1}^{m_K}(a_{ji}^{(K)}-\mu_j^{(K)})^2 \tag{27}$$

Finally, the features are combined and the results are stored.

### 3.2. Authentication

Authentication is the second phase of the model, which uses the finger images as the input. In this phase, the input finger images are pre-processed, and features are extracted and selected using approaches similar to those employed during the enrollment phase. Once the feature selection is completed, blockchain (Akanfe et al., 2024) technology is used to securely transfer the generated data. With the use of a fixed distributed database and a hash chain of blocks that each include time-stamped transactions, this system organizes data. Every block in the chain has a distinct code, or hash, that identifies it and establishes a sequential relationship with the blocks that came before it. The hash function employed in blockchain depends on several important factors for its success.

On secure transmission of data through the blockchain, finally, the Fusion Net-3 architecture is used to detect real and fake fingerprints (Fig. 2). CNNs, ResNet-50, and U-Net are combined to provide an efficient method for extracting and processing image features. Raw picture data are first fed into the network to start the process. The CNN-ResNet-50 (Wang et al., 2020) branch uses convolutional layers to extract local image features, batch normalization to normalize these features, and activation functions to introduce non-linearity. To obtain robust features and reduce computational costs, feature maps are down-sampled through pooling layers. Deeper architectures are made possible by ResNet-50 blocks, which solve the vanishing gradient issue in deep NNs. The encoder-decoder structure used by the U-Net (Wang & Yang, 2024) branch allows it to extract both high-level and low-level image features simultaneously. While pooling layers down-sample features in the encoder path, convolutional layers extract local features at various scales. In the decoder path, up-sampling layers retrieve spatial information and merge features from corresponding encoder and decoder layers. The complementary information is then combined by merging the feature maps from the two branches. To map features to class probabilities, a fully connected layer receives this flattened representation of the combined features. The ultimate class probabilities for classification are output by a SoftMax layer.

#### 3.2.1. Convolutional neural network–Resnet-50

Convolutional layers are usually the most important components in CNNs. At each convolutional layer, the input is convolved with an array of learnable filters, yielding a variety of feature maps. Let $s_i$ represent $i^{th}$ feature map of $S$. We can utilize the weight $W_k$ and bias $b_k$ to characterize the $c^{th}$ filter. The $k^{th}$ output is given as:

$$y_k=\sum_{i=1}^{d} f\left(s_i\times W_k+b_k\right);\ \mathrm{k}=1,\ 2,\ \mathrm{n} \tag{28}$$

Where f (•) is an activation function, while $W_k$ and $b_k$ are weights and bias, respectively. The extraction of local features from input fingerprint images is largely dependent on the CNN component. It identifies images' patterns and textures, both of which are essential for fingerprint recognition, by applying convolutional filters to images.

A 50-layer network, called ResNet-50, has demonstrated efficacy in pre-trained image classification. Deeper NN trainings are difficult due to disappearing gradient problems. Such problems are attempted to be addressed by residual learning. A layer that learns low- or high-level features is taught specifically for that task. Deep NN training can be stabilized and sped up with the use of batch normalization.

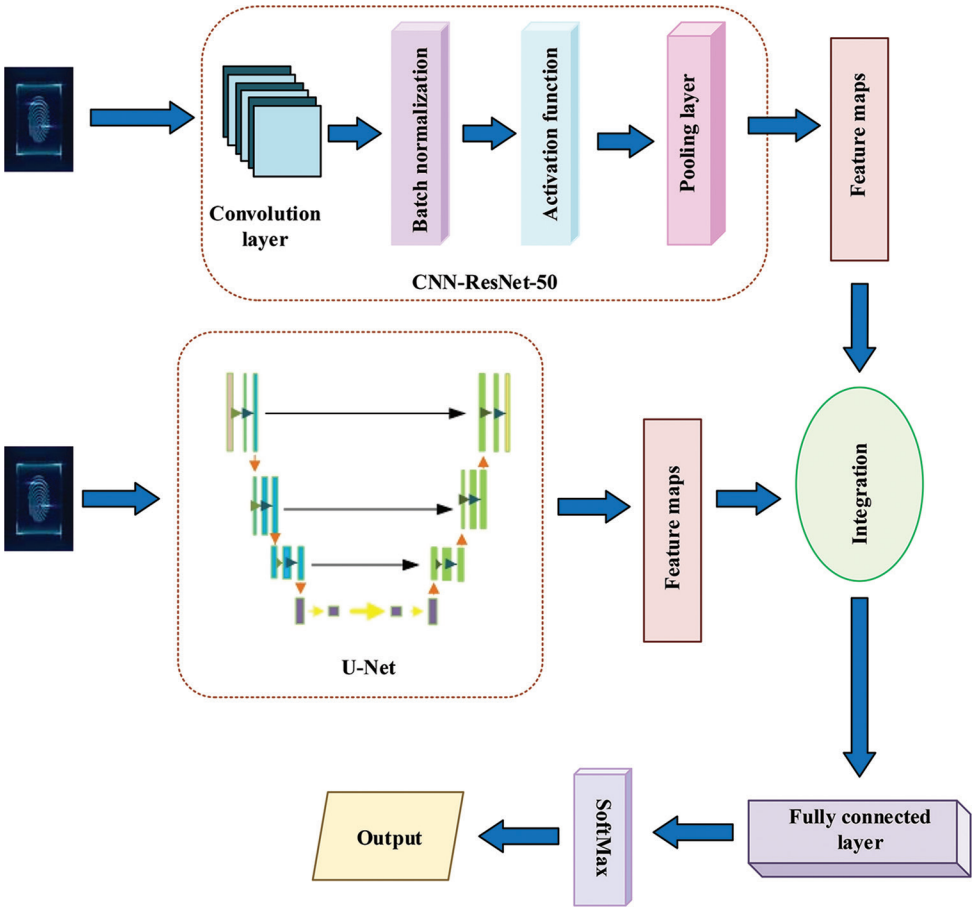


**Fig. 2.** Fusion Net-3 architecture

Fusion Net-3 integrates ResNet-50 into its architecture. The residual connections in the model enable the network to learn residual functions rather than directly approximating the underlying mapping. ResNet-50 allows Fusion Net-3 to train deeper NNs without sacrificing efficiency. In addition, batch normalization is applied to accelerate convergence and stabilize the training process.

Batch normalization works by modifying and scaling each layer's activations to normalize them. It is usually used before the activation function in ResNet-50, following the convolutional layers. Each feature map essentially generates a new mean and standard deviation for every pixel. The procedure involves normalizing the *z*-score, then multiplying the results by an arbitrary scale parameter ($\alpha$) and adding another arbitrary offset value ($\beta$). These are the specifications for the batch normalization.

$$s`=\left(\frac{(s-\mu)}{\sigma}\times\alpha\right)+\beta \tag{29}$$

Where s, s` are feature maps and batch-normalized value, element, and $\mu$ is the mean.

The activation function is used after batch normalization, improving non-linearity. The rectified linear unit (ReLU) is used, and it is given as:

$$\sigma(s) = max(0, s) \tag{30}$$

### 3.2.2. Pooling layer

At times, there is redundant information existing in signals. The pooling process reduces the spatial size of the feature maps steadily, reducing the computation and parameter count of the network. With an $n \times n$ window-size neighbor denoted as $P$, the standard pooling technique is represented as:

$$Z = \frac{1}{F}\sum_{i,j\epsilon P} s_{i,j} \tag{31}$$

Where $F$ is the number of elements in $P$, and $s_{i,j}$ is an activation value of position $i, j$.

### 3.2.3. U-Net

The U-Net architecture is used to extract contextual information and fine-grained details from images, providing pertinent data for categorization. In the Fusion Net-3 model, the U-Net component is crucial for extracting both high-level and low-level features from the input fingerprint. The autoencoder architecture, in which the left path (encoder) is referred

to as the contracting or compressive path and is built on a standard CNN deep network, is the most similar to the Fusion Net-3 model's basic structure, which consists of two main paths. The network's second path, known as the decoder or expanding path (also called the up-sampling or synthesis path in some references), is made up of both convolutional and deconvolutional layers. The expanding path uses optimized techniques, such as concatenating skip connections, to recover the input image resolution and spatial structure, which are both compromised during down-sampling. The network generates dense predictions at higher resolutions in the expanding path, helping it to learn spatial classification information. Furthermore, it increases the output's resolution, which is then transferred to the final convolutional layer to produce a segmented image with the same shape as the input image.

The contracting path is a typical CNN network, consisting of two successive 3 × 3 convolutions, followed by non-linear activations (e.g., ReLU), and a max pooling layer. This structure is repeated numerous times until the bottleneck is reached. The strided convolutions and pooling layers in the contracting path decrease dimensions while increasing the channel number and receptive field. This expanding path, which involves up-sampling feature maps from the bottleneck using 2 × 2 up-convolutions to recover the input image's dimensions, is where the novelty of the U-Net originates. There are normal 3 × 3 convolutions and ReLU activations along with a 2 × 2 up-convolution in every step of the expanding path. This path's up-sampling ability reduces the number of channels by half, while the image's width and height are increased through the up-convolution. After cropping, a concatenation from the same level layer in the feature map's contracting path is added to expand the image's dimensions, while the spatial features are preserved following each 2 × 2 up-convolution.

### 3.2.4. Fully connected layer

The combined output features of CNN–ResNet-50 and U-Net are input into the fully connected layer to improve detection accuracy. The output is input into the SoftMax function to predict the class of an input image.

$$\sigma(z) = \frac{\exp(z)}{\sum_{i=1}^{r} \exp(z_i)} \tag{32}$$

Where z and r are input and classes, respectively. These architectures are combined in Fusion Net-3, which is used in this study, to produce a strong feature representation that improves its ability to distinguish between real and fake fingerprints. ResNet-50 is used as a pre-trained backbone, while CNN and U-Net convolutional layers are configured based on empirical results. Key hyperparameters, including learning rate, batch size, number of epochs, dropout rate, and Adam optimizer, are selected based on grid search experiments from the training dataset. The FIJO algorithm is used to optimize feature selection, whereas hyperparameters and network topology are manually tuned to balance system performance and training time. When compared to using individual models alone, this integration improves fingerprint authentication's robustness and accuracy.

## 4. Results and Discussion

Performance indicators were used to assess the outcomes of the dataset obtained. The computed results were compared across the proposed model and existing models (CNN, ResNet-50, and GoogLeNet) through a Python platform. The results were computed by considering a learning rate of 70% for training and 30% for testing. The equations are shown as follows:

- Accuracy: It is the proportion of correctly predicted values to all observations, including total positive (TP), total negative (TN), false positive (FP), and false negative (FN). It is expressed as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{33}$$

- Precision: It is the percentage of a model's true positive predictions. Precision is key in determining whether an observation reflects a real phenomenon. It is stated as:

$$Precision = \frac{TP}{TP + FP} \tag{34}$$

- Recall: It is the percentage of true positives that are correctly identified. It is stated as:

$$Recall = \frac{TP}{TP + FN} \tag{35}$$

- F-measure: It is a statistic from the combination of precision and recall, serving as a general performance evaluation score. It is stated as:

$$F\bar{m}easure = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{36}$$

- Matthews correlation coefficient (MCC): It is the degree of correlation between the predicted and actual outcomes. It is expressed as:

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{37}$$

- Peak signal-to-noise ratio (PSNR): It is the ratio between the examined image and the recovered image. *Max* represents an image's maximum value, where the maximum value is 255 if 8 bits/sample are utilized to represent the pixel. Higher PSNR indicates better quality. It is given as:

$$PSNR = 10log\left(\frac{Max^2}{MSE}\right) \quad (38)$$

- Mean squared error (MSE): It is a regression model's confidence measure, indicating the error between predicted class probabilities and true labels. A lower MSE value indicates stronger prediction confidence, especially when using soft probability outputs from the SoftMax layer. The average squared variance of the actual and predicted values is MSE. It is expressed as:

$$MSE = \frac{1}{N}\sum_{x=1}^{N}\left[Z_x - \widehat{Z_x}\right]^2 \quad (39)$$

Where $Z_c$ and $\widehat{Z_c}$ are the actual and projected values, respectively, and $V$ is the total number of data points.

- False acceptance rate (FAR): It is calculated by dividing the number of false-positive recognitions by the total number of identified attempts. It is expressed as:

$$FAR = \frac{FP}{FP + TN} \times 100 \quad (40)$$

- False rejection rate (FRR): It is the number of false rejections divided by the total number of transactions. A lower FRR indicates that fewer cases are being rejected by the biometric system. It is expressed as:

$$FRR = \frac{FN}{FN + TP} \times 100 \quad (41)$$

### 4.1. Parameter Evaluation

Performance measures, including accuracy, precision, recall, F1-score, MCC, MSE, FAR, and FRR, were used to evaluate the proposed Fusion Net-3 model and conventional strategies (CNN, ResNet-50, and GoogLeNet) for three datasets (LUMID, LivDet, and Biometrika; refer to Appendix A1). The models' numerical results for Datasets 1, 2, and 3 are shown in Tables 2-4, respectively.

Fig. 3 shows the graphical analysis of accuracy and precision of all tested models across databases, with the Fusion Net-3 model achieving the highest accuracy of 98.956%. In Dataset 2, the accuracy of the proposed model (95.654%) outperformed other models, followed by GoogLeNet (93.876%), ResNet-50 (92.654%), and CNN (91.765%). Similarly,

**Table 2.** Numerical results for Dataset 1 by models

| Parameter | Fusion Net-3 | CNN | ResNet-50 | GoogLeNet |
|---|---|---|---|---|
| Accuracy (%) | 98.956 | 94.562 | 95.632 | 96.327 |
| Precision (%) | 98.548 | 94.685 | 95.975 | 96.852 |
| Recall (%) | 98.967 | 94.536 | 95.524 | 96.384 |
| F-measure (%) | 98.675 | 94.687 | 95.862 | 96.247 |
| MCC (%) | 98.635 | 94.368 | 95.427 | 96.784 |
| FAR (%) | 15.573 | 45.453 | 34.543 | 52.112 |
| FRR (%) | 19.534 | 46.642 | 36.8765 | 48.765 |
| PSNR (dB) | 18.524 | 15.527 | 14.753 | 12.864 |
| Time complexity | 5.324 | 9.325 | 8.357 | 7.368 |
| MSE | 0.0234 | 0.0612 | 0.0560 | 0.0474 |

Abbreviations: CNN: Convolutional neural network; MCC: Matthews correlation coefficient; MSE: Mean squared error; PSNR: Peak signal-to-noise ratio.

**Table 3.** Numerical results for Dataset 2 by models

| Parameter | Fusion Net-3 | CNN | ResNet-50 | GoogLeNet |
|---|---|---|---|---|
| Accuracy (%) | 95.654 | 91.765 | 92.654 | 93.876 |
| Precision (%) | 94.876 | 91.543 | 92.876 | 92.543 |
| Sensitivity | 94.123 | 91.876 | 92.543 | 92.432 |
| Specificity | 93.543 | 91.321 | 92.654 | 92.765 |
| Recall (%) | 94.432 | 91.765 | 92.876 | 92.654 |
| F-measure (%) | 93.765 | 91.654 | 92.765 | 92.876 |
| MCC (%) | 93.432 | 90.876 | 91.876 | 92.123 |
| FAR (%) | 12.987 | 22.876 | 21.543 | 17.654 |
| FRR (%) | 10.543 | 23.654 | 20.876 | 18.543 |
| PSNR (dB) | 32.432 | 29.876 | 16.432 | 15.876 |
| Time complexity | 5.987 | 17.543 | 16.432 | 15.654 |
| MSE | 0.0201 | 0.1123 | 0.0987 | 0.0912 |

Abbreviations: CNN: Convolutional neural network; FAR: False acceptance rate; FRR: False rejection rate; MCC: Matthews correlation coefficient; MSE: Mean squared error; PSNR: Peak signal-to-noise ratio.

in Dataset 3, Fusion Net-3 recorded an accuracy of 95.432%, markedly higher than those of CNN (92.876%), ResNet-50 (93.654%), and GoogLeNet (94.876%). The proposed model's precision was 98.548%, indicating a better performance compared to CNN, ResNet-50, and GoogLeNet. In Datasets 2 and

3, the proposed model achieved the highest precision of 94.876% and 95.654%, respectively, indicating accurate fingerprint classification. This precision value is markedly higher than those in previous works by Yin et al. (2019).

Fig. 4 compares the recall and F-measure results of the tested models. The Fusion Net-3 model achieved the highest recall with a value of 98.967%, outperforming CNN, ResNet-50, and GoogLeNet. The proposed model's recall values were 94.432% for Dataset 2 and 95.543% for Dataset 3, also outperforming other models. Similarly, the F-measure of the proposed model was 98.675% for Dataset 1, markedly higher than CNN, ResNet-50, and GoogLeNet. Its F-measure values were 93.765% for Dataset 2 and 95.432% for Dataset 3. These findings indicate the proposed model's superiority over other models in previous research by Zheng et al. (2019). They also highlight the importance of considering both recall and F-measure in the development of effective machine learning models.

The graphical analyses of MCC and MSE are presented in Fig. 5. The results showed that the MCC of the Fusion Net-3 model has a higher MCC value of 98.635% in comparison to CNN, ResNet-50, and GoogLeNet, which recorded 94.368%, 95.427%, and 96.784%, respectively, in Dataset 1. In Datasets 2 and 3, the MCC of the proposed model also demonstrated the highest values of 93.432% and 94.654%, respectively. These results indicate that Fusion Net-3 is superior to the models in previous research Akanfe et al. (2024). Meanwhile, the comparison results across the tested models in terms of MSE showed that, in Dataset 1, the Fusion Net-3 model achieved a lower rate, with a MSE value of 0.0234, compared to CNN (0.0612), ResNet-50 (0.0560), and GoogLeNet (0.0474). In Datasets 2 and 3, the proposed model's MSEs were 0.0201 and 0.0434, respectively. Although the error rate was comparatively low, some research Stolk & Sbrizzi (2019) reported even lower rates, highlighting the need for further research in this area.

**Table 4.** Numerical results for Dataset 3 by models

| Parameter | Fusion Net-3 | CNN | ResNet-50 | GoogLeNet |
|---|---|---|---|---|
| Accuracy (%) | 95.432 | 92.876 | 93.654 | 94.876 |
| Precision (%) | 95.654 | 92.543 | 93.432 | 94.543 |
| Sensitivity | 95.321 | 92.654 | 93.876 | 94.321 |
| Specificity | 94.876 | 92.876 | 93.543 | 94.876 |
| Recall (%) | 95.543 | 92.765 | 93.432 | 94.654 |
| F-Measure (%) | 95.432 | 92.876 | 93.654 | 94.876 |
| MCC (%) | 94.654 | 91.543 | 92.654 | 94.123 |
| FAR (%) | 12.543 | 20.654 | 18.543 | 15.654 |
| FRR (%) | 10.876 | 21.876 | 19.876 | 16.432 |
| PSNR (dB) | 32.654 | 30.876 | 31.765 | 30.876 |
| Time complexity | 9.123 | 16.654 | 15.876 | 10.543 |
| MSE | 0.0434 | 0.1034 | 0.0976 | 0.0897 |

Abbreviations: CNN: Convolutional neural network; FAR: False acceptance rate; FRR: False rejection rate; MCC: Matthews correlation coefficient; MSE: Mean squared error; PSNR: Peak signal-to-noise ratio.

#### 4.1.1. Time complexity

The graphical analysis of time complexity is presented in Fig. 6. Time complexity is a measure of computing difficulty that characterizes how long a model takes to execute. The results revealed that the proposed model exhibited a lower time complexity of 5.324, compared to CNN (9.325), ResNet-50 (8.357), and GoogLeNet (7.368). In Datasets 2 and 3, the time complexity values of the proposed model were 5.987 and 9.123, respectively, indicating a higher efficiency than the other models. With its lower time complexity, along with superior precision and accuracy, the proposed model outperformed all other models in the

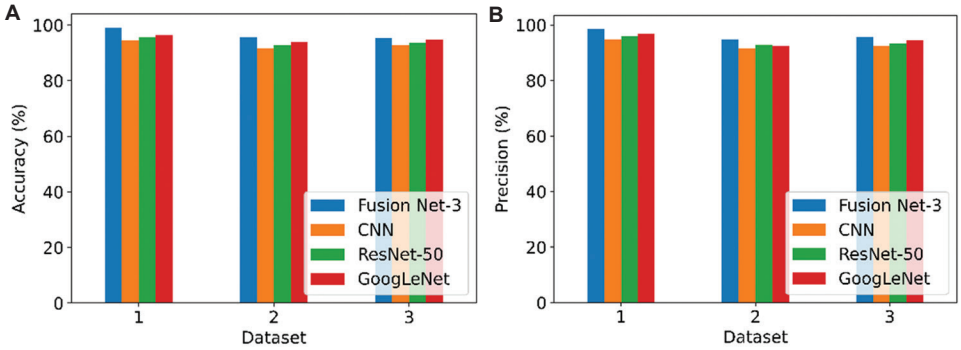


**Fig. 3.** Graphical representation of the (A) accuracy and (B) precision results
Abbreviation: CNN: Convolutional neural network

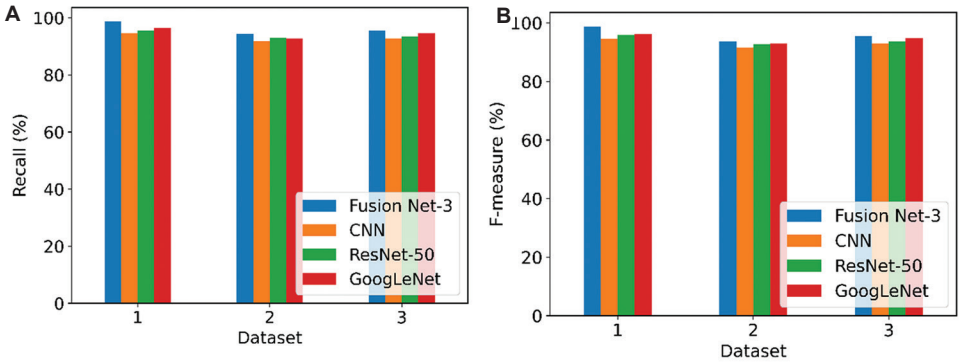


**Fig. 4.** Graphical representation of the (A) recall and (B) F-measure analysis
Abbreviation: CNN: Convolutional neural network

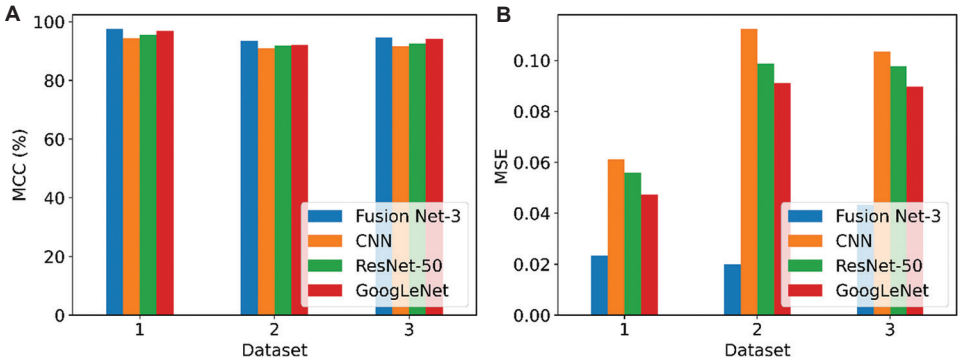


**Fig. 5.** Graphical representation of the (A) Matthews correlation coefficient (MCC) and (B) mean squared error (MSE) analysis
Abbreviation: CNN: Convolutional neural network

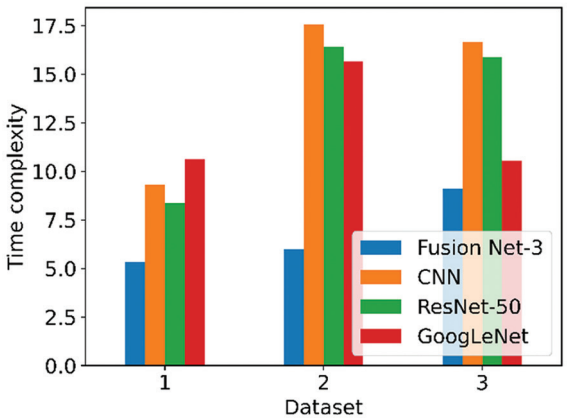


**Fig. 6.** Time complexity analysis
Abbreviation: CNN: Convolutional neural network

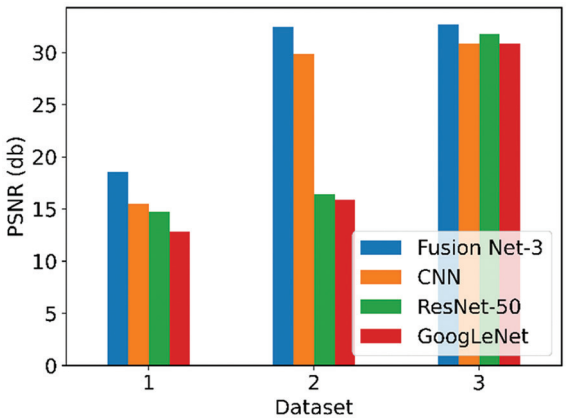


**Fig. 7.** Peak signal-to-noise ratio analysis
Abbreviation: CNN: Convolutional neural network

present study as well as in earlier research Arini et al. (2022) and Chopra & Ansari (2022).

The PSNR graphical analysis is displayed in Fig. 7. The results revealed that, in Dataset 1, the PSNR of the Fusion Net-3 model attained a higher value of 18.524 dB, compared to CNN (15.527 dB), ResNet-50 (14.753 dB), and GoogLeNet (12.864 dB). In Datasets 2 and 3, the PSNR values of the proposed model were 32.432 dB and 32.654 dB, respectively, suggesting better image clarity. Notably, previous research has reported lower PSNR values than the proposed model.

Fig. 8 shows the FAR and FRR of the tested models. The results showed that, in Dataset 1, the FAR of the Fusion Net-3 model exhibited a superior performance with an FAR of 0.5%, compared to CNN (1.2%), ResNet-50 (1.6%), and GoogLeNet (1.9%). In Datasets 2 and 3, the FARs of Fusion Net-3 were relatively lower at 12.987% and 12.543%, respectively.

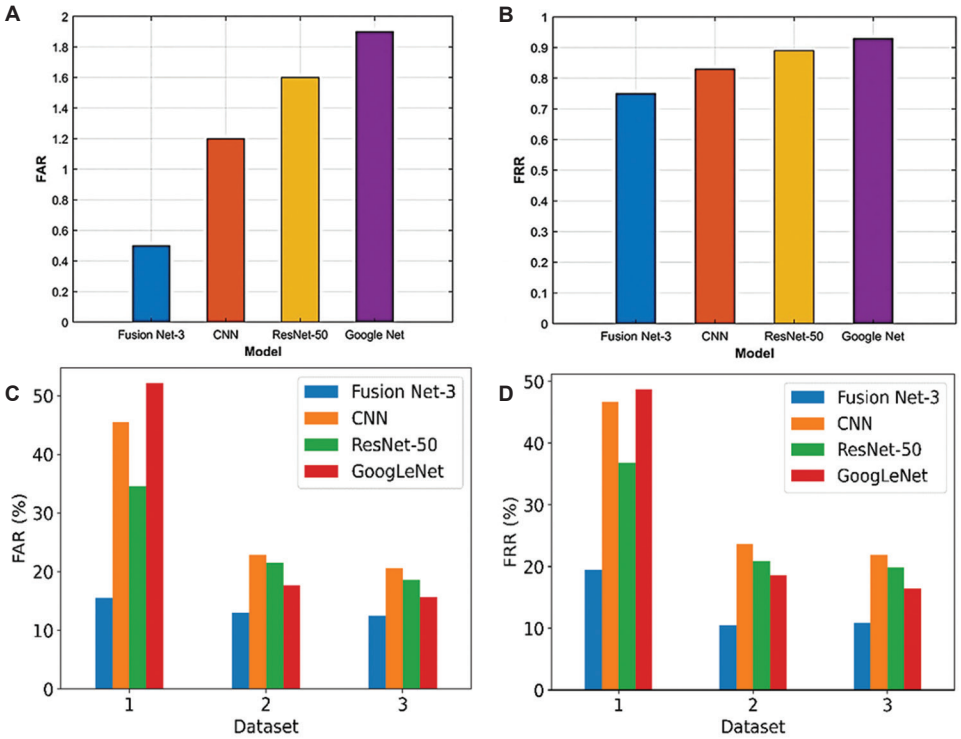


**Fig. 8.** Graphical representation of the (A) false acceptance rate and (B) false rejection rate by models
Abbreviation: CNN: Convolutional neural network

These comparatively low FAR results indicate a strong reliability of the proposed model. Besides, in Dataset 1, the FRR of the Fusion Net-3 model was 0.75%, lower than those of CNN (0.83%), ResNet-50 (0.89%), and GoogLeNet (0.93%). In Datasets 2 and 3, the FRRs of Fusion Net-3 were 10.543% and 10.876%, respectively. These findings suggest the reliability of the proposed model when compared with the other models.

#### 4.1.2. Computational complexity

This section presents the performance of computational complexity in runtime measurements. As shown in Table 5, the Fusion Net-3 model demonstrates superior runtime performance compared to the other models. The higher flop performance indicates the superiority of the proposed model over the other models.

**Table 5.** Performance of flops across models

| Model | Flops |
|---|---|
| CNN | $634\times10^9$ |
| ResNet-50 | $1.57\times10^9$ |
| GoogLeNet | $3.80\times10^9$ |
| Fusion Net-3 | $4.20\times10^9$ |

Abbreviation: CNN: Convolutional neural network.

### 4.2. Statistical Analysis

The statistical analysis evaluates the performance and data balance of the Fusion Net-3 model using various statistical tests, such as the Mann–Whitney *U*-test, Kruskal–Wallis test, and chi-squared test. These tests were applied to a balanced dataset to assess whether the models exhibit statistically significant differences. Fig. 9A-C illustrates the results of the chi-squared test, Kruskal–Wallis test, and Mann–Whitney *U*-test, respectively.

Significant differences were observed between expected and observed image counts across categories, especially in the "Altered-easy," "Altered-medium," and "Real" categories. To ensure the proposed approach was trained and assessed on a balanced dataset, statistical tests were used to detect dataset imbalances. Table 6 depicts a comparison of the three statistical tests in terms of mean, error, and *p*-value.

With an error of 36,680.745 and $p$=0.0300, the results displayed a high Chi-squared statistic of 4,497,877.2. This result illustrates notable variations and potential biases in the procedures used to define categories or collect data. When two independent groups were compared using the Mann–Whitney *U*-test, the results showed a mean of 4,630,356.2, an error of 45,933.445, and $p$=0.0146. These results suggest a

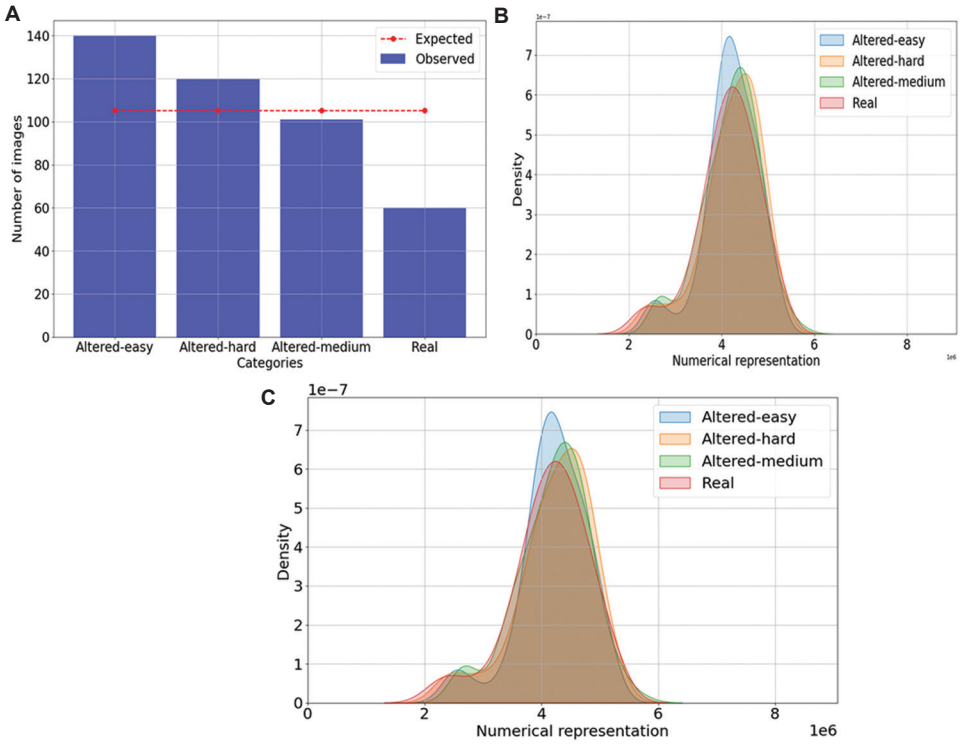


**Fig. 9.** Statistical analyses of the Fusion Net-3 model. (A) Chi-squared test. (B) Kruskal–Wallis test. (C) Mann–Whitney *U*-test

**Table 6.** Comparison of the statistical tests of Fusion Net-3

| Statistical test | Mean | Error | *p*-value |
|---|---|---|---|
| Chi-square test | 4,497,877.2 | 36,680.745 | 0.0300 |
| Mann–Whitney *U*-test | 4,630,356.2 | 45,933.445 | 0.0146 |
| Kruskal–Wallis test | 4,564,060.8 | 38,432.850 | $4.04\times10^{-49}$ |

significant difference between the groups compared, adding to the evidence supporting the effectiveness of the proposed Fusion Net-3 model in various scenarios. Notably, when comparing more than two groups, the Kruskal–Wallis test yielded a mean of 4,564,060.8, an error of 38,432.850, and an incredibly low $p=4.04\times10^{-49}$. This remarkably low *p*-value indicates significant variations across the groups, underscoring the resilience and efficacy of the proposed model. The combined outcomes of these experiments indicate that the Fusion Net-3 model performs noticeably better than CNN, ResNet-50, and GoogLeNet, while effectively managing dataset imbalances.

### 4.3. Different Adversarial Attack Comparison

Tables 7-9 compare the Fusion Net-3 model with existing fingerprint authentication methods, focusing on accuracy as a common metric due to the lack of publicly available metrics, such as precision, recall, and MCC, in many baseline studies. Table 7 presents the robustness of fingerprint authentication models against adversarial attacks using the fast gradient sign method (FGSM). Fusion Net-3 exhibited the highest accuracy of 98.956%, surpassing CNN (94.562%), ResNet-50 (95.632%), and GoogLeNet (96.327%). The table also presents the adversarial samples' impact, where Fusion Net-3 demonstrated a minimal impact with an adversarial sample value of 0.37678, compared to CNN (0.32263), ResNet-50 (0.36442), and GoogLeNet (0.36010). These findings imply that Fusion Net-3 is more resistant to adversarial attacks, even in the presence of potential perturbations in fingerprint image input.

Table 8 details the accuracy obtained by fingerprint-based authentication models when subjected to adversarial attacks generated using the projected gradient descent (PGD) method. The proposed model reported an accuracy of 98.245%, outperforming CNN (92.654%), ResNet50 (93.432%), and GoogleNet (92.543%). The minimum difference was noted with Fusion Net-3 models at 0.38234, compared to larger differences recorded for CNN (0.32212), ResNet-50 (0.33345), and GoogLeNet (0.34123). These results indicate that Fusion Net-3 offers superior resilience to PGD attacks, retaining high accuracy with minimal degradation in the presence of adversarial perturbations.

**Table 7.** Accuracy and adversarial samples of models against black-box attack using fast gradient sign method

| Dataset | Metric | Fusion Net-3 | CNN | ResNet-50 | GoogLeNet |
|---|---|---|---|---|---|
| 1 | Accuracy (%) | 98.956 | 94.562 | 95.632 | 96.327 |
| | Adversarial samples | 0.37678 | 0.32263 | 0.36442 | 0.360100 |
| 2 | Accuracy (%) | 98.234 | 92.543 | 92.123 | 96.327 |
| | Adversarial samples | 0.36749 | 0.31122 | 0.35895 | 0.34921 |
| 3 | Accuracy (%) | 97.932 | 93.765 | 93.432 | 92.327 |
| | Adversarial samples | 0.39234 | 0.32865 | 0.36675 | 0.35472 |

Abbreviation: CNN: Convolutional neural network.

**Table 8.** Accuracy and adversarial samples of models against black-box attack using projected gradient descent

| Dataset | Metric | Fusion Net-3 | CNN | ResNet-50 | GoogLeNet |
|---|---|---|---|---|---|
| 1 | Accuracy (%) | 98.245 | 92.654 | 93.432 | 92.543 |
| | Adversarial samples | 0.38234 | 0.32212 | 0.33345 | 0.34123 |
| 2 | Accuracy (%) | 98.543 | 93.234 | 93.765 | 92.543 |
| | Adversarial samples | 0.37122 | 0.30643 | 0.31434 | 0.32344 |
| 3 | Accuracy (%) | 97.976 | 94.432 | 93.432 | 92.543 |
| | Adversarial samples | 0.36533 | 0.34245 | 0.33123 | 0.32875 |

Abbreviation: CNN: Convolutional neural network.

**Table 9.** Accuracy and adversarial samples of models against black-box attacks using a replay attack

| Dataset | Metric | Fusion Net-3 | CNN | ResNet-50 | GoogLeNet |
|---|---|---|---|---|---|
| 1 | Accuracy (%) | 97.542 | 92.643 | 93.234 | 92.123 |
| | Adversarial samples | 0.37455 | 0.30865 | 0.31235 | 0.32133 |
| 2 | Accuracy (%) | 97.654 | 93.765 | 92.876 | 92.123 |
| | Adversarial samples | 0.37546 | 0.33434 | 0.32675 | 0.32764 |
| 3 | Accuracy (%) | 98.123 | 92.876 | 93.76 | 92.123 |
| | Adversarial samples | 0.38123 | 0.34342 | 0.32450 | 0.31457 |

Abbreviation: CNN: Convolutional neural network.

Table 9 summarizes the replay attack resilience of the models. Replay attacks try to cheat the system using replayed biometric data captured previously. Fusion Net-3 demonstrated the highest performance with an accuracy of 97.542%, compared to CNN (92.643%), ResNet-50 (93.234%), and GoogLeNet (92.123%). The value of the adversarial sample of Fusion Net-3 was 0.37455, lower than CNN (0.30865), ResNet-50 (0.31235), and GoogLeNet (0.32133). The results indicate that Fusion Net-3 is effective in countering threats from adversarial replay attacks, making it a secure solution for fingerprint authentication.

### 4.4. Results in the Pre-Processing and Feature Selection Phases of the Models

Denoising performance was evaluated using the signal-to-noise ratio (SNR). The ratio measures the proportion of the image's valuable information relative to undesired artifacts or disruptions. Denoising the input images during the pre-processing phase revealed that the proposed improved bilateral filtering method achieved a higher SNR of 20.8 dB. In comparison, the median and Gaussian filters produced lower SNRs of 17.3 dB and 18.6 dB, respectively.

Feature selection using optimization, which is used for selecting the accurate features, demonstrated that the proposed Fusion Net-3 model outperformed existing algorithms by achieving a 98.12% performance. In comparison, the FOA and GJO achieved lower performances of 97.35% and 97.65%, respectively.

The accuracy of 98.956% achieved by the proposed model surpasses that of previous research Srinivasan et al. (2023), Trivedi et al. (2020), indicating its superiority over the other models used in this paper and those from previous works by other researchers. The enhanced bilateral filtering approach for denoising and the combination of CNN–ResNet-50 and U-Net features are some of the architectural enhancements

that contribute to the superior performance of the proposed Fusion Net-3 model. Feature extraction and noise reduction are enhanced by these factors, resulting in increased accuracy and robustness. The model's capacity to preserve excellent image quality and prediction accuracy is further supported by the lower MSE and higher PSNR. In addition, the computational efficiency of the proposed method is also enhanced, with a time complexity of 5.324, demonstrating its usefulness in real-world applications.

The graphical analysis of receiver operating characteristic for the proposed and existing methods is shown in Fig. 10. Fusion Net-3 exhibited the highest area under the curve score (0.97), indicating its superior ability to balance reducing false positives (high specificity) with accurately identifying positive cases (high sensitivity).

The study's findings show that the proposed Fusion Net-3 model consistently outperforms other models, CNN, ResNet-50, and GoogLeNet, in a number of performance metrics. Specifically, Fusion Net-3 achieves an accuracy of 98.956%, surpassing CNN (94.562%), ResNet-50 (95.632%), and GoogLeNet (96.327%). It also exhibits higher precision (98.548%), recall (98.967%), and F-measure (98.675%) than the other models. In addition, Fusion Net-3 performs better than other models according to the MCC, which stands at 98.635%. This suggests a strong correlation between expected and actual outcomes. Furthermore, the proposed model outperforms the other models in its resilience to black-box attacks using FGSM, attaining an accuracy of 98.956% against adversarial samples.

The proposed model of Fusion Net-3 demonstrates an accuracy level of 98.956%, alongside enhanced security features that address crucial challenges in fingerprint-based authentication,

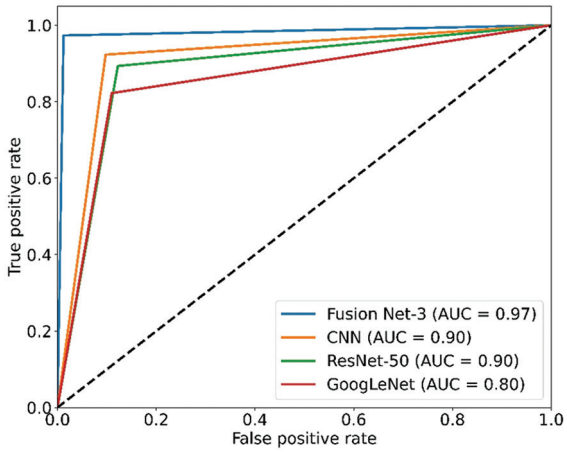


**Fig. 10.** Receiver operating characteristic curve analysis
Abbreviations: AUC: Area under the curve; CNN: Convolutional neural network

including noise reduction, feature extraction, and resistance to cyberattacks. In industries such as finance, healthcare, and national security, where the integrity of data and authenticity are important, this model would improve access control mechanisms, reduce fraud cases, and enhance operational efficiency. Moreover, the integration of blockchain technology in the model ensures secure data transmission, making it a viable solution for large-scale deployments in government and corporate settings. Furthermore, improved processing speed and low error rates also make it suitable for real-time applications, such as mobile authentication and border control systems, fostering wider acceptance of biometric security solutions. Such advances not only raise the confidence level of users in biometric systems but also pave the way for integrating them with newer technologies, such as Internet of Things-enabled smart environments and automated customer service kiosks.

The most significant limitation of this study is the variability in fingerprint image quality due to variations in acquisition devices, environment, and user-related inconsistencies. This may introduce noise and degrade the robustness of the model. In addition, adversarial attacks still pose a threat since an intelligent spoofing technique can potentially bypass the system with advanced security functionalities. To address these limitations, future work should expand the dataset diversity, improve computational efficiency, and further strengthen resilience against emerging attack vectors.

## 5. Conclusion

A fingerprint-based authentication system is a biometric authentication method that uses multiple techniques to enhance overall security and authentication accuracy. This study proposes the denoising-based Fusion Net-3 model to address the shortcomings of the currently existing methods. There are two stages to it: enrollment and authentication. The scanned information of hands is collected and pre-processed in the first phase using enhanced bilateral filtering, where the filter parameters are optimized using an SOA and the images are enhanced using a contrast enhancement technique. The pre-processed output is then used to extract features based on shapes and textures. Ultimately, a unique FIJO algorithm, a combination of the FOA and GJO algorithms, is used for feature selection to extract the optimal features. The selected features are combined using geometric mean and Fisher score. In the second phase, the fingerprint images are input and undergo pre-processing, feature extraction, and feature selection using similar methods utilized during the enrolment phase. The efficient (correct or incorrect) fingerprints are detected using the Fusion Net-3 model, which combines CNN,

ResNet-50, and U-Net models. By implementing the proposed model on the Python platform, it achieved an accuracy of 98.956%, a precision of 98.548%, a recall of 98.967%, an F-measure of 98.675%, an MCC of 98.635%, a time complexity of 5.324, a PSNR of 18.524 dB, and an MSE of 0.0234. The Fusion Net-3 model outperforms the currently existing models based on these results. The proposed model is a classifier with high performance, but it has limitations, such as being influenced by poor-quality fingerprints and computational costs. Further work includes multimodal biometric systems and lightweight NNs in mobile or embedded systems, as well as investigating adversarial robustness and real-time spoof detection.

## 6. Acknowledgments

The authors would like to thank the Deanship of Cochin University of Science and Technology for their institutional support of this work.

## References

Abolfathi, M., Inturi, S., Banaei-Kashani, F., & Jafarian, J.H. (2024). Toward enhancing web privacy on HTTPS traffic: A novel SuperLearner attack model and an efficient defense approach with adversarial examples. *Computers and Security*, 139, 103673. https://doi.org/10.1016/j.cose.2023.103673

Abolfathi, M., Shomorony, I., Vahid, A., & Jafarian, J.H. (2022). A game-Theoretically Optimal Defense Paradigm Against Traffic Analysis Attacks using Multipath Routing and Deception. In: *Proceedings of the 27th ACM Symposium on Access Control Models and Technologies*, p67–78. https://doi.org/10.1145/3532105.3535015

Adiga, V.S., & Sivaswamy, J. (2019). Fpd-m-net: Fingerprint image denoising and inpainting using m-net based convolutional neural networks. In: *Inpainting and Denoising Challenges*. Cham: Springer International Publishing, p51–61. https://doi.org/10.1007/978-3-030-25614-2_4

Afshari, H.H., Gadsden, S.A., & Habibi, S. (2017). Gaussian filters for parameter and state estimation: A general review of theory and recent trends. *Signal Processing*, 135, 218–238. https://doi.org/10.1016/j.sigpro.2017.01.001

Akanfe, O., Lawong, D., & Rao, H.R. (2024). Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, 76, 102753. https://doi.org/10.1016/j.ijinfomgt.2024.102753

Akter, A., Nosheen, N., Ahmed, S., Hossain, M., Yousuf, M.A., Almoyad, M.A.A., et al. (2024). Robust clinical applicable CNN and U-Net based algorithm for MRI classification and segmentation for brain tumor. *Expert Systems with Applications*, 238, 122347. https://doi.org/10.1016/j.eswa.2023.122347

Algarni, M.H. (2024), Fingerprint sequencing: An authentication mechanism that integrates fingerprints and a knowledge-based methodology to promote security and usability. *Engineering, Technology and Applied Science Research*, 14(3), 14233–14239. https://doi.org/10.48084/etasr.7250

Ali, S.S., Baghel, V.S., Ganapathi, I.I., & Prakash, S. (2020). Robust biometric authentication system with a secure user template. *Image and Vision Computing*, 104, 104004. https://doi.org/10.1016/j.imavis.2020.104004

Arini, F.Y., Sunat, K., & Soomlek, C. (2022). Golden jackal optimization with joint opposite selection: An enhanced nature-inspired optimization algorithm for solving optimization problems. *IEEE Access*, 10, 28800–128823. Available from: https://www.kaggle.com/datasets/ruizgara/socofing

Balsiger, F., Jungo, A., Scheidegger, O., Carlier, P.G., Reyes, M., & Marty, B. (2020). Spatially regularized parametric map reconstruction for fast magnetic resonance fingerprinting. *Medical Image Analysis*, 64, 101741. https://doi.org/10.1016/j.media.2020.101741

Banitaba, F.S., Aygun, S., & Najafi, M.H. (2024). *Late Breaking Results: Fortifying Neural Networks: Safeguarding Against Adversarial Attacks with Stochastic Computing*. [arXiv Preprint].

Chopra, N., & Ansari, M.M. (2022). Golden jackal optimization: A novel nature-inspired optimizer for engineering applications. *Expert Systems with Applications*, 198, 116924.

Dhiman, G., & Kumar, V. (2019). Seagull optimization algorithm: Theory and its applications for large-scale industrial engineering problems. *Knowledge-Based Systems*, 165, 169–196. https://doi.org/10.1016/j.knosys.2018.11.024.

Ding, B., Wang, H., Chen, P., Zhang, Y., Guo, Z., Feng, J., et al. (2020). Surface and internal fingerprint reconstruction from optical coherence tomography through convolutional neural network. *IEEE Transactions on Information Forensics and Security*, 16, 685–700. https://doi.org/10.1109/TIFS.2020.3016829

Ephin, M., & Vasanthi, N.A. (2013). A highly secure integrated biometrics authentication using finger-palmprint fusion. International Journal of Scientific and Engineering Research, 4(1).

Galbally, J., Beslay, L., & Böstrom, G. (2020).

3D-FLARE: A touchless full-3D fingerprint recognition system based on laser sensing. *IEEE Access*, 8, 145513–145534. https://doi.org/10.1109/ACCESS.2020.3014796

Gao, Z., Gao, Y., Wang, S., Li, D., Xu, Y. (2020). CRISLoc: Reconstructable CSI fingerprinting for indoor smartphone localization. *IEEE Internet of Things Journal*, 8(5), 3422–3437. https://doi.org/10.1109/JIOT.2020.3022573

Gavaskar, R.G., & Chaudhury, K.N. (2018). Fast adaptive bilateral filtering. *IEEE Transactions on Image Processing*, 28(2), 779–790. https://doi.org/10.1109/TIP.2018.2871597

Gupta, R., Khari, M., Gupta, D., & Crespo, R.G. (2020). Fingerprint image enhancement and reconstruction using the orientation and phase reconstruction. *Information Sciences*, 530, 201–218. https://doi.org/10.1016/j.ins.2020.01.031

Husson, L., Bodin, T., Spada, G., Choblet, G., & Kreemer, C. (2018). Bayesian surface reconstruction of geodetic uplift rates: Mapping the global fingerprint of Glacial Isostatic Adjustment. *Journal of Geodynamics*, 122, 25–40. https://doi.org/10.1016/j.jog.2018.10.002

Jia, H., Xing, Z., & Song, W. (2019). A new hybrid seagull optimization algorithm for feature selection. *IEEE Access*, 7, 49614–49631. https://doi.org/10.1109/ACCESS.2019.2909945

Kareem, S.W., & Okur, M.C. (2021). Falcon optimization algorithm for bayesian network structure learning. *Computer Science*, 22, 553–569. https://doi.org/10.7494/csci.2021.22.4.3773

Khodadoust, J., Khodadoust, A.M., Mirkamali, S.S., & Ayat, S. (2020). Fingerprint indexing for wrinkled fingertips immersed in liquids. *Expert Systems with Applications*, 146, 113153. https://doi.org/10.1016/j.eswa.2019.113153

Koonce, B., & Koonce, B.E. (2021). *Convolutional Neural Networks with Swift for Tensorflow: Image Recognition and Dataset Categorization*. Apress, New York, USA. https://doi.org/10.1007/978-1-4842-6168-2

Lee, S.H., Kim, W.Y., & Seo, D.H. (2022). Automatic self-reconstruction model for radio map in Wi-Fi fingerprinting. *Expert Systems with Applications*, 192, 116455. https://doi.org/10.1016/j.eswa.2021.116455

Li, J., Feng, J., & Kuo, C.C.J. (2018). Deep convolutional neural network for latent fingerprint enhancement. *Signal Processing: Image Communication*, 60, 52–63. https://doi.org/10.1016/j.image.2017.08.010

Li, Y., Xia, Q., Lee, C., Kim, S., & Kim, J. (2022). A robust and efficient fingerprint image restoration method based on a phase-field model. *Pattern Recognition*, 123, 108405. https://doi.org/10.1016/j.patcog.2021.108405

Liang, Y., & Liang, W. (2023). *ResWCAE: Biometric Pattern Image Denoising Using Residual Wavelet-Conditioned Autoencoder*. [Preprint]. https://doi.org/10.1007/978-981-96-6603-4_17

Lin, C., & Kumar, A. (2018). Contactless and partial 3D fingerprint recognition using multi-view deep representation. *Pattern Recognition*, 83, 314–327. https://doi.org/10.1016/j.patcog.2018.05.004

Liu, F., Kong, Z., Liu, H., Zhang, W., & Shen, L. (2022). Fingerprint presentation attack detection by channel-wise feature denoising. *IEEE Transactions on Information Forensics and Security*, 17, 2963–2976. https://doi.org/10.1109/TIFS.2022.3197058

Liu, F., Liu, G., Zhao, Q., & Shen, L. (2020a). Robust and high-security fingerprint recognition system using optical coherence tomography. *Neurocomputing*, 402, 14-28. https://doi.org/10.1016/j.neucom.2020.03.102

Liu, F., Liu, H., Zhang, W., Liu, G., & Shen, L. (2021). One-class fingerprint presentation attack detection using auto-encoder network. *IEEE Transactions on Image Processing*, 30, 2394–2407. https://doi.org/10.1109/TIP.2021.3052341.

Liu, F., Shen, C., Liu, H., Liu, G., Liu, Y., Guo, Z., et al. (2020b). A flexible touch-based fingerprint acquisition device and a benchmark database using optical coherence tomography. *IEEE Transactions on Instrumentation and Measurement*, 69(9), 6518–6529. https://doi.org/10.1109/TIM.2020.2967513

Mahum, R., Irtaza, A., Nawaz, M., Nazir, T., Masood, M., Shaikh, S., et al. (2023). A robust framework to generate surveillance video summaries using combination of zernike moments and r-transform and a deep neural network. *Multimedia Tools and Applications*, 82(9), 13811–13835. https://doi.org/10.1007/s11042-022-13773-4

Narodytska, N., & Kasiviswanathan, S.P. (2017). Simple Black-Box Adversarial Attacks on Deep Neural Networks. In: *CVPR Workshops*. Vol. 2. Available from: https://openaccess.thecvf.com/content_cvpr_2017_workshops/w16/papers/kasiviswanathan_simple_black-box_adversarial_cvpr_2017_paper.pdf

Nasri, M., Kosa, M., Chukoskie, L., Moghaddam, M., & Harteveld, C. (2024). Exploring Eye Tracking to Detect Cognitive Load in Complex Virtual Reality 1 Training. In: *2024 IEEE International Symposium on Mixed and Augmented Reality*

*Adjunct (ISMAR-Adjunct)*. IEEE, p51–54. https://doi.org/10.1109/ISMAR-Adjunct64951.2024.00022

Paris, S., Kornprobst, P., Tumblin, J., & Durand, F. (2009). Bilateral filtering: Theory and applications. *Foundations and Trends® in Computer Graphics and Vision*, 4(1), 1–73. https://doi.org/10.1561/0600000020

Praseetha, V.M., Bayezeed, S., & Vadivel, S. (2019). Secure fingerprint authentication using deep learning and minutiae verification. *Journal of Intelligent Systems*, 29(1), 1379–1387. https://doi.org/10.1515/jisys-2018-0289

Prybylo, M., Haghighi, S., Peddinti, S. T., & Ghanavati, S. (2024b). *Evaluating privacy perceptions, experience, and behavior of software development teams. USENIX*. Available from: https://www.usenix.org/conference/soups2024/presentation/prybylo

Rahman, M.M., Mishu, T.I., & Bhuiyan, M.A.A. (2022). Performance analysis of a parameterized minutiae-based approach for securing fingerprint templates in biometric authentication systems. *Journal of Information Security and Applications*, 67, 103209. https://doi.org/10.1016/j.jisa.2022.103209

Santos, S., Breaux, T., Norton, T., Haghighi, S., Ghanavati, S. (2024). *Requirements Satisfiability with in-Context Learning*. [arXiv Preprint]. https://doi.org/10.1109/RE59067.2024.00025

Shadab, S.A., Ansari, M.A., Singh, N., Verma, A., Tripathi, P., & Mehrotra, R. (2022). Detection of Cancer from Histopathology Medical Image Data Using ML with CNN ResNet-50 Architecture. In: *Computational Intelligence in Healthcare Applications*. Academic Press, United States, p237–254 https://doi.org/10.1016/B978-0-323-99031-8.00007-7

Shehu, Y.I., Ruiz-Garcia, A., Palade, V., & James, A. (2018). *Sokoto Coventry Fingerprint Dataset.* [arXiv Preprint]. https://doi.org/10.48550/arXiv.1807.10609

Srinivasan, D.S., Ravichandran, S., Indrani, T.S., & Karpagam, G.R. (2023). Local Binary Pattern-Based Criminal Identification System. In: *Sustainable Digital Technologies for Smart Cities*. United States: CRC Press. p45–56. Available from: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003307716-4/local-binary-pattern-based-criminal-identification-system-dhana-srinithi-srinivasan-soundarya-ravichandran-thamizhi-shanmugam-indrani-karpagam

Stolk, C.C., & Sbrizzi, A. (2019). Understanding the combined effect of ${k} $-space undersampling and transient states excitation in MR fingerprinting reconstructions. *IEEE Transactions on Medical Imaging*, 38(10), 2445–2455. https://doi.org/10.1109/TMI.2019.2900585

Trivedi, A.K., Thounaojam, D.M., & Pal, S. (2020). Non-invertible cancellable fingerprint template for fingerprint biometrics. *Computers and Security*, 90, 101690. https://doi.org/10.1016/j.cose.2019.101690

Vogel, R.M. (2022). The geometric mean? *Communications in Statistics-Theory and Methods*, 51(1), 82–94. https://doi.org/10.1080/03610926.2020.1743313

Wang, D., Ostenson, J., & Smith, D.S. (2020). snapMRF: GPU-accelerated magnetic resonance fingerprinting dictionary generation and matching using extended phase graphs. *Magnetic Resonance Imaging*, 66, 248–256. https://doi.org/10.1016/j.mri.2019.11.015

Wang, W., & Yang, Y. (2024). A histogram equalization model for color image contrast enhancement. *Signal, Image and Video Processing*, 18(2), 1725–1732. https://doi.org/10.1007/s11760-023-02881-9

Wong, W.J., & Lai, S.H. (2020). Multi-task CNN for restoring corrupted fingerprint images. Pattern Recognition, 101, 107203. https://doi.org/10.1016/j.patcog.2020.107203

Xu, Z., Ye, H., Lyu, M., He, H., Zhong, J., Mei, Y. (2019). Rigid motion correction for magnetic resonance fingerprinting with sliding-window reconstruction and image registration. *Magnetic Resonance Imaging*, 57, 303–312. https://doi.org/10.1016/j.mri.2018.11.001

Yin, X., Zhu, Y., & Hu, J. (2019). 3D fingerprint recognition based on ridge-valley-guided 3D reconstruction and 3D topology polymer feature extraction. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 43(3), 1085–1091. https://doi.org/10.1109/TPAMI.2019.2949299

Zhang, L., Tan, T., Gong, Y., & Yang, W. (2019). Fingerprint database reconstruction based on robust PCA for indoor localization. *Sensors (Basel)*, 19(11), 2537.

Zheng, H., Gao, M., Chen, Z., Liu, X.Y., & Feng, X. (2019). An adaptive sampling scheme via approximate volume sampling for fingerprint-based indoor localization. *IEEE Internet of Things Journal*, 6(2), 2338–2353. https://doi.org/10.1109/jiot.2019.2906489

## AUTHOR BIOGRAPHIES

**R. Sreemol** received her Bachelor's degree in Computer Science and Engineering in 2014 and her Master's degree in Computer Science and Engineering in 2017. She earned her Ph.D. from the Department of Computer Applications, Cochin University of Science and Technology, South Kalamassery, Kochi, Kerala, India. Her research interests include pattern recognition and image processing, with applications in biometrics and security systems

**M. B. Santosh Kumar** received his Ph.D. in 2018 from Cochin University of Science and Technology, South Kalamassery, Kochi, Kerala, India. His dissertation was titled Development of Innovative Procedures for Information Technology Articulated Agriculture. He is a Professor in the Division of Information Technology, School of Engineering, CUSAT. He was granted a patent for a Portable Agriculture Network System in 2017. His research interests focus on knowledge-based systems in agriculture and artificial intelligence applications in agriculture

**A. Sreekumar** received his Ph.D. in Cryptography from Cochin University of Science and Technology, South Kalamassery, Kochi, Kerala, India, in 2010. He is a retired Professor from the Department of Computer Applications, CUSAT, with 27 years of teaching experience. His research interests include cryptography, number theory, and secret sharing.

## Appendix

### Appendix A1. Dataset details

Dataset 1: Six thousand fingerprints from 600 African participants make up the Sokoto Coventry Fingerprint Dataset (SOCOFing; https://www.kaggle.com/datasets/ruizgara/socofing; Xiao et al., 2019). The experimental settings and datasets used were consistent across all models. Each participant, all of whom were at least 18 years old, submitted 10 fingerprints. Gender designations and hand and finger names are included in SOCOFing. The STRANGE toolbox was utilized to generate synthetic modifications of these fingerprints, including three distinct levels of obliteration, central rotation, and *z*-cut change. The SDU03PTM sensor (SecuGen, USA) and Hamster Plus sensor (HSDU03PTM, SecuGen, USA) scanners were used to acquire the original images.

Dataset 2: FVC2002 fingerprints (https://www.kaggle.com/datasets/nageshsingh/fvc2002-fingerprints). These datasets were chosen due to their inclusion of benchmarked and standard fingerprints collected from various sensors, displaying various characteristics.

Dataset 3: Fingerprint Dataset for FVC2000_DB4_B (https://www.kaggle.com/datasets/peace1019/fingerprint-dataset-for-fvc2000-db4-b). A collection of fingerprint photos utilized for fingerprint recognition studies. This fingerprint dataset can also be used for data augmentation activities. It comprises 800 excellent fingerprint photographs, each measuring 160 × 160 pixels and having a resolution of 500 DPI.

## Reference

Xiao, J., Hu, F., Shao, Q., & Li, S. (2019). A low-complexity compressed sensing reconstruction method for heart signal biometric recognition. *Sensors (Basel)*, 19(23), 5330. https://doi.org/10.3390/s19235330