Journal of Information Technology Management
ISSN-OnLine: 2980-7972
University of Tehran

Adaptive Fingerprint Verification Using Siamese Neural Networks and Transfer Learning for Robust Authentication of Damaged Prints

Suman M*

*Corresponding author, Assistant Professor, Department of Artificial Intelligence and Data Science, B.M.S College of Engineering, Affiliated to Visvesvaraya Technological University, Belagavi, India. E-mail: 9sumanm@gmail.com

Shobha N

Associate Professor, Department of Computer Science and Design, Dayananda Sagar College of Engineering, Bangalore, Visvesvaraya Technological University, Belagavi, India. E-mail: shobha.venk20@gmail.com

Sridevi Muruhan

Professor, Department of Biotechnology, Vinayaka Mission`s Kirupananda Variyar Engineering College, Salem (Vinayaka Mission`s Research Foundation), India. E-mail: sridevi@vmkvec.edu.in

Vinothkumar S

Assistant Professor, (SRG), Department of Information Technology, Kongu Engineering College, Perundurai, Erode, India. E-mail: vinoths.it@kongu.edu

Ramkumar R

Associate Professor, Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam. E-mail: ramkumarr@bitsathy.ac.in

R J Poovaraghan

Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India. E-mail: poovaraghanrj@veltech.edu.in

Journal of Information Technology Management, 2025, Vol. 18, Issue 1, pp. 1-16
Published by the University of Tehran, College of Management
doi: https://doi.org/10.22059/jitm.2026.106251
Article Type: Research Paper

Received: August 07, 2025
Received in revised form: September 13, 2025
Accepted: December 12, 2025
Published online: January 20, 2026

Abstract

Fingerprint recognition is a vital component of biometric authentication, yet its reliability often declines with damaged or partial inputs. This study introduces a fingerprint verification framework based on Siamese Neural Networks (SNN) with transfer learning to enhance adaptability and accuracy. Using the Sokoto Coventry Fingerprint Dataset (SOCOFing), fingerprint images were preprocessed into labeled pairs of similar and dissimilar samples for model training and evaluation. A distinctive feature of the proposed system is dynamic class expansion, enabling new user integration without retraining. The framework also ensures privacy-preserving verification by securely encrypting and storing extracted feature embeddings. Experimental results across four difficulty levels—real, easy, medium, and hard—demonstrate high reliability and robustness in both intact and degraded fingerprint conditions. Overall, the proposed approach offers a scalable, secure, and efficient solution for fingerprint-based identification, addressing key challenges in real-world biometric authentication systems.

Keywords: Fingerprint Authentication, ConvNeXt Feature Extraction, Siamese Neural Network (SNN), AES Encryption, Biometric Security

Introduction

One of the most effective biometric authentication methods is fingerprint recognition because it is unique, permanent, and easy to obtain. It is commonly used in online security, banking, forensic, and access control. Nevertheless, in the real world, fingerprints tend to be damaged, distorted, or captured partially, resulting in diminished recognition accuracy and system reliability. Besides, as cybersecurity threats increase, there is an increasing requirement for privacy-protective and tamper-resistant authentication systems capable of securing sensitive biometric data.

Recent developments in deep learning have greatly enhanced the recognition of fingers by extracting and classifying automatic features. Transformers and deep learning have demonstrated high accuracy on large and clean datasets (Kumar, Kumar, 2023; Grosz, Jain, 2023; Zhang, Liu, and Liu, 2021). But they deteriorate with low-quality prints or incomplete fingerprints, and most systems still need retraining when new users are introduced, which restricts scalability. Similar studies in metaheuristic optimization and hybrid feature extraction have improved performance, and encryption-based studies, such as AES and Chaotic Map algorithms, have enhanced data protection (Altameem et al., 2023; Khande et al., 2021). However, few frameworks merge these components to deliver accuracy and security in a single model.

This paper introduces a three-level damaged fingerprint authentication using Transfer Learning and SNN to perform similarity-based matching, and AES encryption to store

biometric templates in a safe place. The intended approach will improve accuracy and flexibility without compromising the privacy of data. The system is tested in reference to benchmark SOCOFing fingerprint datasets in recognition accuracy, F1, AUC, Precision, and Recall, and computational efficiency to different degrees of noise and degradation.

The experimental evidence shows that the proposed work has higher verification rates and resistance to damaged fingerprints. Moreover, the AES encryption integrated provides secure storage and transfer of biometric templates without affecting the performance of the system. On the whole, this study adds a scalable, secure, and resilient fingerprint verification model, which develops the biometric authentication technologies.

Literature Review

In the field of fingerprint authentication, the following discusses deep learning, optimization, multimodal biometrics, and encryption methods that enhance the accuracy, scalability, and safety of data.

Advancements in biometric security continue to evolve rapidly. Altameem et al. (2023) highlighted the necessity of template protection using hybrid AES–Chaotic Map encryption for fingerprint authentication in IoT and Industry 4.0, while Benchallal et al. (2024) demonstrated the promise of ConvNeXt within semi-supervised learning frameworks, achieving high accuracy even with limited labeled data. Equally, Bradley et al. (2019) developed PAKE to enhance secure key exchange, and Chen et al. (2024) confirmed the efficiency of MobileNetV2 in lightweight image-based tasks, reinforcing its potential for biometric applications.

Daas et al. (2020) emphasized the importance of feature extraction through CNN-based multimodal fusion using AlexNet, VGG16, and ResNet50, achieving 99.89% accuracy in finger-vein/knuckle recognition. Goel et al. (2020) similarly explored deep learning for fingerprint analysis with their Patch-based CNN (P-DCNN), achieving an EER of 2.08%, while Grosz and Jain (2023) proposed AFR-Net, combining CNNs and Vision Transformers for near-perfect accuracy.

Hsiao et al. (2019) demonstrated that Siamese Neural Networks (SNNs) exhibit strong generalization in one-shot learning scenarios, a capability later leveraged by Solano et al. (2021) for behavioral biometrics and Loster et al. (2021) for low-resource entity resolution. Hussain et al. (2022) also showed the adaptability of MobileNetV2 for constrained environments such as face-mask detection.

Iskandar et al. (2024) advanced multimodal biometric fusion by integrating spatial and traditional features. Kaleem et al. (2024) supported secure cloud-based architectures through lightweight cryptography, complemented by Khande et al. (2021), who introduced AES-256

with PBKDF2 for resistance against brute-force attacks. Kapoor et al. (2021) achieved robust finger-vein recognition using LPQ, Grey Wolf Optimization, and SVM.

Kumar and Kumar (2023) improved fingerprint recognition performance using their GSDF model, while Modugula (2020) applied Argon2i with AES-256 for secure password handling. Mustacoglu et al. (2020) contributed additional security by encrypting cloud data using password-based schemes.

Rehman et al. (2022) and Trabelsi et al. (2022) explored palmprint identification and verification through Extended LBP and deep-learning–based feature selection, respectively. Shekhar et al. (2023) demonstrated that multimodal fusion of CNN, SVM, and GMM significantly enhances robustness, achieving 99.59% accuracy with low spoofing risk.

Suman and Shobha (2025) emphasized integrating deep learning with biometric and cloud security systems, identifying emerging ethical and privacy considerations. Yong et al. (2023) expanded the utility of MobileNetV2 through its successful use in waste classification. Finally, Zhang, Liu, and Liu (2021) introduced ContactlessMinuNet, a multitask deep CNN for minutiae extraction using attention mechanisms, achieving high accuracy across multiple datasets.

Despite these advances, challenges remain. Methods such as those of Grosz and Jain (2023); Goel et al. (2020), Kumar and Kumar (2023), and Zhang et al. (2021) perform well on clean fingerprints but fail under distortion or partial input. Lean architectures like ConvNeXt and MobileNetV2 (Benchallal et al., 2024; Chen et al., 2024; Yong et al., 2023) lack fingerprint-specific adaptations. AES-based encryption techniques (Altameem et al., 2023; Khande et al., 2021; Mustacoglu et al., 2020) remain underexplored within deep-learning biometric pipelines. To overcome these limitations, this paper proposes a ConvNeXt-based Siamese fingerprint verification system capable of dynamically adding new users without retraining. This approach yields high accuracy even under challenging conditions and provides a privacy-preserving, flexible, and scalable next-generation digital identity solution.

Methodology

The section outlines the dataset, preprocessing, network architecture, training, inference mechanism, and performance evaluation methods applied in the development of the proposed system. It describes the design, implementation, and testing of the model to provide correct and safe fingerprint identification.

Dataset Description

The given work involves the application of the Sokoto Coventry Fingerprint Dataset (SOCOFing), a free biometric dataset popular in research relating to fingerprint recognition. It involves 6000 gray scale fingerprint images of 600 people, each giving 10 impressions. The

data are categorized into four sets: Real, Easy, Medium, and Hard that depict the degrees of degradation and distortion. In particular, unaltered fingerprints are included in the Real category, whereas the Easy, Medium, and Hard categories represent real-world acquisition problems by introducing controlled distortions (blurring, occlusion, damage, etc.) as shown in Figure 1. This diversity allows for considering model robustness under different conditions of fingerprints in a more thorough way. All images were downsampled to 90 x 90 x 1 (grayscale) to fit into the ConvNeXt feature extractor of the network.

(a) (b) (c) (d)

Figure 1. Representative Fingerprint Samples from the dataset

(a) Real, (b) Easy, (c) Medium, and (d) Hard.

This study uses the SOCOFing dataset, a publicly accessible dataset on fingerprint research, Suman et al. (2026), which only used the Real category, in this paper, by involving Easy, Medium, and Hard categories to test system adaptability and generalization.

Dataset Preprocessing and Pair Generation

Normalization of fingerprint images was done by scaling pixel values within the range of zero to one, and then using the Gaussian filter to suppress noise but retain ridge-valley contrasts. Histogram equalization followed, followed by local contrast boosting by random augmentation, e.g., by 10 degrees rotation, by five pixels translation, and by fifteen percent brightness adjustment, to bring more sample diversity. In order to train the Siamese Neural Network, fingerprint pairs were built in two ways: positive pairs, or two fingerprints of the same individual with label one, and negative pairs formed by fingerprints of other individuals with label zero. The training instances were therefore two 90-by-90 grayscale channel input images. This is structured pair generation, based on the balanced-pairing approach by Kumar and Kumar (2023), which guarantees equal representation of match and non-match classes to improve generalization and stability in metric learning.

Siamese Neural Network Architecture

The System Architecture of the Working Process of SNN is illustrated in Figure 2. The architecture comprises two identical ConvNeXt subnetworks sharing parameters to ensure symmetric feature extraction from both inputs. Each branch processes its input fingerprint

image x_1 or x_2 through convolutional filters $f_\theta$parameterized by weights θ, yielding latent representations $h_1 = f_\theta(x_1)$and $h_2 = f_\theta(x_2)$.

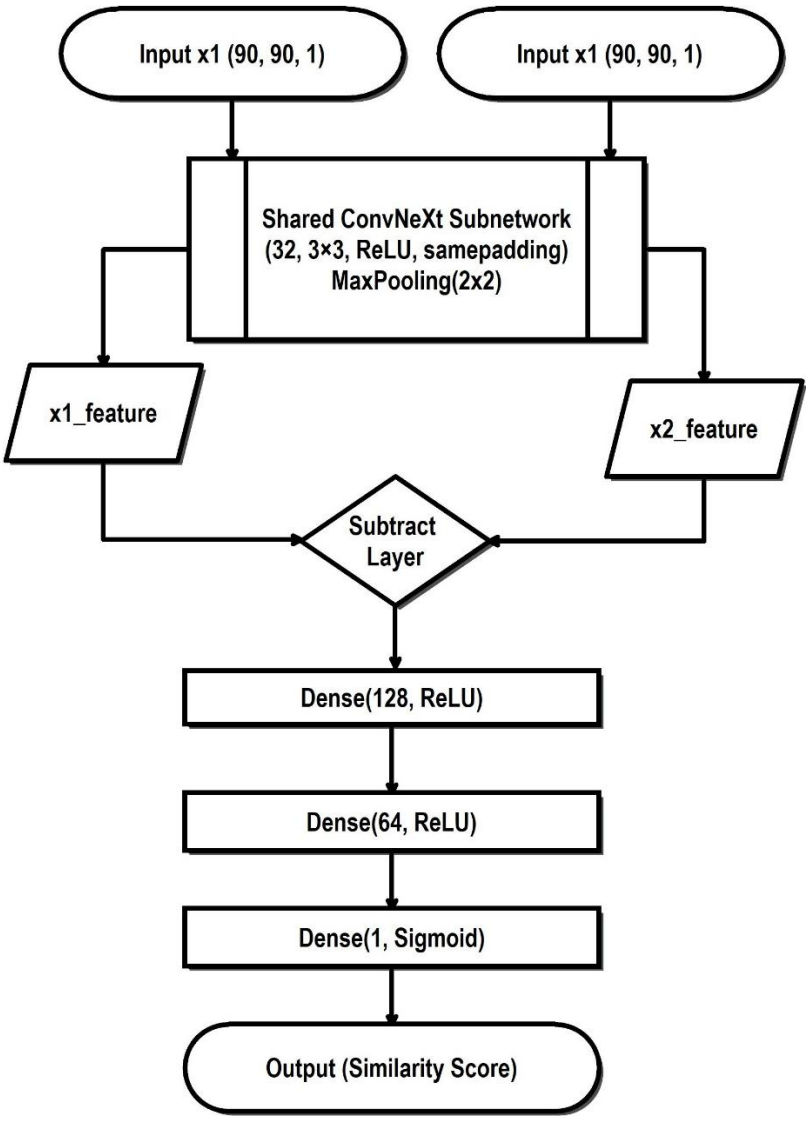


Figure 2. Siamese Neural Network architecture

A subtraction layer computes the absolute element-wise difference:

$$D = | h_1 - h_2 | \quad (1)$$

where Ddenotes the feature difference vector encoding dissimilarities between two inputs. This difference is passed through fully connected layers with 128 and 64 neurons, each activated by the ReLU function $\sigma(z) = \max(0, z)$, followed by a final sigmoid output layer:

$$\hat{y} = \sigma(WD + b) \quad (2)$$

where $W$and $b$are the learned weights and bias terms, respectively, and $\hat{y}$ is the predicted similarity score in [0,1]. The shared ConvNeXt feature extractor employs 3×3 convolution

kernels, ReLU activation, and 2×2 max pooling layers. This configuration provides efficient local feature encoding and spatial invariance, while the subtraction layer and dense stack translate spatial differences into a continuous similarity metric. The architecture's design reflects hierarchical texture learning principles demonstrated in deep convolutional and hybrid transformer frameworks

Model Training and Implementation Details

SNN with ConvNeXt was trained on fingerprint pairs in each of 3 subsets of difficulty to enable generalization to both clean and degraded samples. ConvNeXt backbone is an effective representation learner, which integrates convolutional efficiency with transformer design philosophy to achieve better texture and ridge-pattern classification (Dosovitskiy et al., 2020).

During training, each input pair $(x_1, x_2)$was independently passed through the shared ConvNeXt network $f_\theta$to generate latent embeddings $h_1 = f_\theta(x_1)$and $h_2 = f_\theta(x_2)$. The network was optimized using binary cross-entropy (BCE) loss:

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (3)$$

where $y_i \in \{0,1\}$represents the ground truth (match or non-match) and $\hat{y}_i \in [0,1]$is the predicted similarity score for the i^{th}pair.

The model was trained using the Adam optimizer with an initial learning rate of 1×10^{-4}, batch size of 32, and early stopping based on validation loss to prevent overfitting. Dropout regularization was applied in the dense layers to stabilize convergence. Training was implemented using TensorFlow with CUDA acceleration on an NVIDIA RTX GPU, and convergence was typically achieved within 20 epochs. The unified training approach allowed the SNN to learn domain-invariant fingerprint representations, improving adaptability across varying quality conditions and damage levels.

Inference System Working Process

The Inference System Working Process, illustrated in Figure 3, operates in two primary phases: Registration and Authentication. In the Registration Phase, the user's fingerprint sample $x_r$is captured and passed through the ConvNeXt feature extractor f_θ, producing a discriminative feature vector $F_r = f_\theta(x_r)$. The extracted features are then encrypted using the Advanced Encryption Standard (AES) before being securely stored with the corresponding user ID. AES ensures the confidentiality of biometric templates, making it computationally infeasible to reconstruct the original fingerprint without the encryption key.

During the Authentication Phase, the user provides their ID and a new fingerprint sample x_t. The system extracts its feature vector $F_t = f_\theta(x_t)$, retrieves and decrypts the stored feature F_r, and computes the absolute difference vector $D' = |F_t - F_r|$. This vector is

processed by the Siamese Neural Network (SNN) to produce a similarity score $\hat{y} \in [0,1]$. A decision threshold of $\tau = 0.75$ is applied: if $\hat{y} \geq \tau$, the system classifies the input as a match; otherwise, it is deemed a non-match. This ensures both reliable verification and data security within the end-to-end inference pipeline.

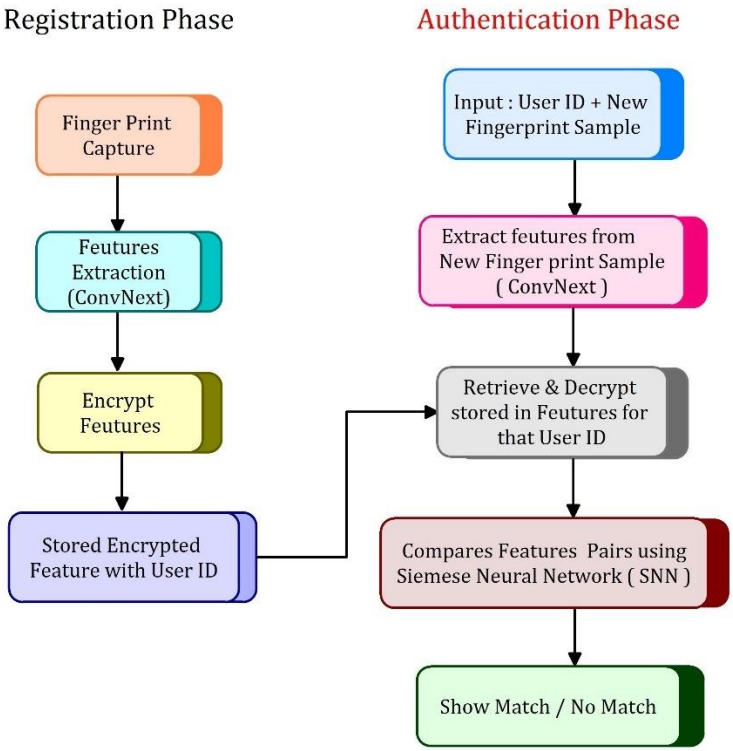


Figure 3. Inference System workflow process

Performance Evaluation

To examine resilience to false match and false rejection in all the distortion categories, performance was evaluated using unseen test pairs of accuracy and precision, recall, F1-score, and ROC-AUC. Easy, Medium, and Hard subset results indicate the robustness of the system and gradual degradation tolerance efficiency.

Results

The findings are given in this section. The measures of interest are classified performance, confusion matrix analysis, convergence of training and validation processes, and ROC analysis in four unique levels of fingerprint complexity.

Table 1 summarizes the strong categorization performance of the ConvNeXt model in all four categories. In the case of the Real category, the model had an accuracy of 98.61, a precision of 100, and a recall of 97.00. Different class and Similar class of 97.00 and 100, respectively. This excellent balance of sensitivity and specificity of the model was evidenced by the macro average precision and recall of 99.00% and 99.00%, respectively. The F1-scores

of both classes are high, which shows that there is little misclassification, and generalization is stable when there is no distortion. ConvNeXt remained effective in the Easy category with a total accuracy of 96.78. The Different class had a precision of 98.00% and a recall of 95.31%, whereas the Similar class had a precision of 95.00% and a recall of 98.24%. The almost similar F1-scores of 96.64% and 96.60% between the two classes underscore the unbiasedness and fairness of the model in low-complexity fingerprint matching. The macro average values were relatively close to 96.6, thus showing similar performance in both classes. In the Medium category, which added more intra-class variability, the ConvNeXt model had an average accuracy of 95.21%. The Different class received a precision of 96.00% and a recall of 94.33, and the Similar class received a precision of 94.00% and a recall of 96.09. The outcome of these values was near convergence in F1-scores at about 95%, which highlighted the ability of the model to conform to moderately complex patterns without considerable loss of performance. Macro average accuracy and F1-score were consistent at 95.10, indicating balanced model learning in the two classes. The model registered 92.77 in the Hard category, where intra-class similarity was greatest. The Different and the Similar classes had a precision of 95.62% and 90.26%, respectively, and a recall of 89.65 and 95.90, respectively. Nonetheless, the model maintained the F1-scores in the range of 92.8-93, which reflects the difficulty of the classification conditions. These findings support that ConvNeXt is both fair and discriminative as the fingerprint similarity grows.

Table 1. ConvNeXt Classification Report Across Categories

Category	Class	Precision	Recall	F1-Score	Accuracy
Real Suman M, et al (2026)	Different	100%	97.00%	99.00%	98.61%
	Similar	97.30%	100%	99.00%	
	Macro Avg	99.65%	99.00%	99.00%	
Easy	Different	98.00%	95.31%	96.64%	96.78%
	Similar	95.00%	98.24%	96.60%	
	Macro Avg	96.50%	96.78%	96.62%	
Medium	Different	96.00%	94.33%	95.16%	95.21%
	Similar	94.00%	96.09%	95.03%	
	Macro Avg	95.00%	95.21%	95.10%	
Hard	Different	95.62%	89.65%	92.54%	92.77%
	Similar	90.26%	95.90%	92.99%	
	Macro Avg	92.94%	92.77%	92.77%	

The confusion matrices in Figure 4 give a more detailed visualization of classification results in all categories. In the case of 288 fingerprints in the Real category, Suman et al. (2026), the model correctly classified 280 of 288 Different fingerprints, and all 288 Similar fingerprints were correctly predicted. This result is consistent with the high accuracy and recall rates in Table 2, meaning that ConvNeXt is able to distinguish between classes without confusion. The confusion matrix in the Easy category (Figure 4a) indicates that 488 of the total of 512 Different fingerprints were correctly recognized, and 24 were mistakenly classified as Similar. Likewise, 503/512 Similar samples were correctly identified, and nine were wrongly identified. These outcomes confirm the model of close-to-perfect

discrimination and low bias as well as the balanced F1-scores in Table 1. In the Medium category (Figure 4b), ConvNeXt had a correct rate of 483/512 Different and 492/512 Similar fingerprints with 29 and 20 misclassifications, respectively. Although it was moderately complex, the model still had high discriminative capability and fair performance in the two classes. In the Hard category (Figure 4c), the confusion matrix showed that 459 Different and 491 Similar samples were correctly identified, 53 and 21 were misidentified. These misclassifications are higher by the higher similarity of the fingerprints in the given category, yet the equal regard in the two classes proves that ConvNeXt maintained fairness in the conditions of high complexity.

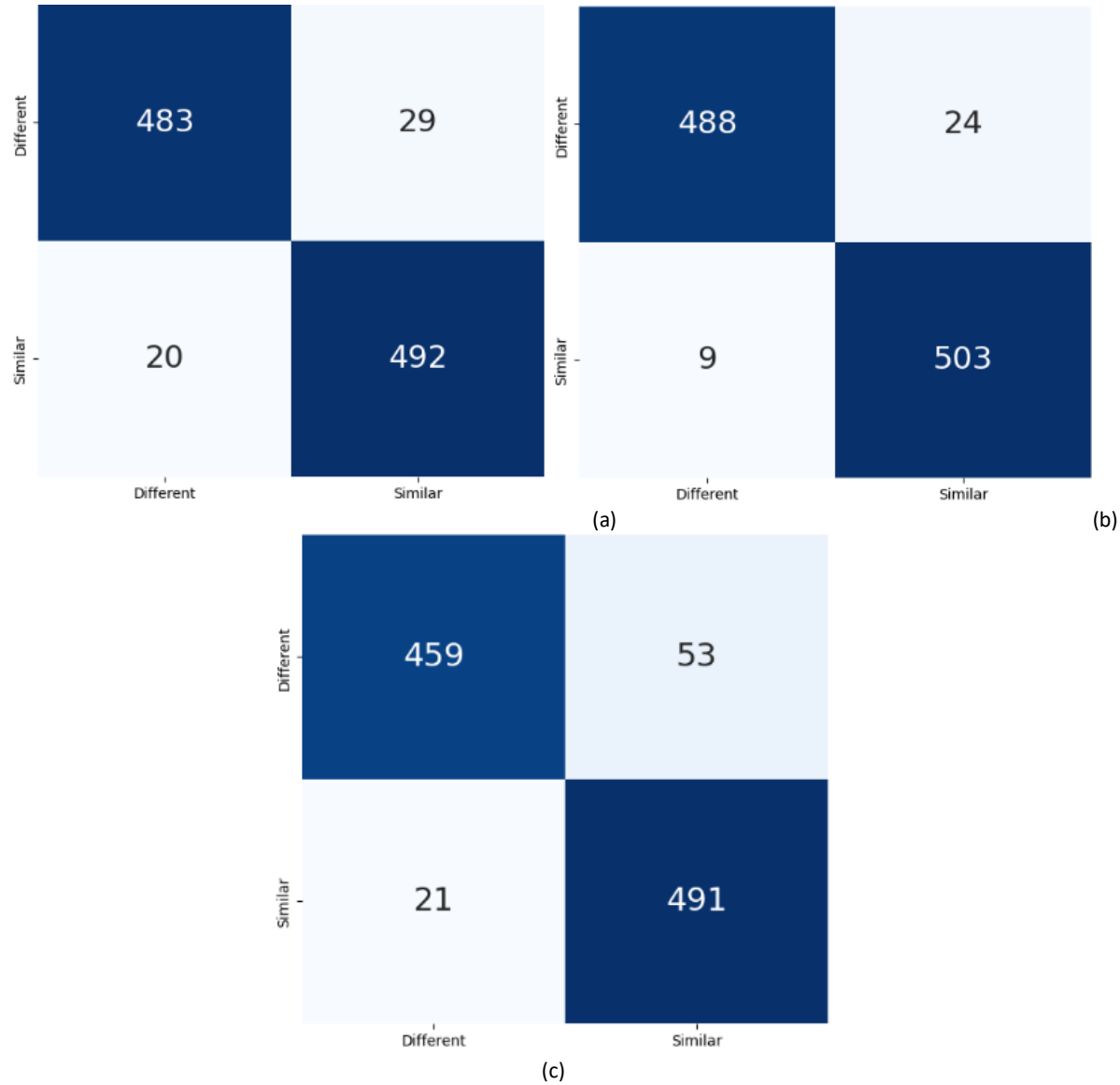
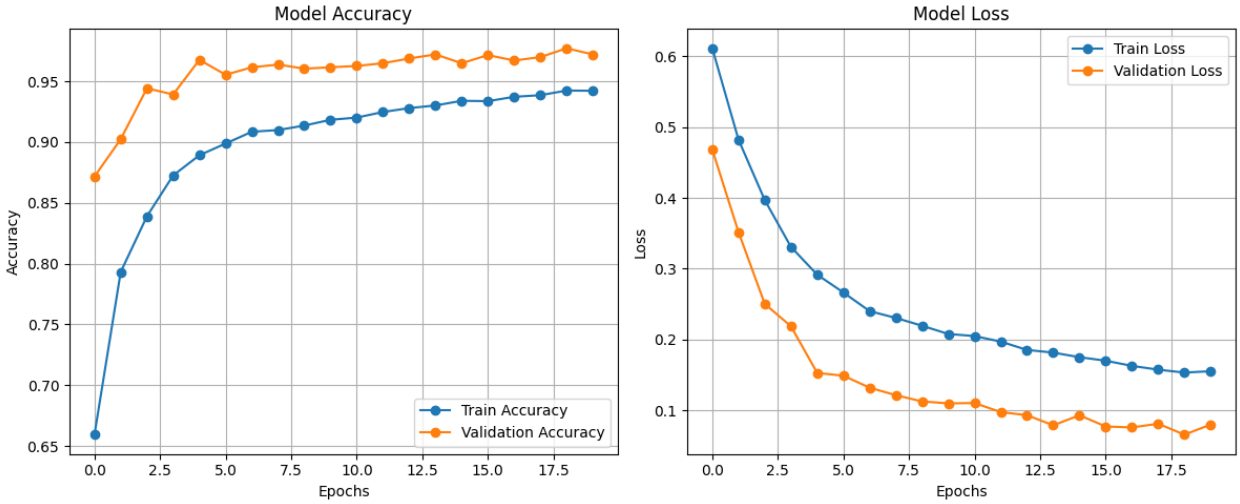


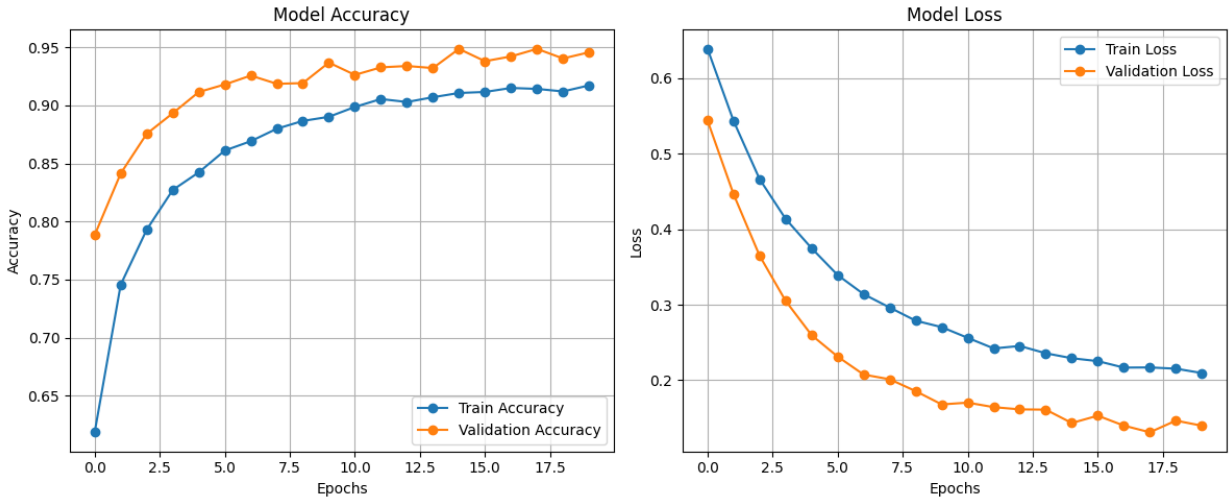
Figure 4. (a)Easy, (b) Medium, (d) Hard category Confusion matrix ConvNeXt

Figure 5 demonstrates the training and validation accuracy and loss curves of ConvNeXt on all three types of fingerprints. The model had general convergence behavior, and the smooth, gradual rise in accuracy and corresponding fall in loss over 20 epochs. According to

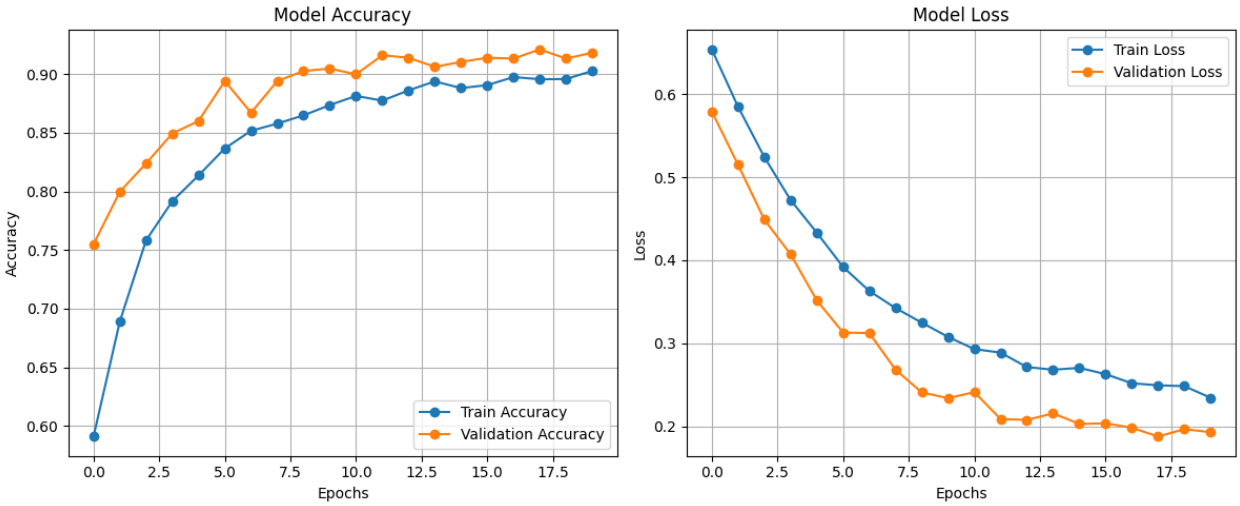
per, the accuracy of training was 57.99% and gradually rose to 96.33% with each epoch, whereas validation accuracy was constant at 97-98%. The ultimate validation loss was 0.0631, which is a great generalization without overfitting. The strength of ConvNeXt against perfect fingerprint conditions is confirmed by this uniformity. Training accuracy with the Easy category increased to 94.38 after 20 epochs, with the highest validation accuracy of 97.21 and a level of 96.80. In line with this, the loss of training and validation reduced to 15.60 and 8.01, respectively. The similarity of the training and validation curves is a sign of the balanced learning of the model and the validity of the ConvNeXt model, given the low-complexity fingerprint data. In the Medium category, training accuracy was 57.21 to 91.55, and validation accuracy was 78.83 to 94.58. Losses in training and validation decreased to 21.38% and 13.97 respectively, which indicates effective learning.



(a)



(b)



(c)

Figure 5. (a) Easy, (b) Medium, (d) Hard category Accuracy & loss plot ConvNeXt for 20 epochs

The minor decrease in accuracy in relation to the Easy category is due to the additional intra-class variability, but nonetheless, it demonstrates a high ability to generalize. Convergence in the Hard category was lower because fingerprint patterns were very similar. The accuracy of training improved to 90.51%, and the accuracy of validation improved to 91.83 percent. Loss of training reduced to 22.92 and validation loss to 19.30. Both curves stabilized without drifting, which indicated that ConvNeXt did not overfit and continued learning behavior in the more difficult setting.

Receiver Operating Characteristic (ROC) curves in Figure 6 indicate the discriminatory power of the ConvNeXt model between Different and Similar classes. Under the Real category, Suman et al. (2026), the two classes yield an AUC of 1.00, which proves perfect separability and a false positive prediction of 0. The sharp, almost vertical upward trend of the ROC curve means that ConvNeXt had a 100 percent true positive rate with zero specificity. Figure 6a shows that the Different class had a True Positive Rate (TPR) of 95.31 and a False Positive Rate (FPR) of 1.76, and the Similar class had a TPR of 98.24 and an FPR of 4.69. Both classes had an AUC of 1.00, indicating that they had optimal discriminatory ability as it relates to classification and the confusion matrix. In the Medium category, Figure 6b, the two classes had an AUC of 0.99 with high TPR (>95) and low FPR (<10). The high separability is indicative of the sensitivity and specificity of the model even at higher levels of variability. The model in the Hard Figure 6c category had an AUC of 0.98 in both classes. At FPR 10.35, the Different class had a TPR of 89.65%, whereas the similar class had a TPR of 95.90%. Whereas in this category classification is made more difficult, ConvNeXt nevertheless obtained high overall discrimination with low interclass bias.

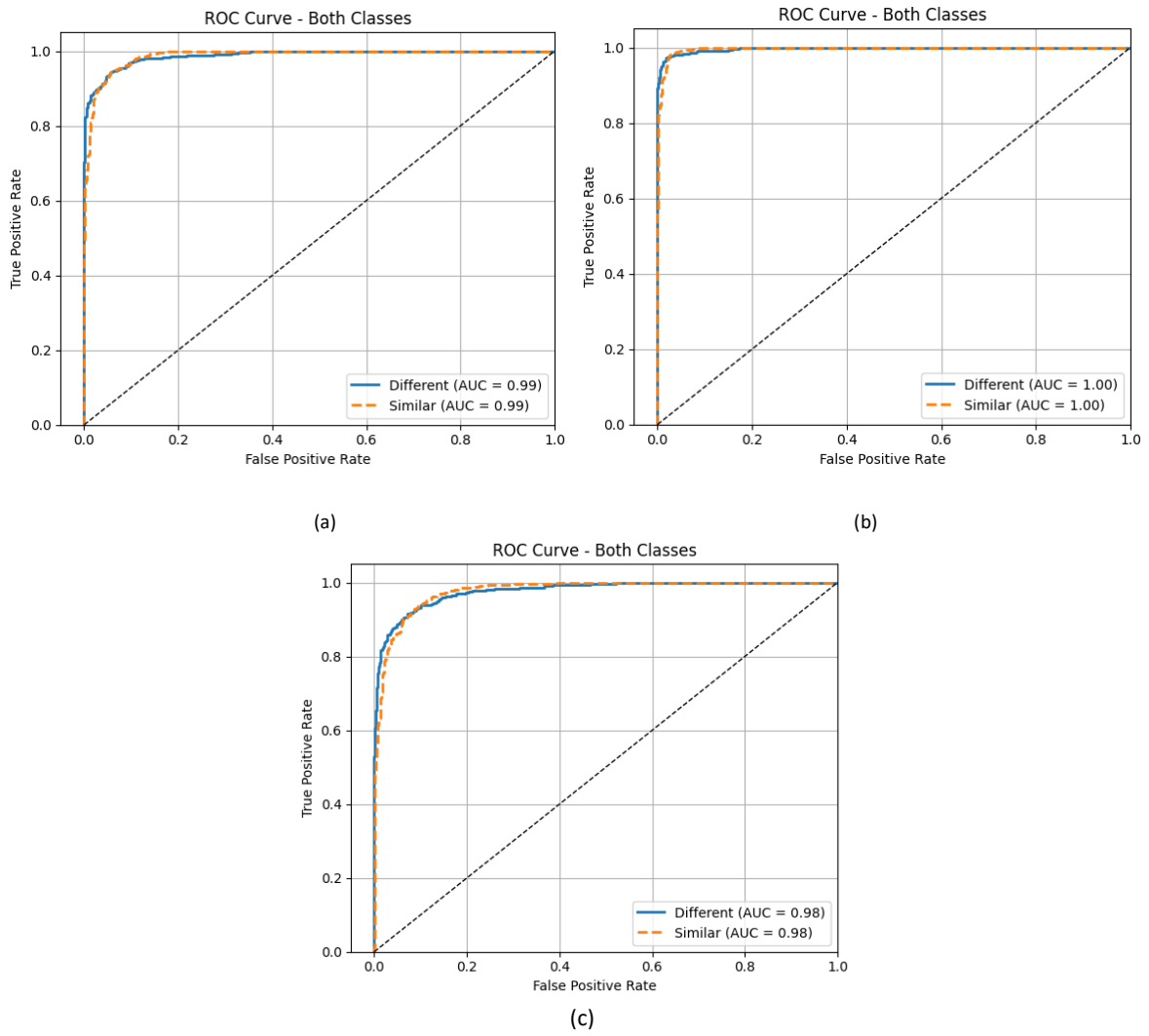


Figure 6. (a) Easy, (c) Medium, (d) Hard category ROC curves of ConvNeXt for both classes

Discussion

The evaluation across the proposed fingerprint verification system with different degrees of image degradation reveals that the performance persistently deteriorated as the distortion increased. ConvNeXt registered high, medium, and lower but still significant accuracy on the Easy set (96.78%), the medium set (95.21%), and the Hard set (92.77%). The trend suggests that the feature of the model is easily extracted, especially in extreme blur or occlusion, and the clarity of fingerprints and the visibility of ridge-valleys play a crucial role in the model. Irrespective of them, the model architecture was very generalized, with little to no overfitting, as evidenced by near-perfect values of AUC (1.00 with Easy and Medium, and 0.98 with Hard). The deep convolutional nature of ConvNeXt and large receptive fields enabled it to maintain important structural information even when the fingerprints were damaged. Corresponding observations were made by Grosz and Jain (2023), who noted that attention-based architectures make challenging fingerprint conditions more robust. The secure authentication model enhances the verification accuracy of the model with AES-based

encryption that guarantees that the biometric embedding is confidential and tamper-resistant without compromising the classification quality. The overall findings show that the suggested system is characterized by high accuracy in verification and secure inference in the presence of degraded fingerprints, which proves the appropriateness of the suggested system in the real-world biometric uses where the quality of the acquisition conditions is diverse.

Conclusion

The results of this study proved to be very accurate and generalizable to different complexities of fingertips. The model was highly discriminative, achieving 98.61, 96.78, 95.21, and 92.77 accuracy in the Real, Easy, Medium, and Hard categories, respectively. The ROC analysis proved that it could separate classes with AUC values of between 0.98 and 1.00, meaning that it made few false matches and could work with serious distortions. These findings confirm the capability of the ConvNeXt model to be aligned to varying quality conditions and fair and consistent across the fingerprint classes. This research has implications suggesting that ConvNeXt can be used as a scalable and secure backbone in fingerprint-based authentication systems, especially when there is a range of image quality based on the conditions of acquisition. Integration with AES encryption provides not only high accuracy of verification, but also complies with the data security standards that are necessary in practical biometric usage. Future research can be spent on improving the model to use in real-time and on edge devices, and to connect it with retinal verification to provide extra security.

Acknowledgements

The authors extend their sincere gratitude to B.M.S College of Engineering, Bengaluru, and Dayananda Sagar College of Engineering, Bengaluru, affiliated with Visvesvaraya Technological University, Belagavi, for their valuable support and encouragement throughout this research. The conducive academic environment and research infrastructure provided by these institutions significantly contributed to the successful completion of this work.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Altameem, A., P, P., T, S., Poonia, R. C., & Saudagar, A. K. J. (2023). A hybrid AES with a chaotic map-based biometric authentication framework for IoT and Industry 4.0. *Systems*, *11*(1), 28.

Benchallal, F., Hafiane, A., Ragot, N., & Canals, R. (2024). ConvNeXt based semi-supervised approach with consistency regularization for weeds classification. *Expert Systems with Applications*, *239*, 122222.

Bradley, T., Camenisch, J., Jarecki, S., Lehmann, A., Neven, G., & Xu, J. (2019). Password-authenticated public-key encryption. In *International Conference on Applied Cryptography and Network Security*, 442-462.

Chen, H., Zhou, G., He, W., Duan, X., & Jiang, H. (2024). Classification and identification of agricultural products based on improved MobileNetV2. *Scientific Reports*, *14*(1), 3454.

Daas, S., Yahi, A., Bakir, T., Sedhane, M., Boughazi, M., & Bourennane, E. B. (2020). Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion. *IET Image Processing*, *14*(15), 3859-3868.

Goel, I., Puhan, N. B., & Mandal, B. (2020). Deep convolutional neural network for double-identity fingerprint detection. *IEEE Sensors Letters*, *4*(5), 1-4.

Grosz, S. A., & Jain, A. K. (2023). Afr-net: Attention-driven fingerprint recognition network. *IEEE Transactions on biometrics, behavior, and identity science*, *6*(1), 30-42.

Hsiao, S. C., Kao, D. Y., Liu, Z. Y., & Tso, R. (2019). Malware image classification using one-shot learning with siamese networks. *Procedia Computer Science*, *159*, 1863-1871.

Hussain, D., Ismail, M., Hussain, I., Alroobaea, R., Hussain, S., & Ullah, S. S. (2022). Face Mask Detection Using Deep Convolutional Neural Network and MobileNetV2-Based Transfer Learning. *Wireless Communications and Mobile Computing*, *2022*(1), 1536318.

Iskandar, A., Alfonse, M., Roushdy, M., & El-Horbaty, E. S. M. (2024). Biometric systems for identification and verification scenarios using spatial footsteps components. *Neural Computing and Applications*, *36*(7), 3817-3836.

Kaleem, M., Mushtaq, M. A., Jamil, U., Ramay, S. A., Khan, T. A., Patel, S., ... & Hussain, S. K. (2024). New efficient cryptographic techniques for cloud computing security. *Migration Letters*, *21*(S11), 13-28.

Kapoor, K., Rani, S., Kumar, M., Chopra, V., & Brar, G. S. (2021). Hybrid local phase quantization and grey wolf optimization-based SVM for finger vein recognition. *Multimedia Tools and Applications*, *80*(10), 15233-15271.

Khande, R., Ramaswami, S., Naidu, C., & Patel, N. (2021). An effective mechanism for securing and managing password using AES-256 encryption & PBKDF2. *Technology (IJEET)*, *12*(5), 1-7.

Kumar, M., & Kumar, D. (2023). An efficient gravitational search decision forest approach for fingerprint recognition. *Kuwait Journal of Science*, *50*(2A).

Loster, M., Koumarelas, I., & Naumann, F. (2021). Knowledge transfer for entity resolution with siamese neural networks. *Journal of Data and Information Quality (JDIQ)*, *13*(1), 1-25.

Modugula, R. S. R. (2020). *A Hybrid approach for Augmenting password security using Argon2i hashing and AES Scheme* (Doctoral dissertation, Dublin, National College of Ireland).

Mustacoglu, A. F., Catak, F. O., & Fox, G. C. (2020). Password-based encryption approach for securing sensitive data. *Security and Privacy*, *3*(5), e121.

Rehman, A., Harouni, M., Karchegani, N. H. S., Saba, T., Bahaj, S. A., & Roy, S. (2022). Identity verification using palm print microscopic images based on median robust extended local binary

pattern features and k-nearest neighbor classifier. *Microscopy research and technique*, *85*(4), 1224-1237.

Shekhar, M., Patgiri, R., Trivedi, A. K., & Dhar, P. (2023). A Critical Study of Biometrics and Their Fusion. In *2023 International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC)*, 1-7.

Solano, J., Rivera, E., Castelblanco, A., Tengana, L., Lopez, C., & Ochoa, M. (2021). A Siamese Neural Network for Behavioral Biometrics Authentication.

Suman, M., & Shobha, N. (2025). Advancements in biometric authentication: A systematic review of machine learning and cloud security innovations. *Grenze International Journal of Engineering and Technology*, *11*(2), 4954–4963.

Suman, M., Shobha, N., & Ashoka, S. B. (2026). Biometric Fingerprint Verification with Siamese Neural Network & Transfer Learning.

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.

Yong, L., Ma, L., Sun, D., & Du, L. (2023). Application of MobileNetV2 to waste classification. *Plos one*, *18*(3), e0282336.

Zhang, Z., Liu, S., & Liu, M. (2021). A multi-task fully deep convolutional neural network for contactless fingerprint minutiae extraction. *Pattern Recognition*, *120*, 108189.

Bibliographic information of this paper for citing:

M, Suman; N, Shobha; Muruhan, Sridevi; S, Vinothkumar; R, Ramkumar & Poovaraghan, R J (2026). Adaptive Fingerprint Verification Using Siamese Neural Networks and Transfer Learning for Robust Authentication of Damaged Prints. *Journal of Information Technology Management*, 18 (1), 1-16. https://doi.org/10.22059/jitm.2026.106251