

Development of an Improved Fingerprint Biometric Model for Automated Teller Machine Security System

SAMUEL, O. D.¹, AFOLABI, A. O.², ADEOSUN O. O.³, AKANDE, O.V.⁴, ADEPOJU, J. A.⁵

^{1,4} Department of Computer Science, Federal Polytechnic Ayede, Oyo State, Nigeria

² Department of Cybersecurity Science, Ladoke Akintola University of Technology, Oyo State, Nigeria

³ Department of Computer Science, Ladoke Akintola University of Technology, Oyo State, Nigeria

⁵ Department of Computer Science, Federal University of Agriculture and Technology, Okeho, Nigeria

Abstract- Fingerprint authentication provides a biometric approach for improving user verification in ATM systems. However, fingerprint images may contain variations and alterations that can affect reliable classification. This study developed a Hybrid Autoencoder–CNN–ANN model for fingerprint-based ATM authentication using the Sokoto Coventry Fingerprint Dataset (SOCOFing). The model used an autoencoder for feature representation, convolutional neural network (CNN) layers for spatial feature extraction, and artificial neural network (ANN) layers for classification. Fingerprint images were converted to grayscale, resized to 128×128 pixels, and normalized before training. The autoencoder was first trained to learn compact fingerprint representations, after which the learned features were used by the CNN–ANN classification stage. Experimental results showed that the developed model achieved a test accuracy of 89.48%, with 95% recall and 82% F1-score for the real fingerprint class, while the weighted F1-score was 90%. The confusion matrix recorded 3,934 altered fingerprints correctly classified as altered and 1,435 real fingerprints correctly classified as real. However, 563 altered fingerprints were classified as real, indicating that false acceptance remains a limitation. Compared with the CNN-based study of Okorie et al. [1], the developed model achieved higher accuracy, recall, and F1-score, although its precision was lower. The findings demonstrate the feasibility of combining autoencoder, CNN, and ANN techniques for fingerprint classification in a simulated ATM authentication environment.

Index Terms - Fingerprint authentication; biometric security; autoencoder; convolutional neural network; artificial neural network; SOCOFing; ATM security; deep learning.

I. INTRODUCTION

Automated Teller Machines (ATMs) have become an essential component of modern banking by providing

customers with convenient access to services such as cash withdrawal, balance inquiry, fund transfer, and other financial transactions. The widespread use of ATMs has also increased the importance of reliable user authentication because unauthorized access can result in financial loss and compromise of customer information. Conventional ATM authentication generally depends on a combination of a physical bank card and a Personal Identification Number (PIN). Although this approach provides a basic level of security, the authentication factors can be lost, stolen, copied, or disclosed to unauthorized persons. The continued dependence on possession-based and knowledge-based authentication therefore creates a need for alternative approaches that can provide stronger identity verification. Biometric authentication offers an alternative by verifying users through physiological or behavioural characteristics rather than something they possess or remember. Fingerprints are among the most established biometric characteristics because the patterns formed by ridges and valleys are distinctive among individuals and can be captured using electronic sensors. Fingerprint authentication can also support cardless access, thereby reducing dependence on physical cards during ATM transactions. However, the effectiveness of a fingerprint authentication system depends heavily on the quality of the captured image and the ability of the recognition model to distinguish between genuine and non-genuine fingerprint patterns. Variations in fingerprint images can arise from differences in finger placement, image quality, distortion, and other acquisition conditions. These variations can lead to incorrect acceptance or rejection during authentication.

Another important challenge is the presence of altered or forged fingerprints. An altered fingerprint may contain deliberate modifications to ridge patterns intended to interfere with recognition or impersonate another fingerprint. The availability of datasets containing both genuine and altered fingerprint images has therefore provided opportunities for developing automated methods for distinguishing between these classes. The Sokoto Coventry Fingerprint Dataset (SOCOFing), for example, contains real fingerprint images together with altered versions generated using different alteration techniques. Research using SOCOFing has demonstrated that machine-learning and deep-learning approaches can be applied to distinguish real and altered fingerprints [1]. Such datasets are particularly useful for investigating the ability of recognition models to learn discriminative fingerprint characteristics. Traditional fingerprint recognition methods often depend on manually designed features such as minutiae, ridge structures, texture information, or other descriptors. Although these features can be useful, their effectiveness may depend on the quality of the fingerprint image and the feature-extraction procedure. Deep learning has provided a different approach by allowing models to learn representations directly from input data. A systematic review of deep-learning applications in fingerprint authentication reported that deep learning has been applied to fingerprint preprocessing, quality enhancement, feature extraction, classification, and end-to-end recognition, with Convolutional Neural Networks (CNNs) being particularly common [2]. This ability to automatically learn representations makes deep learning suitable for developing fingerprint authentication systems.

CNNs are particularly relevant to fingerprint image analysis because they can learn spatial patterns from images through successive convolutional operations. Fingerprint ridge structures, local textures, and other spatial characteristics can therefore be learned by convolutional layers without requiring every feature to be manually specified. For example, FingerNet demonstrated the use of an end-to-end CNN framework for learning fingerprint representations and performing recognition [3]. CNN-based approaches have also been applied specifically to real and altered fingerprint classification using the SOCOFing dataset,

demonstrating the usefulness of learned image features for this task [1]. These studies support the application of CNNs to fingerprint recognition, but they also demonstrate that different architectural choices can influence the resulting representation and classification performance. Autoencoders provide another approach to representation learning. An autoencoder is a neural-network architecture that learns to encode input data into a lower-dimensional representation and reconstruct the original input from that representation. The encoder component can therefore learn compact representations that capture important characteristics of the input data. In fingerprint-related research, Saponara et al. applied a convolutional neural network autoencoder to fingerprint image reconstruction and demonstrated its ability to learn representations from complex fingerprint images [4]. This suggests that autoencoder-based representation learning can provide a useful preprocessing or feature-learning stage before a subsequent classification process.

The combination of different neural-network components provides an opportunity to exploit their complementary characteristics. Rather than using a single network to perform all aspects of feature learning and classification, a hybrid architecture can assign different stages of the process to different components. In the context of fingerprint authentication, an autoencoder can first learn a compact representation of fingerprint images, CNN layers can subsequently process spatial patterns within the learned representations, and ANN dense layers can perform the final classification. Hybrid deep-learning approaches have also been investigated in biometric authentication, showing the broader potential of combining neural-network architectures for representation learning and classification [5]. Despite the progress in deep-learning-based fingerprint recognition, much of the existing work has concentrated on CNN-based architectures or other individual deep-learning approaches. There is comparatively less attention to the combination of an autoencoder-based feature-learning stage with CNN spatial processing and ANN classification for real and altered fingerprint classification. This provides an opportunity to investigate whether a hybrid architecture can produce useful fingerprint

representations while maintaining effective classification performance. The present study addresses this gap by developing a Hybrid Autoencoder–CNN–ANN fingerprint biometric authentication model for ATM security.

The developed model uses the SOCOFing dataset containing real and altered fingerprint images. During preprocessing, the fingerprint images are converted to grayscale, resized to 128×128 pixels, and normalized to values between 0 and 1. The first stage of the approach uses an autoencoder trained to reconstruct the fingerprint images and learn their underlying representations. The encoder component is then used to obtain feature representations that are supplied to the CNN component for further spatial feature processing. The resulting features are passed to ANN dense layers for classification of the fingerprint images into the defined classes. The model is implemented using Python 3.11 and TensorFlow 2.19 and evaluated using classification performance measures including accuracy, precision, recall (sensitivity), specificity, and F1-score, together with recognition speed. The experimental evaluation is intended to determine the classification capability of the developed hybrid architecture rather than to claim performance of a fully deployed ATM hardware system. The study is conducted in a simulated environment using fingerprint images from SOCOFing.

The contribution of this study is therefore the development and evaluation of a hybrid Autoencoder–CNN–ANN architecture that combines unsupervised representation learning with CNN-based spatial processing and ANN classification for fingerprint-based ATM authentication. The study further provides an experimental comparison with an existing CNN-based fingerprint authentication model using the SOCOFing dataset, allowing the performance of the developed hybrid approach to be examined against a directly relevant baseline.

II. LITERATURE REVIEW

Fingerprint biometrics is widely used for identity verification because fingerprint patterns contain distinctive ridge and valley structures that can be used to differentiate individuals. However, fingerprint

recognition systems can be affected by poor image quality, variations in fingerprint appearance, and deliberate alterations or forgery. These challenges have encouraged the use of machine-learning and deep-learning techniques that can automatically learn useful patterns from fingerprint images. Reviews of fingerprint identification research have reported the application of deep-learning techniques to image enhancement, feature extraction, classification, and recognition [2], [6]. Deep learning has therefore become an important approach for improving fingerprint recognition systems. CNNs are particularly suitable for fingerprint images because convolutional operations can learn spatial patterns and local structures directly from the input images. Studies have demonstrated that CNN-based models can automatically extract discriminative fingerprint features without depending entirely on manually designed features [3], [7]. Efrizoni et al. evaluated different CNN configurations using the SOCOFing dataset and reported high performance across accuracy, precision, recall, and F1-score, demonstrating the effectiveness of CNN architectures for fingerprint recognition [7]. FingerNet also demonstrated the use of an end-to-end CNN framework for learning fingerprint representations and recognition [3]. These findings support the use of CNNs for extracting relevant characteristics from fingerprint images.

The application of CNNs to real and altered fingerprint classification has also been investigated using the SOCOFing dataset. Okorie et al. developed a CNN-based fingerprint authentication model using SOCOFing and reported an accuracy of 78.02%, precision of 79.00%, recall of 77.98%, and F1-score of 78.20% [1]. This study is particularly relevant to the present research because it uses the same dataset and provides a direct CNN-based benchmark. Aljafary and Hussian similarly developed a five-convolution-layer CNN for fingerprint classification using SOCOFing and reported high training and validation performance [8]. Jabbar et al. also investigated deep-learning techniques for fingerprint forgery detection and person identification [9]. These studies demonstrate the ability of CNN-based approaches to learn useful characteristics from fingerprint images and distinguish between different fingerprint classes. Traditional

feature-based methods have also been applied to real and altered fingerprint classification. Hameed et al. used texture features, including Histogram of Oriented Gradient (HOG) and Segmentation-based Feature Texture Analysis (SFTA), together with conventional classifiers to classify real and altered fingerprints using SOCOFing [10]. Their results demonstrate that handcrafted features can provide effective discrimination between authentic and altered fingerprints. However, such approaches depend on the selection and extraction of appropriate features. Deep-learning methods provide an alternative by learning representations directly from fingerprint images [2], [6].

Autoencoders provide another approach to feature representation. An autoencoder consists of an encoder that transforms an input into a compact representation and a decoder that reconstructs the original input. The encoder can therefore learn features that capture important characteristics of the input data. Saponara et al. applied a convolutional autoencoder to fingerprint image reconstruction and demonstrated its ability to learn representations from complex fingerprint images [4]. This provides a basis for using an autoencoder as an initial feature-learning stage before classification. The combination of different neural-network components has also been investigated in biometric authentication. Hussian et al. proposed a hybrid CNN–LSTM architecture in which CNN layers extracted fingerprint features while the LSTM component further processed the learned representations [5]. Ali et al. investigated another hybrid approach that combined fingerprint texture and geometric features with gradient boosting for fake fingerprint classification using SOCOFing [11]. These studies demonstrate that combining complementary feature-learning or classification techniques can provide an alternative to relying on a single architecture.

Recent research has continued to investigate deep-learning methods for altered fingerprint detection. Madhav et al. examined real and synthetic fingerprint modifications using the SOCOFing dataset and an InceptionV3-based approach [12]. Other research has similarly demonstrated the usefulness of deep-learning models for identifying altered or forged fingerprint

samples. These studies indicate that the representation learned by a model and the architecture used for classification are important factors in distinguishing real fingerprints from altered fingerprints. Although existing studies have established the usefulness of CNNs, autoencoders, and hybrid approaches in fingerprint and biometric applications, the reviewed studies generally focus on individual architectures or hybrid combinations different from the one investigated in this research. In particular, limited attention has been given to a sequential architecture that uses an autoencoder for initial feature learning, CNN layers for spatial feature processing, and ANN layers for final classification of real and altered fingerprint images. The present study addresses this gap by developing and evaluating a Hybrid Autoencoder–CNN–ANN model using the SOCOFing dataset. The performance of the developed model is further compared with the CNN-based approach of Okorie et al. [1], which provides a directly relevant benchmark because it uses the same dataset.

III. METHODOLOGY

This study adopted an experimental research design to develop and evaluate a hybrid fingerprint biometric authentication model for ATM security. The approach involved collecting and preparing fingerprint images, learning feature representations using an autoencoder, processing the learned representations with a Convolutional Neural Network (CNN), and performing final classification using Artificial Neural Network (ANN) layers. The complete process was implemented as a sequential pipeline so that each stage could be developed and evaluated as part of the overall authentication model. The methodology was organized into separate modules for dataset handling, image preprocessing, autoencoder training, feature extraction, CNN processing, ANN classification, and model evaluation. This modular structure allows the individual stages to be reproduced and modified without changing the entire system.

The study used the Sokoto Coventry Fingerprint Dataset (SOCOFing), which contains fingerprint images collected from African subjects together with altered versions of the fingerprints. The dataset includes real fingerprint images and altered images

produced through different alteration techniques. For this study, the fingerprint images were organized into two classification categories: real fingerprints and altered fingerprints. The images were used as the input data for training and evaluating the biometric model. The dataset was divided into the required training, validation, and testing subsets before model training. The training subset was used to learn the model parameters, the validation subset was used during model development, and the testing subset was reserved for final evaluation.

Preprocessing was performed to provide a consistent input format for the neural networks. Each fingerprint image was first converted to grayscale so that the model operated on a single image channel rather than separate colour channels. The images were then resized to 128×128 pixels. Resizing ensured that all fingerprint images had the same spatial dimensions before being supplied to the model. Pixel values were normalized to the range 0 to 1. This was performed by scaling the original pixel intensity values so that the neural networks could process inputs within a consistent numerical range. After preprocessing, the images were converted into the required tensor format for TensorFlow/Keras. The corresponding class labels were retained so that the processed images could subsequently be used for classification.

The system uses a sequential Autoencoder–CNN–ANN architecture. The architecture consists of three main learning stage, Autoencoder, CNN, and ANN, as shown in fig. 2.1. The autoencoder provides the initial feature-learning stage. Its encoder learns a compact representation of the fingerprint image while the decoder reconstructs the input from that representation. After training, the encoder is used to obtain the learned fingerprint features. The extracted representation is then passed to the CNN component. The CNN processes the representation through convolutional operations to learn relevant spatial characteristics of the fingerprint patterns. The resulting features are passed to ANN dense layers, which perform the final classification into the defined fingerprint classes. This arrangement allows the three components to perform different functions rather than requiring one network to perform the entire learning process.

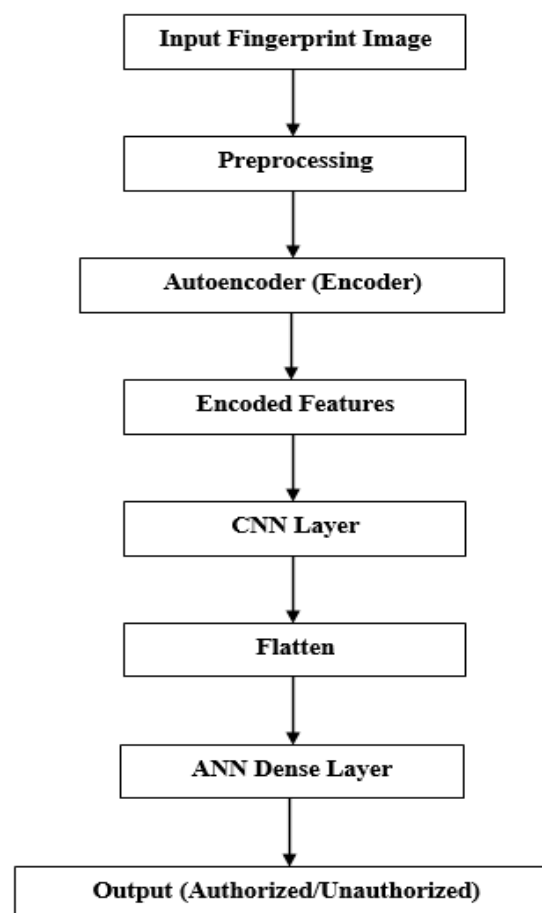


Fig. 2.1: Architectural Model Diagram

The first learning stage uses an autoencoder consisting of an encoder and decoder. The encoder receives the preprocessed fingerprint image and transforms it into a lower-dimensional feature representation. The decoder attempts to reconstruct the original fingerprint image from this representation. During training, the difference between the original image and reconstructed image is used as the reconstruction loss. Binary cross-entropy was used as the reconstruction loss function. The autoencoder was trained using the training fingerprint images. The validation data were used to monitor the reconstruction process during training. Once autoencoder training was completed, the decoder was no longer required for the classification stage. The trained encoder was retained and used to transform the preprocessed fingerprint images into learned feature representations. The use of an autoencoder for fingerprint representation learning

is consistent with previous fingerprint research involving convolutional autoencoder architectures.

The feature representations produced by the trained encoder were supplied to the CNN component. The purpose of this stage was to further process the learned fingerprint representations and identify spatial patterns that could contribute to distinguishing the two fingerprint classes. The CNN performs convolutional operations on its input representation. These operations allow the network to learn local patterns and relationships within the fingerprint features without requiring all features to be manually specified. The output from the convolutional processing stage was transformed into a suitable feature representation for the subsequent ANN classification stage.

The processed CNN features were supplied to fully connected ANN layers. These layers combine the learned features and perform the final classification task. The final ANN output corresponds to the two classes defined for the study: real fingerprint and altered fingerprint. During training, the network learns the relationship between the extracted fingerprint characteristics and their corresponding class labels. The trained classifier can subsequently receive a previously unseen preprocessed fingerprint image and produce a predicted class.

The model was implemented using Python 3.11 and TensorFlow 2.19 with Keras. Additional Python libraries used during development included NumPy, OpenCV, Scikit-learn, and Matplotlib. The implementation was organized into separate modules for data loading, preprocessing, model construction, training, and evaluation. This separation makes the experimental procedure easier to reproduce and allows individual components of the system to be modified independently. The autoencoder was trained first. The trained encoder was then used to generate feature representations for the subsequent CNN-ANN classification stage. The CNN and ANN components were subsequently trained using the extracted representations and their corresponding class labels. After training, the developed model was saved in HDF5 (.h5) format for subsequent loading and evaluation. The experiments were conducted in a simulated computing environment rather than on a

physical ATM device. Therefore, the methodology evaluates the machine-learning authentication component using fingerprint images rather than a complete ATM hardware implementation.

The developed model was evaluated using standard classification metrics. Accuracy was used to measure the proportion of correctly classified fingerprint samples. Precision was used to measure the proportion of samples classified as a particular class that actually belonged to that class. Recall (sensitivity) was used to measure the proportion of samples belonging to a class that were correctly identified. Specificity was used to measure the model's ability to correctly identify samples belonging to the negative class. F1-score was used to provide a combined measure of precision and recall. A confusion matrix was also generated to examine the numbers of correctly and incorrectly classified samples for the real and altered fingerprint classes. Recognition speed was considered to assess the time required by the model to process a fingerprint during prediction. The complete experimental workflow followed these steps:

- i. Dataset acquisition: SOCOFing fingerprint images were obtained and organized into real and altered classes.
- ii. Image preprocessing: Images were converted to grayscale, resized to 128×128 pixels, and normalized to the range 0–1.
- iii. Autoencoder training: The preprocessed fingerprint images were used to train the autoencoder for representation learning.
- iv. Feature extraction: The trained encoder was used to transform fingerprint images into learned feature representations.
- v. CNN processing: The extracted representations were processed by the CNN component to learn spatial fingerprint characteristics.
- vi. ANN classification: CNN outputs were passed to ANN dense layers for classification.
- vii. Model evaluation: The trained model was evaluated using accuracy, precision, recall, specificity, F1-score, confusion matrix analysis, and recognition speed.
- viii. Model storage: The trained model was saved in HDF5 format for subsequent use.

This workflow provides the complete sequence from fingerprint-image input to final classification while keeping the experimental procedures separate from the results reported in the next section.

IV. RESULTS AND DISCUSSION

The autoencoder was trained for three epochs to learn useful representations of the fingerprint images. Table 4.1 presents the training and validation losses obtained during the training process.

Table 4.1: Autoencoder Training and Validation Loss

Epoch	Training Loss	Validation Loss
1	0.4543	0.4081
2	0.4104	0.4020
3	0.4064	0.3995

The training loss decreased from 0.4543 in Epoch 1 to 0.4064 in Epoch 3. Similarly, the validation loss decreased from 0.4081 to 0.3995. The reduction in both losses indicates that the autoencoder improved its ability to reconstruct the fingerprint images during training. The validation loss also remained close to the training loss, indicating that the reconstruction performance was consistent between the training and validation data during the three epochs. The learned encoder representations were subsequently used as input to the CNN-ANN classification stage.

Following autoencoder feature learning, the extracted representations were passed to the CNN-ANN classification model. The training and validation performance over five epochs is shown in Table 4.2.

Table 4.2: CNN-ANN Training Performance Across Epochs

Epoch	Training Accuracy	Training Loss	Validation Accuracy	Validation Loss
1	0.6812	0.5922	0.8089	0.4199
2	0.8243	0.4015	0.8833	0.2999
3	0.8667	0.3148	0.9111	0.2522
4	0.8867	0.2925	0.8789	0.2871
5	0.8979	0.2473	0.8867	0.2599

The training accuracy increased from 68.12% in Epoch 1 to 89.79% in Epoch 5, while the training loss decreased from 0.5922 to 0.2473. Validation accuracy increased from 80.89% to 91.11% by Epoch 3, before decreasing slightly to 88.67% in Epoch 5. The lowest validation loss was recorded in Epoch 3 at 0.2522, while the highest validation accuracy was also

obtained in Epoch 3 at 91.11%. After Epoch 3, validation performance fluctuated slightly, whereas training accuracy continued to improve. This indicates that the model continued learning from the training data, while its validation performance did not improve consistently during the final two epochs. Overall, the results show that the CNN-ANN classifier learned to

distinguish the fingerprint classes effectively after receiving the representations generated by the autoencoder.

The developed model achieved a test accuracy of approximately 89%, with an exact accuracy of 89.48%. The class-level classification results are presented in Table 4.3.

Table 4.3: Classification Performance of the Developed Model

Class	Precision	Recall	F1-Score
Altered	98%	87%	93%
Real	72%	95%	82%
Weighted Average	—	—	90%

The model recorded a 98% precision for altered fingerprints, meaning that most samples classified as altered were actually altered. Its recall for the altered class was 87%, indicating that some altered fingerprints were classified as real. For real fingerprints, the model achieved 72% precision and 95% recall. The high recall indicates that the model correctly identified most of the real fingerprints in the test data. However, the lower precision shows that some fingerprints classified as real were actually altered. The weighted F1-score was 90%, showing a

strong overall balance between precision and recall when the class distribution is taken into account.

The confusion matrix provides a more detailed view of the classification results. The model produced the following results as presented in fig. 4.1

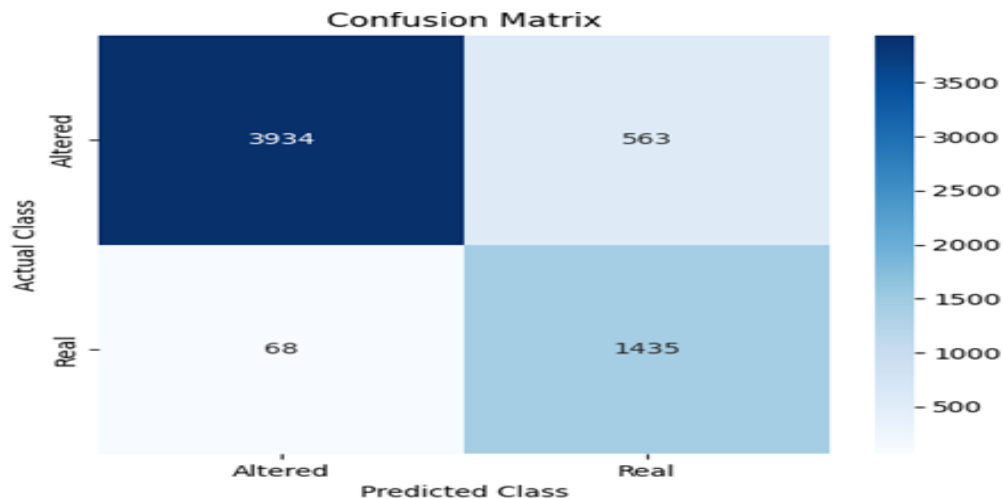


Fig. 4.1: Confusion Matrix of the Developed Fingerprint Authentication System

The model correctly classified 3,934 altered fingerprints as altered and 1,435 real fingerprints as real. These represent the correctly classified samples. However, 563 altered fingerprints were classified as real, while 68 real fingerprints were

classified as altered. The 563 altered fingerprints incorrectly classified as real are particularly important for an authentication application because such classifications represent cases where an altered fingerprint could potentially be accepted as genuine.

In contrast, the 68 real fingerprints classified as altered represent genuine users who could potentially be rejected. Therefore, although the model achieved high overall classification performance, the confusion matrix shows that classification errors remain, particularly in distinguishing some altered fingerprints from real fingerprints.

To assess the performance of the developed model against a relevant existing approach, its results were compared with the CNN-based fingerprint authentication model developed by Okorie et al. [1]. The comparison is particularly relevant because both studies use the SOCOFing dataset and report the same major classification metrics.

Table 4.3: Comparison of the Developed Fingerprint Biometric Model with Okorie et al. (2026)

Performance Metric	Okorie et al. (2026)	Developed Fingerprint Biometric Model
Accuracy (%)	78.02	89.48
Precision (%)	79.00	72.00
Recall (%)	77.98	95.00
F1-score (%)	78.20	82.00

The developed model achieved an accuracy of 89.48%, compared with 78.02% reported by Okorie et al., representing an improvement of 11.46 percentage points. Recall increased from 77.98% to 95.00%, an improvement of 17.02 percentage points. The F1-score increased from 78.20% to 82.00%, representing a 3.80 percentage-point improvement. However, precision decreased from 79.00% to 72.00%. This indicates a trade-off between precision and recall: the developed model identified a larger proportion of the relevant class but also produced more false-positive classifications. The results reported by Okorie et al. provide a useful CNN-based benchmark for interpreting the performance of the developed model [1]. The main architectural difference is that Okorie et al. used a CNN-based model, whereas the developed system uses a sequential Autoencoder–CNN–ANN architecture. The autoencoder provides an initial representation-learning stage, followed by CNN-based spatial feature processing and ANN classification. The additional feature-learning stage may have contributed to the differences in classification performance, although the results alone do not establish that the architecture was the sole cause.

The experimental results demonstrate that the developed Autoencoder–CNN–ANN model was able to learn useful representations from fingerprint images and use those representations for classification. The decreasing autoencoder training and validation losses show that the reconstruction stage successfully learned from the fingerprint data. The CNN–ANN stage also showed substantial improvement during training. Training accuracy increased from 68.12% to 89.79%, while validation accuracy reached a maximum of 91.11% at Epoch 3. The subsequent variation in validation performance suggests that additional training did not continuously improve validation accuracy. The final classification results further demonstrate that the model was effective at distinguishing between real and altered fingerprints. The model achieved 89.48% test accuracy and a 90% weighted F1-score. The high recall of 95% for the real class shows that most real fingerprints were correctly identified. However, the confusion matrix shows that 563 altered fingerprints were classified as real, which remains an important issue for a security-oriented authentication system.

Compared with the CNN-based study of Okorie et al. [1], the developed model recorded higher accuracy,

recall, and F1-score but lower precision. The comparison therefore shows an improvement in several reported performance measures while also revealing a precision–recall trade-off. Previous studies have also demonstrated the usefulness of deep-learning approaches for fingerprint classification and altered-fingerprint analysis. CNN-based approaches have been applied to SOCOFing and other fingerprint datasets, while autoencoder architectures have demonstrated the ability to learn useful fingerprint representations [4]. The results of the present study are therefore consistent with the broader use of learned representations for fingerprint analysis. Overall, the findings indicate that combining autoencoder-based representation learning, CNN feature processing, and ANN classification provides a workable approach for real and altered fingerprint classification. However, the false acceptance of altered fingerprints observed in the confusion matrix shows that further improvement would be necessary before considering deployment in a real ATM environment.

V. CONCLUSION

This study developed a Hybrid Autoencoder–CNN–ANN model for fingerprint-based ATM authentication using the SOCOFing dataset. The developed model combined autoencoder-based representation learning, CNN spatial feature processing, and ANN classification to distinguish between real and altered fingerprint images. The experimental results showed that the autoencoder successfully learned fingerprint representations, while the CNN–ANN classification stage achieved a test accuracy of 89.48% and a weighted F1-score of 90%. The model also achieved 95% recall for real fingerprints, indicating that most real fingerprint samples were correctly identified. However, the confusion matrix showed that 563 altered fingerprints were classified as real, demonstrating that false acceptance remains an important limitation. Compared with the CNN-based model of Okorie et al. [1], the developed model achieved higher accuracy, recall, and F1-score, although its precision was lower. The findings therefore demonstrate that the developed hybrid architecture can effectively classify real and altered fingerprints in a simulated authentication environment. The study demonstrates the feasibility of

combining Autoencoder, CNN, and ANN techniques for fingerprint-based authentication. However, further testing and optimization are required before the model can be implemented in a real ATM environment.

REFERENCES

- [1] M. K. Okorie, N. J. Ngene, U. C. Ugwa, and G. O. Ota, “Fingerprint Recognition Using Convolutional Neural Network (CNN) For Secure Authentication Systems,” *European Journal of Theoretical and Applied Sciences*, vol. 4, no. 3, 2026. [European Journal of Theoretical and Applied Sciences](#)
- [2] H. Chiroma, “Deep Learning Algorithms based Fingerprint Authentication: Systematic Literature Review,” *Journal of Artificial Intelligence and Systems*, 2021. [Institute of Electronics and Computer](#)
- [3] S. Minaee, E. Azimi, and A. A. Abdolrashidi, “FingerNet: Pushing the Limits of Fingerprint Recognition Using Convolutional Neural Network,” 2019. [arXiv](#)
- [4] S. Saponara, A. Elhanashi, and Q. Zheng, “Recreating Fingerprint Images by Convolutional Neural Network Autoencoder Architecture,” *IEEE Access*, 2021. [IEEE](#)
- [5] A. Hussian, F. Murshed, M. Al-Andoli, and G. Aljafari, “A Hybrid Deep Learning Approach for Secure Biometric Authentication Using Fingerprint Data,” *Computers*, vol. 14, p. 178, 2025.
- [6] H. G. Muhammad and Z. A. Khalaf, “A Survey of Fingerprint Identification System Using Deep Learning,” *International Journal of Computing and Digital Systems*, 2025. [International Journal of Computing and Digital Systems](#)
- [7] L. Efrizoni, S. Armoogum, and M. Z. Zakaria, “Deep Learning Innovations in Fingerprint Recognition: A Comparative Study of Model Efficiencies,” *International Journal of Advances in Artificial Intelligence and Machine Learning*, 2024. [International Journal of Advances in Artificial Intelligence and Machine Learning](#)
- [8] G. H. Aljafary and A. Hussian, “Deep Convolutional Neural Networks for Fingerprint Classification,” 2025.

- [9] M. A. A. Jabbar, A. Radhi, S. A. Z. Mghames, S. Behadili, and M. Alsaedi, "Fingerprint Forgery Detection and Person Identification Based on Deep Learning," *Iraqi Journal of Science*, 2025. [Iraqi Journal of Science](#)
- [10] S. S. Hameed, I. T. Ahmed, and O. M. Al Okashi, "Real and Altered Fingerprint Classification Based on Various Features and Classifiers," *Computers, Materials & Continua*, 2022.
- [11] M. S. Ali, A. Akram, J. Rashid, M. A. Jaffar, D. Shah, S. Ali, and M. Tahir, "Fake Fingerprint Classification Using Hybrid Features Learning With Gradient Boosting," *Applied Computational Intelligence and Soft Computing*, 2025. [Wiley](#)
- [12] Y. Madhav, S. China Venkateshwarlu, and D. Nagaraju, "Advanced Fingerprint Alteration Detection: A Comparative Analysis of Real and Synthetic Modifications Using InceptionV3 on the SOCOFing Dataset," 2025.