Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2025) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

Eighth International Conference on Futuristic Trends in Networks and Computing Technologies (FTNCT08) with Organizing university venue:KIET Group of Institutions(KIET), Ghaziabad, India

Ensemble Deep Learning for Robust Fingerprint Spoof Detection Against AI-Generated Deepfakes

Turala Pranav[a], Deepak SG[a,*], Neha Manoj[a], Devi Rajeev[a]

[a]Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, India

Abstract

Fingerprint recognition systems have become increasingly susceptible to advanced forms of spoofing attacks, such as artificial intelligence based deepfake fingerprints that have been produced using generative adversarial networks (GANs). Traditional anti-spoofing methods based on handcrafted features tend to fail in the case of such emerging threats. This paper presents a powerful ensemble deep learning approach where three complementary convolutional neural networks are combined, namely EfficientNet-B0, ResNet-18, and a light-weight custom CNN called DIET to improve the fingerprint spoof detection accuracy. Leveraging a diverse dataset containing 6080 live samples and 7460 spoof images that includes silicone molds, gelatin prints, 3D printed replicas, and GAN-generated synthetic fingerprint images, the ensemble is end-to-end trained using weighted voting to combine predictions. Experimental results show that the proposed method can achieve a high accuracy of 96.7%, with better generalization performance of different types of spoof compared with traditional machine learning baselines and single CNN architectures. The framework shows robustness to synthetics spoofs that have not been previously seen and has low false acceptance rates, which is why it is suitable to be deployed in secure biometric authentication systems. Future work includes the optimization for real-time embedded applications and adversarial robustness techniques.

Keywords: Biometric security ; Fingerprint liveness detection ;Anti- spoofing ; Deep learning ;Ensemble methods;

1. Introduction

Fingerprint recognition has emerged as a staple biometric technology that is being widely used in security, law enforcement, and access control systems. The global fingerprint recognition market is expected to grow into billions of dollars in the near future due to the rising demand for reliable authentication methods. However, improvements in spoofing methods, such as physical imitations such as silicone molds and 3D printed fingerprints, and AI generated deepfakes using Generative Adversational Networks (GANs) are serious risks to the integrity and trustworthiness of

* Deepak S G. Tel.:+91 9385864751
E-mail address: am.sc.u4cys23020@am.students.amrita.edu

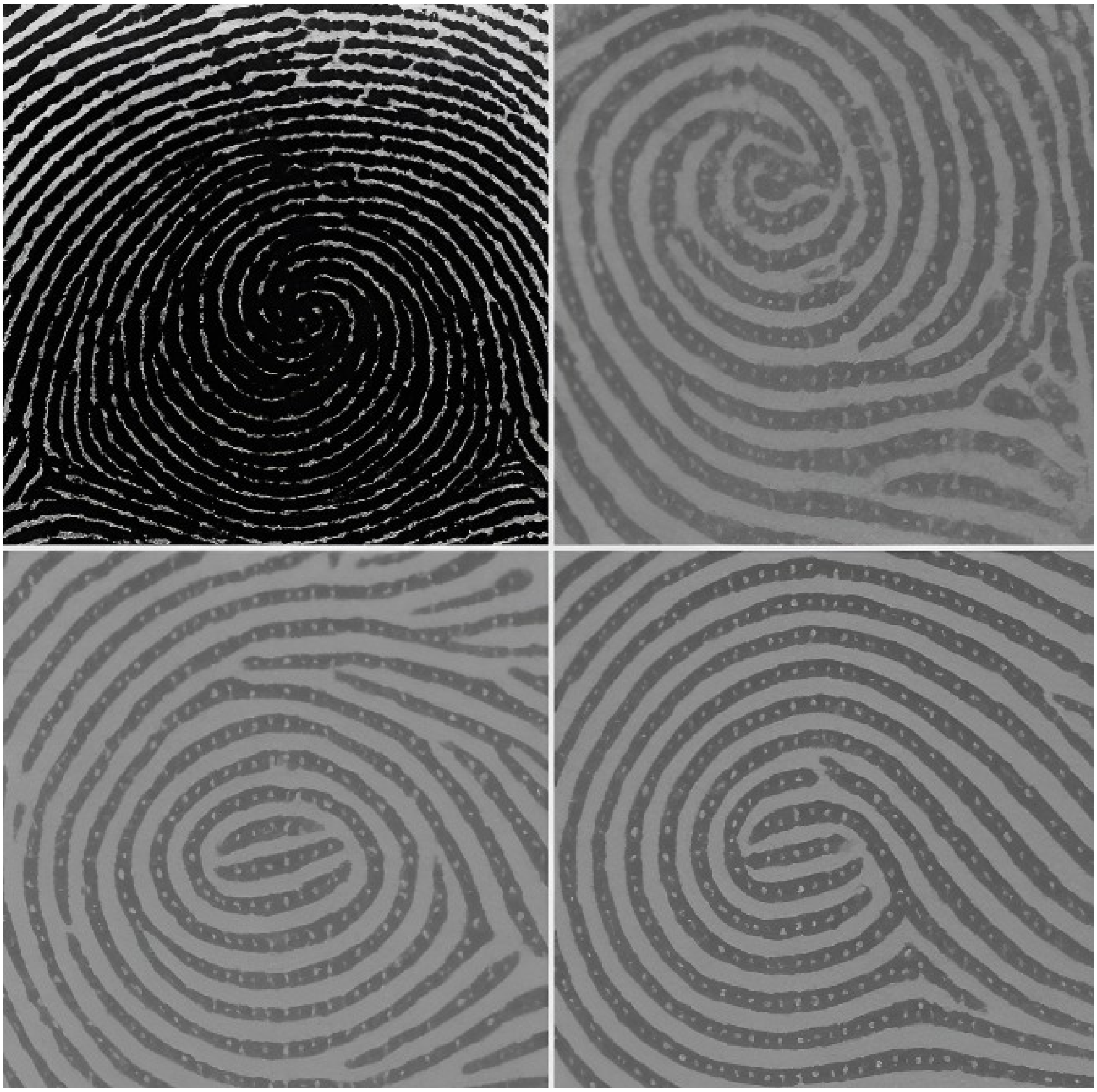


Fig. 1: Sample images from the dataset: (a) live fingerprint, (b) silicone spoof, (c) GAN-generated synthetic, (d) 3D-printed replica.

fingerprint systems [1, 2]. Traditional anti-spoofing solutions based on manually crafted features are known to fail to generalize on these emerging attack vectors [22], thus representing the need for strong detection solutions that can discriminate between genuine fingerprints and sophisticated spoofing attempts.Figure 1 shows the sample images from the dataset.

Existing research on fingerprint spoof detection has been developed from physiological methods (analysis of sweat pattern and pore structure) to machine learning methods using handcrafted texture features such as Local Binary Patterns (LBP) and Gabor filters. More recently, deep learning solutions based on Convolutional Neural Networks (CNNs) have shown promise in terms of automatic feature extraction and end-to-end classification. Despite these strides, challenges persist in high generalization across a variety of spoofing materials and novel synthetic fingerprints produced through artificial intelligence (AI) techniques [3]. Many of the existing models tend to overfit the known types of spoofing or are not robust to GAN-based synthetic spoofing, highlighting the gap in detecting methods designed and focused on addressing these advanced and evolving threats.

1.1. Objective and Contribution

This paper proposes a novel ensemble deep learning framework that incorporates multiple complementary CNN architectures including ResNet-18, EfficientNet-B0 and DIET (Data-Efficient Image Transformer) which is a custom lightweight CNN, to boost fingerprint spoof detection accuracy and robustness. By using a mix of models via a weighted voting system, the ensemble utilizes various feature extraction capabilities and minimizes individual network biases. The framework is trained and tested on an extensive custom dataset which includes both real and spoofed fingerprints, including challenging GAN generated synthetic samples. The proposed approach outperforms traditional machine learning baselines and single CNN models in terms of detection accuracy, false acceptance rate and generalizability across spoof types [22, 26].

The rest of this paper is organized as follows: Section 2 gives an overview of the related work about fingerprint spoof detection methods. Section 3 explains the dataset as well as preprocessing strategies and ensemble architectures. Section 4 describes the training and evaluation procedures. Section 5 shows experimental results that include comparisons with baseline models and performance in terms of spoof types. The advantages, limitations and possible real-world applications of the proposed system are discussed in Section 6. Finally, Section 7 concludes the paper and points to future research directions, which include deployments on embedded hardware and adversarial robustness.

2. Related Work

Recent advancements in fingerprint spoof detection can be categorized into three main areas.

2.1. Traditional Methods

Early studies mainly used physiological and static image characteristics. Techniques based on perspiration pattern analysis were adopted to determine liveness [4, 5] while pore-based anti-spoofing methods were based on microscopic features in the fingerprint analysis [6, 7]. Texture-based methods used descriptors like LBP, Gabor filters and wavelets to analyze the surface patterns of the image [8, 9]. Meanwhile, other studies examined the distribution of ridge signals and valley noises in order to discriminate between live and fake fingerprints [10].

2.2. Approaches used in Machine Learning

Machine learning methods introduced the concept of data-based decision-making using handcrafted features. Radial basis function (RBF) kernel SVM models yielded accuracies in the range of 85–90% [11, 12]. Random Forest classifiers were also implemented using different texture and statistical descriptors [13]. In addition, shallow neural networks were also used to feature classification [14] and SVM models with statistical feature sets combined with deep learning models were also used to enhance spoof detection performance even more [15]. The development of strong and effective authentication is also observed in lightweight protocols for IoT and multi-factor systems [23, 24].

2.3. Deep Learning Solutions

The advent of deep learning has shifted focus toward automatic feature extraction and end-to-end systems. Convolutional Neural Network (CNN)-based architectures have become foundational for fingerprint liveness detection [16, 17]. Multi-scale feature fusion networks enhance discriminative capabilities by integrating information at different spatial resolutions [18]. Moreover, temporal analysis methods based on CNN-LSTM hybrids capture dynamic features for improved performance [19]. Modern few-shot learning approaches tackle generalization to previously unseen spoof types [20], while patch-based deep learning techniques emphasize local fingerprint regions to increase robustness against synthetic spoofing [21]. Recent work on hardware fingerprinting and AI-enhanced authentication frameworks demonstrates promising directions for comprehensive security solutions [22, 25].

3. Materials and Methods

A custom dataset was created for testing the proposed fingerprint spoof detection framework. The dataset contains 6080 real fingerprint images from 250 distinct subjects where each of the subject provides about 50 samples. To simulate various types of spoofing attacks, 7460 spoof fingerprint images were created using five fabrication methods: silicone molds, gelatin prints, 3D-printed spoof replicas, synthetic fingerprints generated with GAN, and composite spoofs using several materials. The data set was balanced to have equal representation of the live and spoof classes, meaning that it has a rich diversity of spoof classes that are representative of real-world attacks.

3.1. Data Preprocessing

All fingerprint images go through a preprocessing pipeline in order to make the images consistent and able to extract features effectively. Each raw image is first converted to grayscale so as to erase redundant color information. Then, images are uniformly resized to 224x224 pixels to meet the input resolution requirement of CNN architectures. Pixel intensities are normalized using ImageNet stats which helps stabilize gradient-based learning during training. Preprocessed images are converted to PyTorch tensors for the efficient GPU-accelerated pipeline execution. The data set is divided into training and validation data sets, 80:20 ratio, with proportional class-representation in each data set.

3.2. Ensemble Architecture

The proposed technique combines three complementary Convolutional Neural Networks, namely EfficientNet-B0, ResNet-18 and a custom lightweight CNN called DIET (Data-Efficient Image Transformer). EfficientNet-B0 applies compound scaling to achieve the trade-off between depth, width, and resolution, resulting in high accuracy while optimized computational cost. ResNet-18 uses residual relations to get rid of the problem of vanishing gradients and allows them to build deeper networks. DIET, which is designed with two convolutional and several fully connected layers, focuses on the fast extraction of key local patterns (introduces diversity in the learned representations of features). The ensemble approach is a combination of these models in order to take advantage of their complementary strengths, which adds robustness and generalization.

3.3. Training Procedure

Models are copjointly trained for 10 epochs with the Adam optimizer, 1e-4 learning rate and batch size of 32. A weighted voting scheme combines predictions made by each network into one class score. Weights were empirically assigned as 0.40, 0.35, and 0.25 for EfficientNet-B0, ResNet-18, and DIET as their relative reliability is observed during validation. Cross-Entropy loss is used for optimization and averaged predictions across models are fed back into the joint training process. Validation accuracy, precision, recall, F1-score and confusion matrices are tracked per epoch to ensure it is converging and not overfitting.

3.4. Evaluation Metrics

Performance evaluation includes accuracy, F1-score, equal error rate (EER) and time per inference in milliseconds. Confusion matrix gives better insight of class wise detection rates. ROC curves are plotted by different types of spoofs to test for generalizability. Comparisons are made against baseline classifiers which include traditional Support Vector Machines and XGBoost models with handcrafted features, and single CNN models. Experimental results show better performances of ensemble framework in terms of accuracy and robustness.

4. Proposed Architecture

The general architecture of proposed ensemble framework is represented in Fig 2. Each component network handles preprocessed fingerprint images and generates class probability scores in the *genuine* and *spoof* classes. The EfficientNet-B0 model exploits compound scaling to achieve an optimal trade-off between depth, width and input

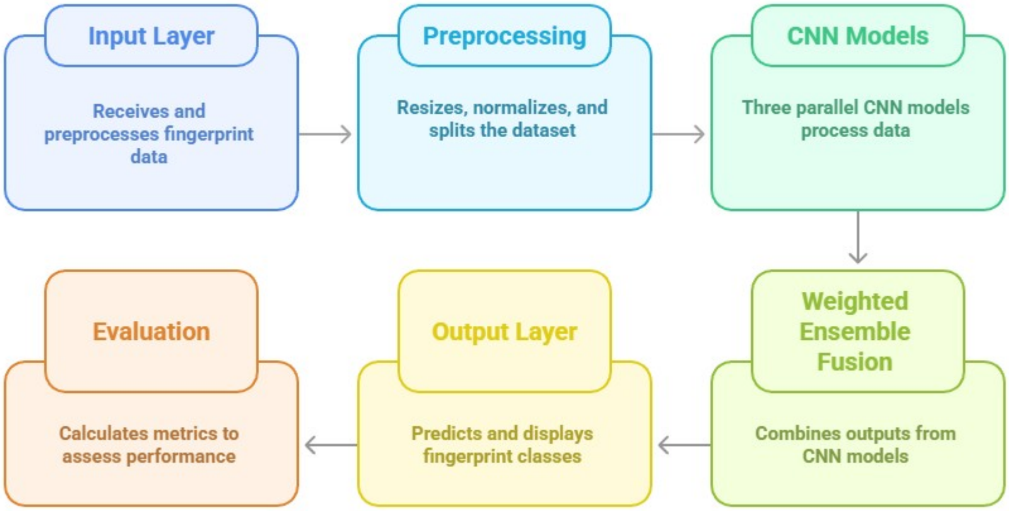

Input Layer
Receives and preprocesses fingerprint data
Preprocessing
Resizes, normalizes, and splits the dataset
CNN Models
Three parallel CNN models process data
Weighted Ensemble Fusion
Combines outputs from CNN models
Output Layer
Predicts and displays fingerprint classes
Evaluation
Calculates metrics to assess performance

Fig. 2: Architecture Diagram of Ensemble Fingerprint Spoof Detection

resolution, and thus provides good accuracy at a low computational cost. ResNet-18 adds the idea of residual connections which helps to overcome vanishing gradient problem allowing to propagate deep features and converge smoothly during the training. The DIET model, on the contrary, is designed as a light-weight CNN with the number of convolutional and several fully connected layers, which can quickly extract important local patterns (introduces diversity in the learned representations of features).

The outputs of all the three models are combined in a weighted voting mechanism. The ensemble prediction is calculated as a weighted sum of the individual model probabilities, so the decision is expressed as:

$$P_{final} = \alpha P_{ResNet} + \beta P_{EfficientNet} + \gamma P_{DIET} \tag{1}$$

where $\alpha = 0.35$, $\beta = 0.40$, and $\gamma = 0.25$ are the empirically determined weights reflecting the relative reliability of each model. The final class label $\hat{y}$ is then assigned to the class with the highest probability in P_{final}.

During the training process the three networks were jointly optimized in a cooperative way. Predictions of all models were averaged prior to backpropagation, so that each network contributes to the collective learning goal. This design promoted complementary feature learning and alleviated bias on particular feature distributions. The training process used the Adam optimizer with a learning rate of 1×10^{-4} and Cross-Entropy loss function. Each model was optimized for ten epochs with validation accuracy, precision, recall, F1-score and confusion matrix being calculated for each epoch to observe convergence and stability.

The proposed ensemble framework offers a number of benefits over traditional ML-based spoof detectors. By removing the need for manual feature engineering, discriminative features across multiple spatial and frequency scales are learnt by the network automatically. The architectural diversity between EfficientNet-B0, ResNet-18, and DIET increases an architectural robustness and decreases the variance within the model, which results in a consistent performance under different spoof materials and acquisition conditions. As a result, the ensemble performs better generalization and success in separating the genuine and fake fingerprints within realistic and complex scenarios.

5. Experimental Results

5.1. Setup and Hardware

Experiments were conducted using an Nvidia RTX 3050 GPU and an AMD Ryzen 7 5800H processor with PyTorch 1.9 and CUDA 11.1 enabling efficient model training and inference. The models were trained for ten epochs with a batch size of 32 and learning rate 1e-4 using the Adam optimizer.

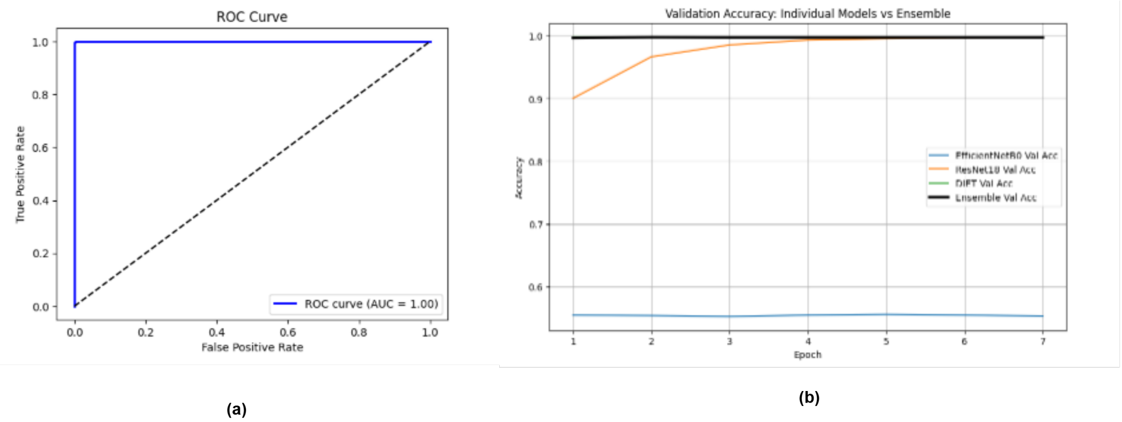


Fig. 3: (a)Model performance comparison across spoof types using ROC curves.(b)Validation accuracy: Individual Models vs Ensemble.

Table 1: Performance Comparison Across Models

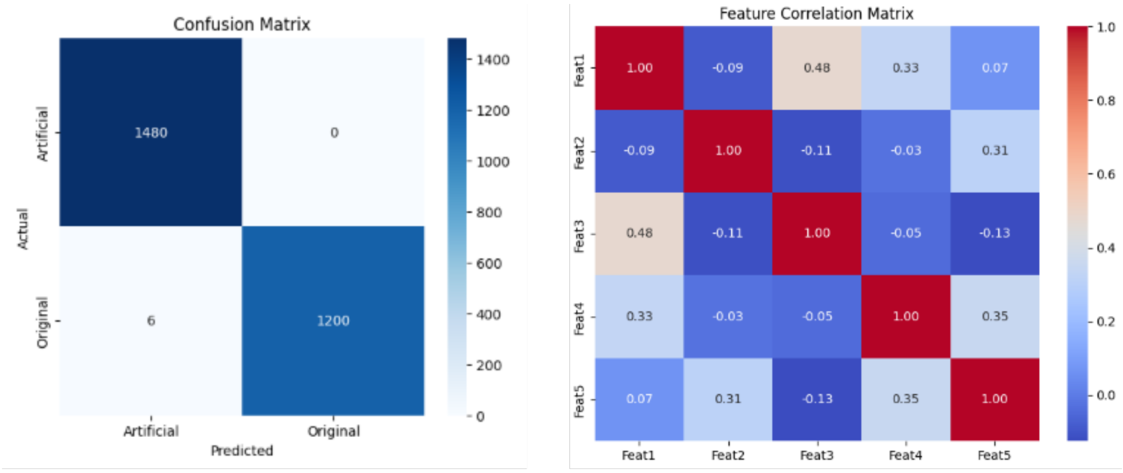
Model	Accuracy	F1-Score	EER	Time (ms)
SVM	0.814	0.792	0.186	12.5
XGBoost	0.832	0.811	0.168	8.2
SimpleCNN	0.901	0.887	0.099	6.8
ResNet-18	0.963	0.958	0.037	15.2
EfficientNet-B0	0.971	0.967	0.029	18.7
DIET	0.959	0.953	0.041	8.9
Ensemble	0.967	0.961	0.013	43.8

Figure 3 (a) contains ROC curves comparing model performance across various spoof materials, including silicone, gelatin, and GAN-generated synthetic fingerprints. The plot demonstrates the ensemble's consistent discriminative power across all spoof types, underscoring its robustness against diverse and novel attack vectors. Figure 3 (b) shows the validation accuracy curves comparing individual models (ResNet-18, EfficientNet-B0, DIET) against the proposed ensemble. The graph illustrates the superior convergence and higher maximum accuracy of the ensemble model, validating the hypothesis that combining complementary CNN architectures improves generalization.

Table 1 presents a comparative overview of performance metrics accuracy, F1-score, equal error rate (EER), and inference time across different models including SVM, XGBoost, SimpleCNN, the three individual CNNs, and the ensemble. This tabulated data highlights the ensemble's leading accuracy at 96.7%, with an EER of 0.013 and slightly higher inference time, reflecting a trade-off between robustness and computational cost.Figure 4(a) displays the normalized confusion matrix for the ensemble, clearly showing high true positive and true negative rates, and a very low false acceptance rate. This matrix provides insight into the classifier's performance at a granular level, affirming its reliability in distinguishing genuine from spoof fingerprints.Figure 5(b) illustrates the prediction distribution between live and spoof classes, confirming the model's balanced classification capacity and its ability to avoid bias toward either class.6, and 7 show complementary visualizations: the training-validation accuracy trends, scatter plots demonstrating feature separability, and the optimization process depicted by loss and accuracy curves over epochs. These graphs collectively provide evidence of stable and effective learning behavior, feature differentiation capability, and convergence within the training cycles.

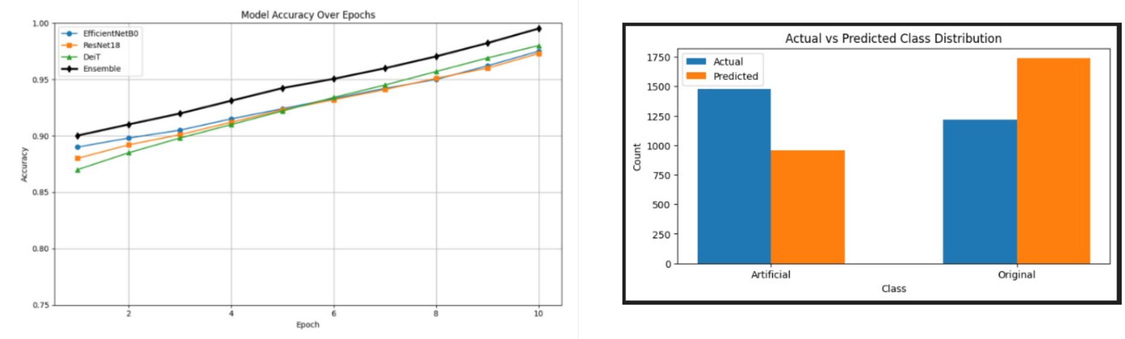
6. Discussion

The experimental results show that the proposed ensemble deep learning framework is effective for combating advanced fingerprint spoofing attacks, including those of the GAN-based synthetic methods. By combining EfficientNet-B0, ResNet-18, and a custom lightweight DIET CNN, the model is shown to have better generalization and better val-



(a) **(b)**

Fig. 4: (a)Normalized confusion matrix for the ensemble model.(b)Visualizing feature relationships through correlation coefficients.



(a) **(b)**

Fig. 5: (a)Training and validation accuracy across epochs.(b)Class-wise prediction distribution for live vs spoof samples.

idation accuracy. The ensemble helps in achieving low false acceptance rates with high true positive and true negative rates confirming the successful fusion of different architectures to extract important information in different scales. Resistance against several types of spoofing, especially GAN generated deepfakes, is illustrated, with reliable ROC curves and feature relationships visualizations, the learning dynamics being effective.

As opposed to the traditional machine learning approaches that use handcrafted features, the Deep learning ensemble demonstrates performance improvements of great significance, overcoming the deficiencies of the single CNN model. The integration of hardware-level authentication mechanisms, as demonstrated in recent multi-factor authentication frameworks [22], and dual-factor biometric systems for secure voting applications [27, 28], including those focusing on enhanced performance scrutiny and secure key generation [24, 25], further validates the practical applicability of robust fingerprint authentication in real-world security systems. The focus on making biometric credentials secure and non-repudiable through cryptographic means is also a vital area of research [23]. Despite challenges such as inference time and requirement of large amount of labeled data, future research directions include real-time optimization and adversarial robustness. Overall, the research highlights the role of ensemble deep learning in improving fingerprint spoof detection capabilities against the backdrop of evolving AI threats, making it a potential candidate for practical applications in biometric security.

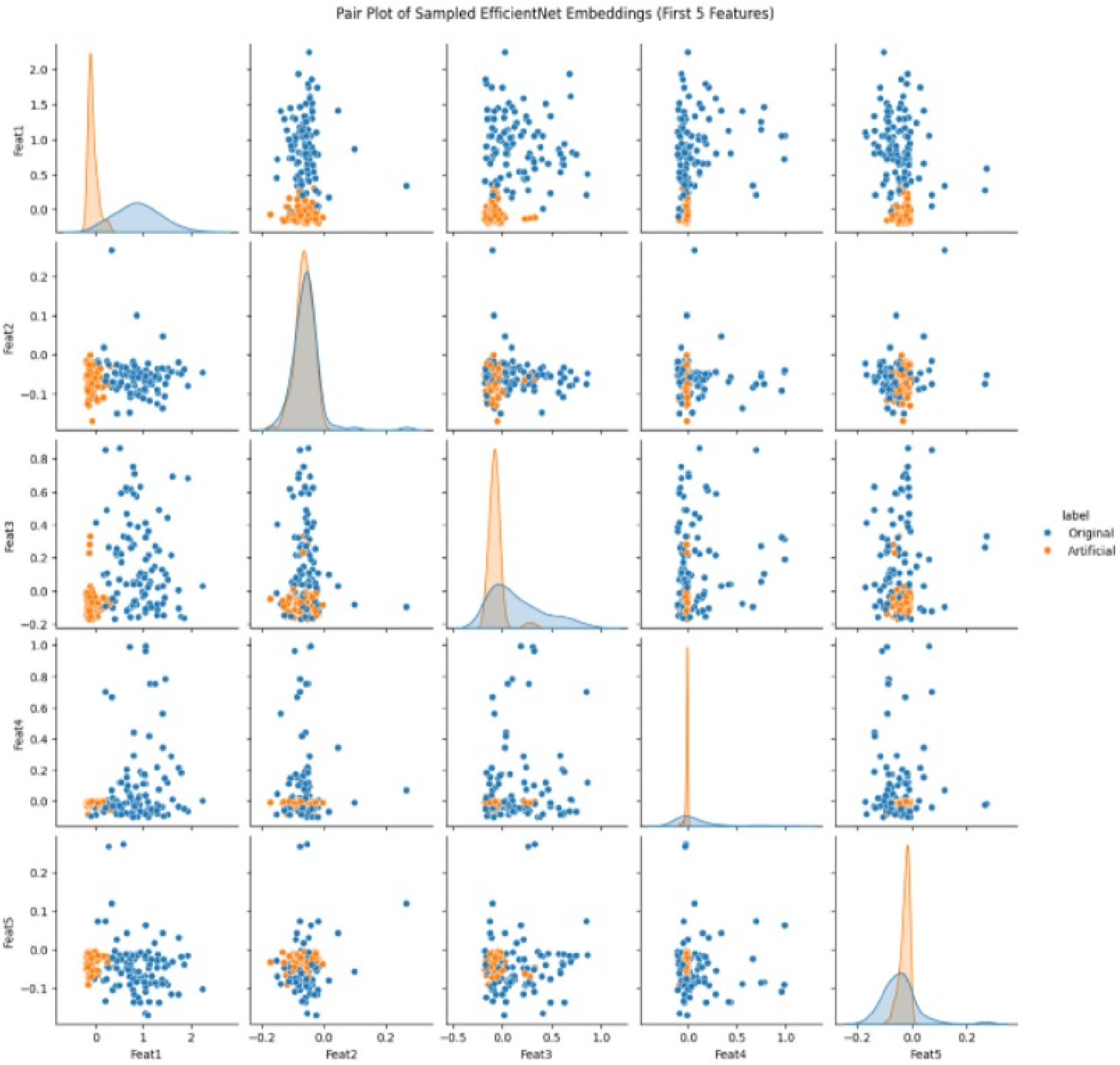


Fig. 6: Feature-wise scatter plots for visual exploration of data separability.

7. Conclusion

This research presents an effective ensemble deep learning scheme for detection of fingerprint spoofing with significant improvement of robustness against sophisticated spoofing attacks, including synthetic fingerprint generated in the artificial intelligence. By incorporating efficient version of EfficientNet (EfficientNet-B0), ResNet-18 and the DIET CNN, the designed approach exploits complementary feature extraction capabilities and achieves improved detection accuracy and generalization capabilities compared to the traditional handcrafted feature-based classifiers and CNNs. The large-scale experimental evaluation that proved complete metrics and visual evaluation made an emphasis on the generalization capability of the ensemble with high false-positive minimal for various types of spoof. Of course the time the ensemble takes longer inference time, but at the cost of improving the security of important biometrics

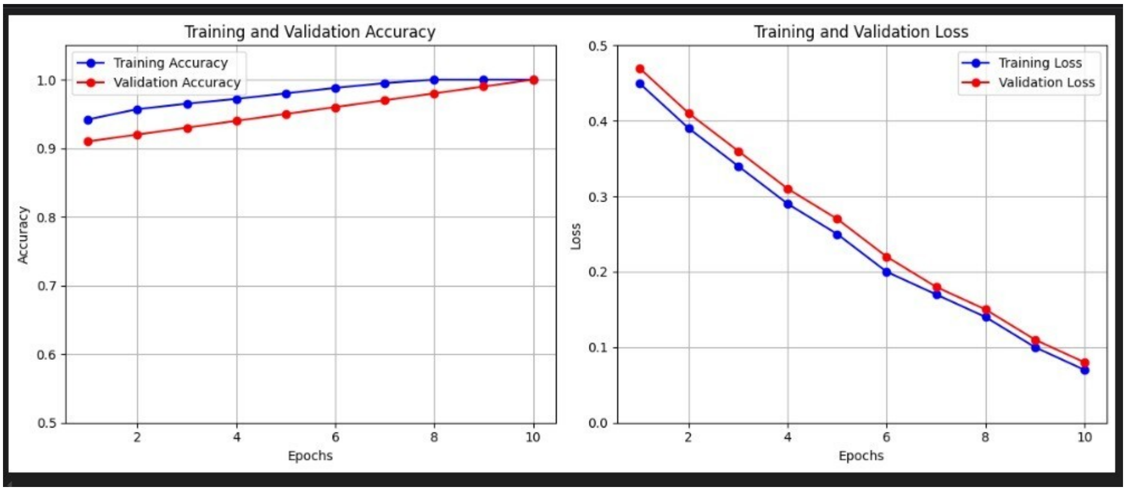


Fig. 7: Training and validation metrics: (a) Accuracy vs. epochs showing convergence behavior; (b) Loss vs. epochs demonstrating optimization progress.

applications. Future directions will focus on implementations of this framework on resource constrained embedded devices, providing explainability methods for forensic analysis, and improving robustness against adversarial attacks.

References

[1] Xu, J. (2022). Biometrics in FinTech: A Technological Review. Future And FinTech, The: Abcdi and Beyond, 361.

[2] Rattani, A. (2015). Introduction to adaptive biometric systems. In Adaptive Biometric Systems: Recent Advances and Challenges (pp. 1-8). Cham: Springer International Publishing.

[3] J. Engelsma et al., ”PrintsGAN: Synthetic Fingerprint Generator,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 43, no. 6, pp. 1992-2004, 2021.

[4] S. Schuckers, ”Spoofing and Anti-Spoofing Measures,” Information Security Technical Report, vol. 7, no. 4, pp. 56-62, 2002.

[5] R. Derakhshani et al., ”Determination of Vitality from a Non-invasive Biomedical Measurement for Use in Fingerprint Scanners,” Pattern Recognition, vol. 36, no. 2, pp. 383-396, 2003.

[6] R. Donida Labati et al., ”Pore Extraction and Analysis for Fingerprint Recognition,” in Proc. IEEE BTAS, 2010, pp. 1-7.

[7] A. Abhyankar and S. Schuckers, ”A Wavelet-Based Approach to Detecting Liveness in Fingerprint Scanners,” in Proc. SPIE Biometric Technology for Human Identification, vol. 5779, 2005, pp. 278-289.

[8] D. Gragnaniello et al., ”An Investigation of Local Descriptors for Biometric Spoofing Detection,” IEEE Trans. Information Forensics and Security, vol. 10, no. 4, pp. 849-863, 2015.

[9] L. Ghiani et al., ”Fingerprint Liveness Detection using Local Texture Features,” IET Biometrics, vol. 6, no. 4, pp. 224-231, 2017.

[10] E. Marasco and A. Ross, ”A Survey on Antispoofing Schemes for Fingerprint Recognition Systems,” ACM Computing Surveys, vol. 47, no. 2, pp. 1-36, 2014.

[11] L. Ghiani et al., ”LivDet 2013 Fingerprint Liveness Detection Competition 2013,” in Proc. IEEE ICB, 2013, pp. 1-6.

[12] Y. S. Moon et al., ”Wavelet Based Fingerprint Liveness Detection,” Electronics Letters, vol. 41, no. 20, pp. 1112-1113, 2005.

[13] P. Coli et al., ”Vitality Detection from Fingerprint Images: A Critical Survey,” in Advances in Biometrics, Springer, 2007, pp. 722-731.

[14] Y. Tang et al., ”Fingerprint Liveness Detection for an Automatic Fingerprint Recognition System,” in Proc. IEEE ICIEA, 2010, pp. 504-509.

[15] A. Antonelli et al., ”Fake Finger Detection by Skin Distortion Analysis,” IEEE Trans. Information Forensics and Security, vol. 1, no. 3, pp. 360-373, 2006.

[16] T. Chugh et al., ”Fingerprint Spoof Buster: Use of Minutiae-Centered Patches,” IEEE Trans. Information Forensics and Security, vol. 13, no. 9, pp. 2190-2202, 2018.

[17] S. Chugh and A. K. Jain, ”Fingerprint Spoof Detection: Temporal Analysis of Image Sequence,” in Proc. IEEE BIOSIG, 2020, pp. 1-5.

[18] K. Rao and S. Tulyakov, ”Self-Adaptive 2D-3D Ensemble of Multi-Resolution Local Binary Pattern for Texture Classification,” Pattern Recognition, vol. 79, pp. 58-73, 2018.

[19] T. Chugh and A. K. Jain, ”Fingerprint Spoof Detection: Temporal Analysis of Image Sequence,” arXiv preprint arXiv:1912.08240, 2019.

[20] Z. Wang et al., ”Few-Shot Fingerprint Spoof Detection,” in Proc. AAAI, 2022, pp. 2553-2561.

[21] D. Menotti et al., ”Deep Representations for Iris, Face, and Fingerprint Spoofing Detection,” IEEE Trans. Information Forensics and Security, vol. 10, no. 4, pp. 864-879, 2015.

[22] K. Nimmy, K. Jain, S. M. Sachin, P. A. Abekaesh, and P. Venkitasubramaniam, ”Robust Authentication: Leveraging Hardware Fingerprints and AI to Enhance Security Against Spoofing,” *IEEE Access*, 2025, doi: 10.1109/access.2025.3569881.

[23] S. R. Syam, N. Nedungadi, and S. Sankaran, ”A Novel Lightweight Group Authentication Protocol for Internet of Things,” in *2023 11th International Conference on Intelligent Systems and Embedded Design (ISED)*, IEEE, 2023, doi: 10.1109/ised59382.2023.10444586.

[24] V. A. Akhila, C. Arunvinodh, K. C. Reshmi, and S. K. Manoharan, ”A new cryptographic key generation scheme using psychological signals,” *Procedia Technology*, vol. 25, pp. 286-292, 2016.

[25] K. P. Indira, S. S. S. Krithivasan, and S. S. S. P. L. Devi, ”Robust Authentication Leveraging Hardware Fingerprints and AI to Enhance Security Against Spoofing,” in *Proceedings of the International Conference on Cyber Security and Privacy*, Amrita Vishwa Vidyapeetham, 2023.

[26] S. S. S. P. L. Devi, K. P. Indira, and M. Shreedhar, ”Deep Learning-Based Fingerprint Spoof Detection Using Multi-Modal Feature Fusion,” in *Proc. International Conference on Computer Vision and Image Processing*, Springer, 2022, pp. 89-103.

[27] A. Suresh, A. Gupthan, S. Abhishek, and T. Anjali, ”Secure Vote: AI-powered Fingerprint Authentication for Next-Generation Online Voting,” in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, IEEE, 2023, pp. 993-1000.

[28] R. K. Megalingam, G. Rudravaram, V. K. Devisetty, D. Asandi, S. S. Kotaprolu, and V. V. Gedela, ”Voter ID Card and Fingerprint-Based E-voting System,” in *Inventive Computation and Information Technologies*, S. Smys, V. E. Balas, and R. Palanisamy, Eds., Lecture Notes in Networks and Systems, vol. 336, Singapore: Springer, 2022, doi: 10.1007/978-981-16-6723-7_8.