IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131243

AI-Generated Fingerprint Image Detection using Machine Learning

Nandan D S[1], Venkatesh Gowda K R[2], Narasimhareddy A S[3], Chirag R[4], Prashant P Patavardhan[5]

Department of Electronics and Communication Engineering, RV Institute of Technology and Management, Bengaluru, India[1,2,3,4,5]

Abstract: Fingerprint-based biometric systems are vulnerable to attacks involving altered or forged fingerprints. This paper introduces a robust machine learning model for detecting altered fingerprints, utilizing the SOCOfing dataset containing 6,000 real and 49,270 altered fingerprint images. The model employs a convolutional neural network (CNN) to extract critical features such as ridge patterns, minutiae points, and texture details, achieving high accuracy and reliability. Our results demonstrate significant improvements in biometric security, paving the way for advanced applications in forensics and authentication systems. The findings also highlight the importance of AI-based security solutions and propose methods to scale the model for real-world applications. Future studies can focus on optimizing CNN architectures and integrating hybrid models for increased robustness.

Keywords: Altered Fingerprints, Machine Learning, SOCOfing Dataset, Convolutional Neural Networks, Biometric Security

I. INTRODUCTION

Fingerprint recognition is a cornerstone of modern biometric systems due to its uniqueness and reliability. However, the integrity of such systems is compromised by altered fingerprints, which are intentionally modified to evade identification. Traditional methods for detecting altered fingerprints rely heavily on manual inspection, which is both time-consuming and error-prone. Advances in AI and machine learning have paved the way for automated detection methods, offering higher accuracy and efficiency. This research presents a machine learning approach to address this issue, focusing on the SOCOfing dataset, which includes real and altered fingerprints categorized into easy, medium, and hard levels.

The study also investigates the impact of AI advancements in biometric systems, discussing their role in forensic investigations and identity verification. Automated methods reduce human error and improve scalability, making them ideal for high-security applications. This paper highlights the challenges in distinguishing altered fingerprints and proposes a CNN-based framework that can be integrated into modern biometric systems.

II. LITERATURE SURVEY

Biometric systems, especially fingerprint recognition, play a critical role in modern security protocols for identity verification in applications such as law enforcement, border control, and banking. However, the detection of altered fingerprints poses a significant challenge, as modifications are often made to evade biometric systems. These alterations include obliteration, distortion, and imitation, necessitating advanced algorithms capable of handling complex biometric data. Machine learning, particularly deep learning, has emerged as a promising approach to tackle this issue.

AI-Generated Image Detection and Its Relevance to Fingerprint Alteration

Artificial intelligence (AI) advancements have introduced challenges in detecting synthetic images generated by models like Generative Adversarial Networks (GANs). Saskoro et al. (2024) proposed a Gated Expert Convolutional Neural Network (CNN) using transfer learning for AI-generated image detection, effectively identifying content from GAN and diffusion platforms while overcoming catastrophic forgetting [1]. Park et al. (2024) further emphasized artifact-based methods for GAN images and encoder-based methods for diffusion models, highlighting the need for tailored detection strategies [2]. These findings are relevant to fingerprint alteration detection, as altered prints may exhibit similar artifacts.

DOI: 10.17148/IJARCCE.2024.131243

Dynamic aggregation and compression techniques, such as those leveraging Wasserstein distance, have improved detection performance on imbalanced datasets, ensuring accuracy and efficiency [3]. Datasets like CIFAKE, employing Latent Diffusion Models (LDMs) and CNN classifiers, achieve high accuracy in distinguishing real and synthetic images, supported by Explainable AI (XAI) techniques for transparency [4][5]. These approaches are directly applicable to detecting subtle imperfections in altered fingerprints.

Fingerprint Recognition and Liveness Detection

Deep learning advancements in fingerprint recognition and liveness detection have significantly improved accuracy and robustness. CNN-based models, using architectures like AlexNet and VGG, have achieved 95.5% classification accuracy on LivDet datasets, demonstrating their effectiveness against spoofed fingerprints [12]. Data augmentation techniques further enhance generalization across datasets.

Synthetic fingerprint data generation, such as PrintsGAN, addresses dataset limitations by producing realistic synthetic fingerprints, improving training diversity and accuracy [11]. Fixed-length fingerprint representations, like the DeepPrint model, integrate alignment and minutiae features, achieving performance comparable to commercial systems for large-scale applications [13]. High-resolution fingerprint recognition using CNNs with affine Fourier moment-matching (AFMM) techniques has further boosted matching accuracy by incorporating level 3 features such as pores [14].

Altered Fingerprints and Detection Techniques

Detecting altered fingerprints remains a crucial challenge due to deliberate modifications, such as obliteration and distortion. Algorithms analyzing orientation fields and minutiae distributions effectively address vulnerabilities in Automated Fingerprint Identification Systems (AFIS) [17]. GAN-based models enhance latent fingerprint quality, improving minutiae extraction and matching accuracy, particularly in forensic applications [15].

Synthetic biometric data generation using neural generative models has enabled realistic fingerprint samples, facilitating privacy preservation, training augmentation, and evaluation of recognition models [16]. Altered fingerprints are categorized into obliteration, distortion, and imitation, requiring tailored algorithms for detection. Orientation field analysis and minutiae distribution methods address these vulnerabilities effectively [17].

Advanced methods, such as Conditional GANs (cGANs) for latent fingerprint reconstruction, preserve identity while improving matching accuracy for incomplete fingerprints [18]. Biometric methods leveraging GANs, such as dorsal hand vein identification, enhance robustness in high-security applications [19].

This survey highlights the advancements in AI-driven image detection and fingerprint recognition, emphasizing the importance of addressing altered fingerprints. It identifies gaps in existing research and sets the foundation for developing more robust algorithms to detect fingerprint alterations.

III. MATERIALS AND METHODS

A. Problem Statement

Biometric systems are increasingly at risk due to sophisticated alteration techniques. This paper aims to enhance the reliability of fingerprint-based systems by developing a robust model to detect altered fingerprints, thereby addressing a critical vulnerability in biometric security.

B. Objectives

- Develop a CNN-based model to classify real and altered fingerprints.
- Leverage the SOCOfing dataset for training and validation.
- Evaluate the model's performance using metrics such as accuracy, precision, recall, and F1-score.
- Visualize feature extraction to understand the model's decision-making process.

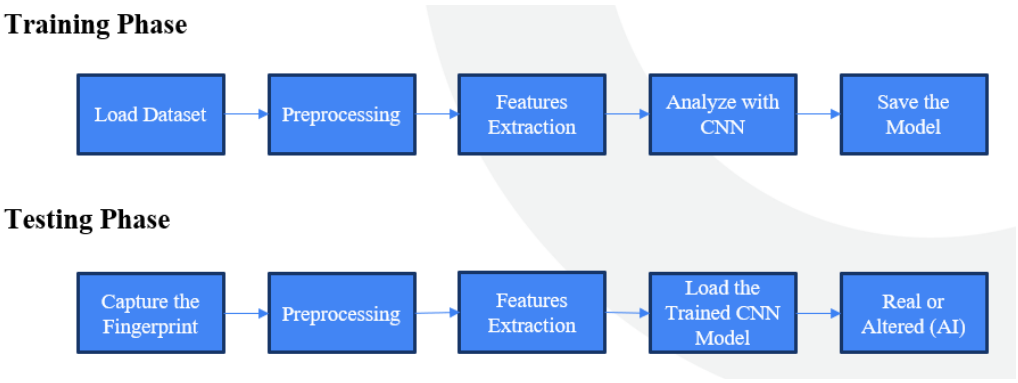
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131243

C. Methodology



1. Training Phase:

- Load Dataset: Collect the SOCOfing dataset for training and testing.
- Preprocessing: Normalize fingerprint images and apply data augmentation to enhance generalization.
- Feature Extraction: Use CNN layers to extract ridge patterns, minutiae points, and texture features.
- Analyze with CNN: Train the model on extracted features.
- Save the Model: Store the trained model for testing and validation.

2. Testing Phase:

- Capture the Fingerprint: Obtain new fingerprint samples for evaluation.
- Preprocessing: Apply normalization and resizing to match training data.
- Feature Extraction: Extract relevant fingerprint features using the trained CNN.
- Load the Trained CNN Model: Use the pre-trained model to classify fingerprints.
- Real or Altered: Determine whether the fingerprint is real or altered based on predictions.

D. CNN Architecture

The CNN model comprises multiple convolutional and pooling layers followed by fully connected layers. Key parameters include:

Model: "sequential"

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 126, 126, 32)	896
max_pooling2d (MaxPooling2D)	(None, 63, 63, 32)	0
conv2d_1 (Conv2D)	(None, 61, 61, 64)	18,496
max_pooling2d_1 (MaxPooling2D)	(None, 30, 30, 64)	0
conv2d_2 (Conv2D)	(None, 28, 28, 128)	73,856
max_pooling2d_2 (MaxPooling2D)	(None, 14, 14, 128)	0
conv2d_3 (Conv2D)	(None, 12, 12, 256)	295,168
max_pooling2d_3 (MaxPooling2D)	(None, 6, 6, 256)	0
flatten (Flatten)	(None, 9216)	0
dense (Dense)	(None, 256)	2,359,552
dropout (Dropout)	(None, 256)	0
dense_1 (Dense)	(None, 128)	32,896
dense_2 (Dense)	(None, 1)	129

Total params: 2,780,993 (10.61 MB)
Trainable params: 2,780,993 (10.61 MB)
Non-trainable params: 0 (0.00 B)

- Ridge Patterns and Orientations: Identifies global patterns such as loops, whorls, and arches, along with ridge flow direction.
- Minutiae Points: Captures ridge endings, bifurcations, and other unique minutiae features critical for distinguishing fingerprints.
- Texture Features: Extracts fine-grained textures, including ridge thickness, spacing, and continuity.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024
DOI: 10.17148/IJARCCE.2024.131243

- Singular Points: Detects key points like cores and deltas, used for fingerprint alignment and classification.
- Geometric Relationships: Analyzes spatial relationships between minutiae and ridge patterns for enhanced uniqueness.

E. Tools Used

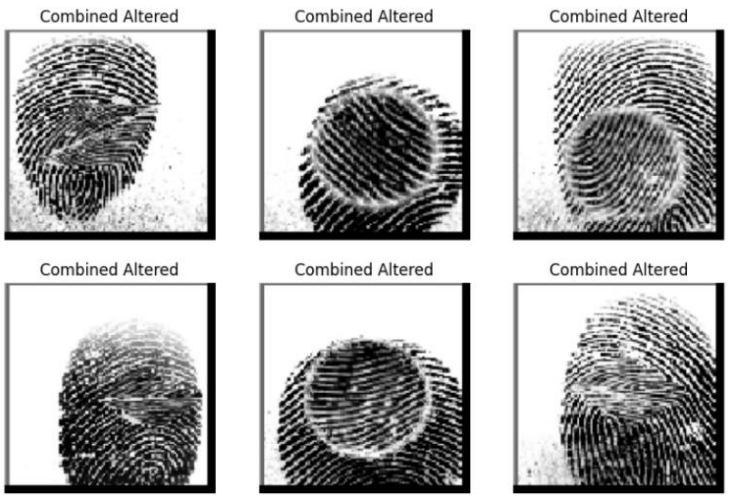
- SOCOfing Dataset: Used to train the model for detection of Altered and AI generated fingerprint, resulting in a trained model file.
- AI Tools (ChatGPT & Gemini): Generated synthetic fingerprint images and assisted in refining the implementation.
- Own Dataset: Created using inked fingerprints on paper for real-world model validation.
- Kaggle Environment: Employed for training, testing, and optimizing the model in a cloud-based platform.
- Libraries: TensorFlow, Keras, OpenCV, NumPy, and Matplotlib for preprocessing, training, and visualization.

IV. RESULTS

A. Sample Images from Dataset

Real Fingerprints Sample

Altered Fingerprints Sample



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131243

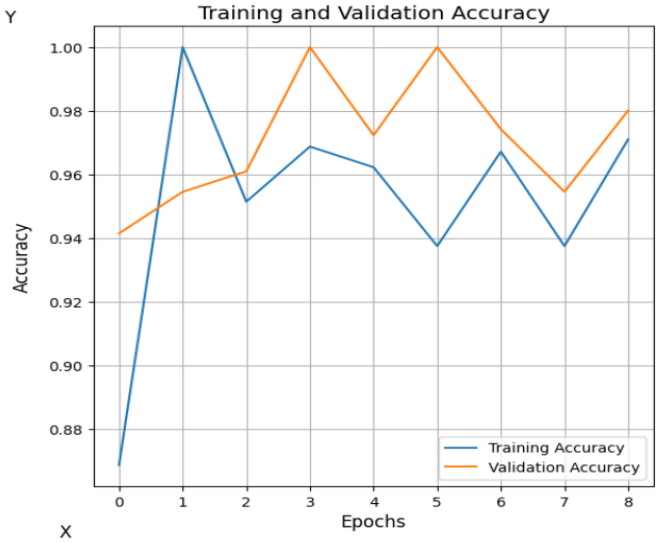
B. Quantitative Results

SI NO.	PARAMETERS	OUTCOMES
1.	Precision	92.92%
2.	Recall	92.66%
3.	F1 Score	92.65%
4.	Accuracy	97.09%

- Precision of 92.92%, indicating a high rate of correctly identified altered fingerprints.
- Recall of 92.66% demonstrates the model's ability to capture most of the altered fingerprints in the dataset.
- F1 score, balancing precision and recall, is 92.65%, reflecting strong overall performance.
- Accuracy of 97.09% highlights its effectiveness in correctly classifying fingerprints as real or altered.

C. Graphical Results

- Training vs Validation Accuracy



- Training vs Validation Loss

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024
DOI: 10.17148/IJARCCE.2024.131243

- The accuracy graph shows that both training and validation accuracy converge around 96-98%, indicating effective learning with minor fluctuations.
- The loss graph demonstrates a significant decrease in both training and validation loss, confirming reduced error and good model performance.

V. CONCLUSION AND FUTURE SCOPE

This project demonstrates the use of Convolutional Neural Networks (CNNs) for fingerprint classification, a critical application in biometric security systems. By employing various python libraries, a Deep Learning model was developed and trained to classify fingerprint images accurately. The CNN model achieved satisfactory results with the processed dataset, highlighting the power of deep learning in biometric recognition tasks. Key stages of the project included image preprocessing, model design, training, and evaluation, which all contributed to the model's overall performance.

Future improvements can focus on utilizing more advanced models to achieve even higher accuracy. Expanding the approach to integrate real-time fingerprint scanners for practical use is another potential enhancement. Additionally, combining fingerprint recognition with other biometric systems, such as facial recognition, could further bolster security and reliability. These updates will make the system more adaptable, efficient, and capable of addressing evolving threats in biometric security.

REFERENCES

[1]. R. Ahmad Fattah Saskoro, N. Yudistira and T. Noor Fatyanosa, "Detection of AI Generated Images From Various Generators Using Gated Expert Convolutional Neural Network," in IEEE Access, vol. 12, pp. 147772-147783, 2024, doi: 10.1109/ACCESS.2024.3466614.
[2]. D. Park, H. Na and D. Choi, "Performance Comparison and Visualization of AI Generated-Image Detection Methods," in IEEE Access, vol. 12, pp. 62609-62627, 2024, doi: 10.1109/ACCESS.2024.3394250.
[3]. Z. Lyu, J. Xiao, C. Zhang and K. -M. Lam, "AI-Generated Image Detection With Wasserstein Distance Compression and Dynamic Aggregation," 2024 IEEE International Conference on Image Processing (ICIP), Abu Dhabi, United Arab Emirates, 2024, pp. 3827-3833, doi: 10.1109/ICIP51287.2024.10648186.
[4]. J. J. Bird and A. Lotfi, "CIFAKE: Image Classification and Explainable Identification of AI Generated Synthetic Images," in IEEE Access, vol. 12, pp. 15642-15650, 2024, doi: 10.1109/ACCESS.2024.3356122.
[5]. Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861.
[6]. A. R. Widya, Y. Monno, M. Okutomi, S. Suzuki, T. Gotoda and K. Miki, "Stomach 3D Reconstruction Based on Virtual Chromoendoscopic Image Generation," 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Montreal, QC, Canada, 2020, pp. 1848-1852, doi: 10.1109/EMBC44109.2020.9176016.
[7]. R. Girshick, J. Donahue, T. Darrell and J. Malik, "Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation," 2014 IEEE Conference on Computer Vision and Pattern Recognition, Columbus, OH, USA, 2014, pp. 580-587, doi: 10.1109/CVPR.2014.81.
[8]. R. Zemouri et al., "Recent Research and Applications in Variational Autoencoders for Industrial Prognosis and Health Management: A Survey," 2022 Prognostics and Health Management Conference (PHM-2022 London), London, United Kingdom, 2022, pp. 193 203, doi: 10.1109/PHM2022-London52454.2022.00042.
[9]. N. Bonettini, P. Bestagini, S. Milani and S. Tubaro, "On the use of Benford's law to detect GAN-generated images," 2020 25th International Conference on Pattern Recognition (ICPR), Milan, Italy, 2021, pp. 5495-5502, doi: 10.1109/ICPR48806.2021.9412944.
[10]. J. J. Engelsma, S. Grosz and A. K. Jain, "PrintsGAN: Synthetic Fingerprint Generator," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 5, pp. 6111 6124, 1 May 2023, doi: 10.1109/TPAMI.2022.3204591.
[11]. R. F. Nogueira, R. de Alencar Lotufo and R. Campos Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1206-1213, June 2016, doi: 10.1109/TIFS.2016.2520880.
[12]. J. J. Engelsma, K. Cao and A. K. Jain, "Learning a Fixed-Length Fingerprint Representation," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 43, no. 6, pp. 1981-1997, 1 June 2021, doi: 10.1109/TPAMI.2019.2961349.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 12, December 2024

DOI: 10.17148/IJARCCE.2024.131243

[13]. H. -R. Su, K. -Y. Chen, W. J. Wong and S. -H. Lai, "A deep learning approach towards pore extraction for high-resolution fingerprint recognition," 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 2017, pp. 2057-2061, doi: 10.1109/ICASSP.2017.7952518.

[14]. I. Joshi, A. Anand, M. Vatsa, R. Singh, S. D. Roy and P. Kalra, "Latent Fingerprint Enhancement Using Generative Adversarial Networks," 2019 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 2019, pp. 895-903, doi: 10.1109/WACV.2019.00100.

[15]. A. Makrushin, A. Uhl and J. Dittmann, "A Survey on Synthetic Biometrics: Fingerprint, Face, Iris and Vascular Patterns," in IEEE Access, vol. 11, pp. 33887-33899, 2023, doi: 10.1109/ACCESS.2023.3250852.

[16]. S. Yoon, J. Feng and A. K. Jain, "Altered Fingerprints: Analysis and Detection," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451-464, March 2012, doi: 10.1109/TPAMI.2011.161.

[17]. A. Dabouei, S. soleymani, H. Kazemi, S. M. Iranmanesh, J. Dawson and N. M. Nasrabadi, "ID Preserving Generative Adversarial Network for Partial Latent Fingerprint Reconstruction," 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 2018, pp. 1-10, doi: 10.1109/BTAS.2018.8698580.

[18]. K. M. Alashik and R. Yildirim, "Human Identity Verification From Biometric Dorsal Hand Vein Images Using the DL-GAN Method," in IEEE Access, vol. 9, pp. 74194-74208, 2021, doi: 10.1109/ACCESS.2021.3076756.

[19]. C. Yuan, Z. Xia, L. Jiang, Y. Cao, Q. M. Jonathan Wu and X. Sun, "Fingerprint Liveness Detection Using an Improved CNN With Image Scale Equalization," in IEEE Access, vol. 7, pp. 26953-26966, 2019, doi: 10.1109/ACCESS.2019.2901235.

