# ABSTRACT

The reliability of biometric systems, particularly those utilizing fingerprints, is increasingly jeopardized by the prevalence of altered fingerprints. Altered fingerprints are deliberately modified to evade detection by biometric or forensic systems, posing a serious challenge to the integrity of security protocols. This issue is particularly critical in sensitive applications such as border control, law enforcement, and identity verification, where the failure to detect altered fingerprints can result in severe consequences. Addressing this challenge demands advanced technological solutions capable of accurately identifying fingerprint alterations and enhancing the robustness of biometric systems.

This study explores the application of machine learning to detect altered fingerprints, leveraging the SOCOfing dataset. The dataset includes 6,000 real fingerprint images and 49,270 altered fingerprints categorized into easy, medium, and hard difficulty levels. The images, available in BMP format, provide a diverse and challenging dataset for model training and evaluation. A convolutional neural network (CNN) was designed to classify fingerprints as real or altered, utilizing preprocessing techniques to standardize input images and ensure consistency in model training. Additionally, feature map visualizations were implemented to provide insights into the patterns and regions influencing the model's decisions, enhancing interpretability and transparency. The absence of a dedicated test image path in the SOCOfing dataset posed a unique challenge. To address this, inked fingerprints on blank paper were used for validation, offering a practical approach to testing the model's performance in real-world scenarios. This innovative strategy ensured a comprehensive evaluation of the model's robustness and generalization capabilities.

This study achieved a precision of 94.40%, indicating a high rate of correctly identified altered fingerprints. The recall of 90.35% demonstrates the model's ability to capture most of the altered fingerprints in the dataset. The F1 score, balancing precision and recall, is 92.17%, reflecting strong overall performance. The model's accuracy of 97.92% highlights its effectiveness in correctly classifying fingerprints as real or altered. While these metrics may vary slightly across training iterations, they emphasize the potential of machine learning to revolutionize fingerprint alteration detection, providing a robust and efficient solution to address this critical issue.

# Table of Contents

# LIST OF TABLES

# LIST OF FIGURES

# ABBREVIATION

CNN: Convolutional Neural Network

SOCOfing: Sokoto Coventry Fingerprint Dataset

DFD: Data Flow Diagram

GAN: Generative Adversarial Network

ML: Machine Learning

CIFAKE: Real and AI-Generated Synthetic Images

LDM: Latent Diffusion Model

VGG: Visual Geometry Group

# CHAPTER 1

## Introduction

Biometric systems, especially those utilizing fingerprint recognition, play a pivotal role in modern security and identity verification processes. However, the increasing prevalence of altered fingerprints poses a significant threat to the reliability and effectiveness of these systems. Altered fingerprints are intentionally modified to bypass biometric or forensic detection, presenting challenges in critical areas such as border control, law enforcement, and access control. The ability to accurately detect altered fingerprints is vital, as failure to do so can lead to severe security breaches, identity fraud, and legal consequences.

With the growing sophistication of fingerprint alteration techniques, traditional methods of fingerprint analysis are becoming less reliable. This calls for the integration of advanced technological solutions that can effectively identify alterations, ensuring that biometric systems maintain their integrity. Machine learning (ML), particularly deep learning techniques, has shown great promise in addressing such challenges. By analyzing large datasets of fingerprint images, ML models can be trained to recognize even the most subtle modifications, improving the detection of altered fingerprints.

This project focuses on the application of convolutional neural networks (CNNs) to detect altered fingerprints, leveraging the SOCOfing dataset. The dataset comprises 6,000 real fingerprint images and 49,270 altered images categorized into easy, medium, and hard difficulty levels. The use of this diverse dataset provides a challenging environment for training and testing the model's robustness. The aim of this research is to enhance the accuracy of fingerprint alteration detection by utilizing ML techniques, ultimately contributing to more secure biometric systems.

By evaluating the performance of the CNN model in identifying real and altered fingerprints, this study explores how machine learning can revolutionize the field of fingerprint recognition, addressing the challenges posed by altered fingerprints and improving the reliability of biometric authentication systems.

### 1.1 Problem Statement

Fingerprint-based biometric systems are integral to modern security infrastructure, used widely in applications such as border control, law enforcement, and identity verification. However, the rise in the use of altered fingerprints—fingerprints intentionally modified to bypass biometric authentication systems—presents a critical challenge to the reliability and effectiveness of these systems. The inability of traditional fingerprint matching methods to reliably detect such alterations undermines the security and integrity of these systems, creating vulnerabilities in sensitive environments.

This project seeks to address this challenge by developing a machine learning-based system designed to detect altered fingerprints with high accuracy. Utilizing advanced deep learning techniques, specifically Convolutional Neural Networks (CNNs), the system will be trained on the SOCOfing dataset, which includes a diverse range of real and altered fingerprint images. This approach aims to enhance the ability of biometric systems to distinguish between genuine and altered fingerprints, thereby improving the robustness of security protocols. By automating the detection process, this system promises a more efficient, scalable, and accurate solution that can significantly reduce the risks posed by fingerprint alteration in biometric authentication applications.

### 1.2 Motivation

The rise of AI-generated images, often indistinguishable from real ones, has created challenges in verifying authenticity, combating misinformation, and ensuring ethical use. Machine learning-based detection of such images is crucial for safeguarding trust in digital media. It aids in identifying fake content, protecting intellectual property, and preventing the misuse of generative AI for malicious purposes like deepfakes. ML models, with their ability to analyse subtle patterns invisible to the human eye, offer a scalable, automated approach to detect manipulated or AI-generated images, promoting transparency and accountability in an increasingly AI-driven visual landscape.

## 1.3 OBJECTIVES

• Build a machine learning model using Convolutional Neural Networks (CNNs) to classify fingerprints as real or altered, enhancing the reliability of biometric security systems.

• Achieve high detection performance by optimizing key metrics such as precision, recall, F1-score, and accuracy to ensure consistent and reliable identification of altered fingerprints.

• Utilize the SOCOfing dataset, which includes a mix of real and altered fingerprint images across various difficulty levels (easy, medium, hard), to train the model and improve its robustness.

• Implement interpretability features, such as feature map visualizations, to provide transparency and clarity in model predictions, aiding forensic experts in understanding the model's decision-making process.

• Validate the model's performance with real-world data, such as inked fingerprints on blank paper, ensuring the model's effectiveness in practical applications like border control and law enforcement.

# CHAPTER 2

## Literature Survey

Biometric systems, particularly fingerprint recognition, are integral to modern security protocols, serving as critical tools for identity verification in various applications, such as law enforcement, border control, and banking. As the reliability of these systems becomes increasingly vital, the detection of altered fingerprints has emerged as a major challenge. Altered fingerprints are modified intentionally to evade biometric systems, often to gain unauthorized access. These modifications can range from obliteration, distortion, and imitation to sophisticated alterations that mimic real fingerprint patterns. Detecting these altered fingerprints requires advanced algorithms capable of handling the variability and complexity of biometric data, making machine learning a promising solution in addressing this growing problem.

Recent studies on biometric recognition have highlighted the significant role of machine learning in enhancing the detection capabilities of altered fingerprints. Deep learning, in particular, has shown tremendous potential in image recognition tasks, including biometric and forensic applications. This literature survey explores the latest advancements in AI-generated image detection and biometric fingerprint recognition, focusing on the methods and models developed to detect altered fingerprints. It discusses key studies that have shaped the field and identifies gaps in existing research that the current project aims to address.

### AI-Generated Image Detection and Its Relevance to Fingerprint Alteration

The rapid evolution of artificial intelligence (AI) and the growing sophistication of AI-generated images have introduced new challenges for both researchers and practitioners in various fields. The ability to distinguish between real and synthetic images, particularly those created by Generative Adversarial Networks (GANs) and other machine learning models, has become a critical issue, especially in fields like forensics and security. Saskoro et al. (2024) proposed a Gated Expert Convolutional Neural Network (CNN) model that utilizes transfer learning to address the detection of AI-generated images. This approach is particularly effective in detecting content from a

wide range of AI image generators, including GAN and stable diffusion platforms. By reducing the need for frequent tuning and overcoming the problem of catastrophic forgetting, the model outperforms traditional CNN models in detecting altered or synthetic images across different platforms [1].

Building on this foundation, Park et al. (2024) expanded their research by comparing the performance of various detection methods across different types of AI-generated content, including those from GAN, diffusion, and transformer models. They found that artifact-based methods, which rely on detecting inconsistencies or imperfections in the image, were more effective for GAN-generated images. In contrast, image-encoder-based methods performed better with diffusion and transformer-generated images, emphasizing the importance of tailoring detection strategies to the specific characteristics of different AI-generated content [2]. This research is highly relevant to the detection of altered fingerprints, as these altered prints can exhibit similar types of inconsistencies, such as minute distortions or artifacts, which are critical for distinguishing real from fake fingerprints.

Another noteworthy contribution to AI-generated image detection is the use of dynamic aggregation and information compression techniques. One study introduced a novel method that improves detection performance by utilizing the Wasserstein distance to aggregate and compress information. This method, which is particularly useful when working with imbalanced datasets, has demonstrated improvements in both accuracy and training efficiency. By compressing training data while preserving feature quality, this approach facilitates better detection of synthetic images, making it an effective tool for improving models designed to detect altered fingerprints [3].

Additionally, the use of synthetic datasets, such as CIFAKE, has proven beneficial for training models that classify real and AI-generated images. The CIFAKE dataset employs Latent Diffusion Models (LDMs) for image classification and uses a CNN for binary classification, achieving high accuracy rates in distinguishing between real and synthetic images. Moreover, the inclusion of Explainable AI (XAI) techniques provides insights into the model's decision-making process, making it easier for researchers and practitioners to understand how subtle imperfections, rather than overt content features, contribute to the detection of AI-generated images [4][5]. These advancements in

synthetic data generation and classification are directly applicable to the detection of altered fingerprints, which may share similar challenges in terms of subtle imperfections that need to be detected.

**Fingerprint Recognition and Liveness Detection**

The role of deep learning in biometric systems, particularly for fingerprint recognition and liveness detection, has undergone significant advancements over the past decade. In the field of fingerprint recognition, convolutional neural networks (CNNs) have demonstrated exceptional capabilities in distinguishing between real and spoofed fingerprints, making them highly valuable in detecting altered or synthetic prints. One notable study in this area is the use of CNNs for fingerprint liveness detection, which utilizes pre-trained models such as AlexNet and VGG. This approach has achieved state-of-the-art performance on datasets like LivDet 2013, with a classification accuracy of 95.5%, demonstrating its robustness in distinguishing between real and spoofed fingerprints [12]. The incorporation of data augmentation techniques further enhances the model's robustness by generating varied training samples that improve its ability to generalize across different fingerprint datasets.

In addition to fingerprint liveness detection, advancements have been made in generating synthetic fingerprint data to augment training datasets. One such approach, PrintsGAN, employs GANs to generate realistic synthetic fingerprints, addressing the challenge of limited fingerprint datasets for training deep networks. This model generates multiple impressions per finger, ensuring that the synthetic fingerprints closely resemble real ones. This is especially useful for training deep learning models that require large amounts of diverse data to achieve high accuracy in recognition tasks. PrintsGAN's ability to generate realistic fingerprint images is crucial for developing more accurate and efficient fingerprint recognition systems, particularly in the context of detecting altered prints [11].

The deep learning approach to fingerprint recognition has been further enhanced by the development of fixed-length fingerprint representations. The DeepPrint model, for instance, generates a 200-byte fixed-length representation that incorporates both alignment and minutiae feature of the fingerprint. This approach not only reduces

search time during the matching process but also achieves accuracy levels comparable to commercial fingerprint recognition systems, making it ideal for large-scale applications such as national ID programs and border security systems [13]. Additionally, deep learning models have been used to explore level 3 fingerprint features, such as pores, which are crucial for high-resolution fingerprint recognition. A novel CNN architecture that incorporates affine Fourier moment-matching (AFMM) techniques has shown improvements in matching accuracy, particularly for high-resolution fingerprint datasets [14].

**Altered Fingerprints and Detection Techniques**

As the capabilities of machine learning models in fingerprint recognition and spoof detection improve, it is crucial to address the specific challenge of detecting altered fingerprints. Altered fingerprints, unlike spoofed ones, may involve deliberate modifications such as obliteration or distortion, which can complicate the matching process. One study on fingerprint alteration detection proposed an algorithm that analyzes orientation fields and minutiae distributions to identify altered prints. This method is particularly effective in addressing vulnerabilities in automated fingerprint identification systems (AFIS), where traditional detection methods may fail to recognize intentionally altered patterns [17].

Another significant advancement in altered fingerprint detection involves the use of Generative Adversarial Networks (GANs) to enhance the quality of latent fingerprints, which are often of poor quality due to factors such as environmental conditions or the nature of the crime scene. A GAN-based model for latent fingerprint enhancement was shown to improve the ridge structure and overall quality of fingerprint images, making minutiae extraction more accurate. This study demonstrated the flexibility of GANs in forensic applications, where high-quality fingerprint matching is essential for criminal investigations [15].

The importance of synthetic biometric data generation has also been emphasized in recent research. The creation of synthetic biometric datasets, such as those generated using GANs, is essential for addressing privacy concerns, augmenting training data, and evaluating fingerprint recognition models in a cost-effective manner. A survey on

synthetic biometrics explored the role of neural generative models in producing realistic biometric samples for fingerprint, face, iris, and vascular pattern recognition. This research highlights the transition from traditional mathematical modeling to modern neural networks, which has enabled the generation of high-quality synthetic fingerprints for use in training and evaluating fingerprint recognition systems [16].

Fingerprint alteration poses a unique challenge to biometric systems, particularly in security applications. Altered Fingerprints: Analysis and Detection categorizes alterations into obliteration, distortion, and imitation. The proposed algorithm in this study analyzes orientation fields and minutiae distributions to detect altered fingerprints, addressing vulnerabilities in automated fingerprint identification systems (AFIS) and emphasizing the need for new detection techniques [17].

Advanced methods for biometric recognition continue to evolve, particularly with the use of GANs and CNNs. ID Preserving Generative Adversarial Network for Partial Latent Fingerprint Reconstruction presents a cGAN-based approach for reconstructing missing ridge information in latent fingerprints while maintaining identity preservation. This method has shown improved matching accuracy, particularly when dealing with distorted or incomplete fingerprints [18]. Another innovative approach, Human Identity Verification From Biometric Dorsal Hand Vein Images Using the DL-GAN Method, combines deep learning with GANs for vein-based identification. This method offers enhanced accuracy and robustness, particularly in high-security applications such as banking and airport security [19]. Finally, Fingerprint Liveness Detection Using an Improved CNN With Image Scale Equalization addresses fingerprint spoofing by using a CNN with image scale equalization. This method preserves texture information and avoids resolution degradation, leading to improved detection accuracy, as demonstrated by results on LivDet datasets [20].

# CHAPTER 3

## Theory and Concept Relevant to the Fingerprint Detection Project

### 3.1 Introduction

Fingerprint detection using machine learning is a critical application in biometrics, particularly in security and authentication systems. This project aims to distinguish between real and altered fingerprints using deep learning techniques, leveraging convolutional neural networks (CNNs) for image-based classification. The project employs principles of digital image processing, dataset preparation, data augmentation, and supervised learning.

### 3.2 Core Concepts and Technology

#### 1. Biometrics and Fingerprint Analysis

Biometric systems use unique physiological or behavioral traits to identify individuals. Fingerprints are an ideal biometric trait due to their **uniqueness** and **persistence over time**. However, altered fingerprints arise due to deliberate manipulation, which poses challenges in forensic and authentication scenarios.

#### 2. Image Processing

The preprocessing and enhancement of fingerprint images are essential steps to standardize the dataset. The following image processing concepts are applied:

- **Grayscale Conversion:** Reduces computational complexity by converting color images into single-channel intensity images.
- **Histogram Equalization:** Enhances contrast in grayscale images, improving feature visibility.
- **Resizing and Padding:** Standardizes images to a fixed size (128x128 pixels) for model input while maintaining aspect ratio.
- **Contrast Enhancement:** Adjusts intensity values to highlight fingerprint ridges and valleys.

**3. Deep Learning with Convolutional Neural Networks (CNNs)**

CNNs are ideal for image-based tasks due to their ability to automatically learn hierarchical features. The architecture implemented includes:

- **Convolutional Layers:** Extract spatial features like ridges, minutiae points, and global fingerprint patterns.
- **Pooling Layers:** Down sample feature maps to reduce dimensionality and computational load.
- **Dense Layers:** Combine extracted features for classification.
- **Dropout:** Regularizes the network by randomly disabling neurons during training, preventing overfitting.

**4. Dataset Preparation and Balancing**

The dataset is prepared by:

- Merging altered fingerprint categories (Easy, Medium, Hard) into a single class.
- Balancing the dataset by combining real and altered images into distinct directories.

To avoid bias, **data augmentation** is applied using techniques such as:

- Rotation, scaling, and flipping to simulate variations.
- Rescaling pixel intensities to the range [0, 1] for normalization.

**5. Training and Validation**

- The dataset is split into **training (80%)** and **validation (20%)** subsets to ensure robust model evaluation.
- The model is trained using:
    - **Binary Cross Entropy Loss Function:** Quantifies the error between predicted probabilities and true labels.
    - **Adam Optimizer:** Efficiently updates model parameters by combining momentum and adaptive learning rates.

**6. Evaluation Metrics**

Model performance is assessed using:

- **Accuracy:** Percentage of correctly classified samples.
- **Precision:** Proportion of true positives among predicted positives.
- **Recall:** Proportion of true positives among actual positives.
- **F1 Score:** Harmonic mean of precision and recall, balancing false positives and negatives.

### 3.3 Experimental Process and Workflow

**Step 1: Data Preparation**

- **Real Fingerprints:** Extracted from the "Real" dataset folder.
- **Altered Fingerprints:** Combined from "Altered-Easy," "Altered-Medium," and "Altered-Hard" datasets.
- **Preprocessing:** Images are resized, padded, and contrast-enhanced.

**Step 2: Data Augmentation**

Augmentation creates synthetic variations, enhancing model robustness. Techniques include:

- Random rotations, width/height shifts, shear transformations, and horizontal flips.

**Step 3: Model Architecture**

The CNN architecture includes:

- **Convolutional and Pooling Blocks:** Extract low- and high-level features.
- **Flattening Layer:** Converts 2D feature maps into 1D vectors.
- **Dense Layers:** Process extracted features for binary classification.
- **Sigmoid Activation:** Outputs probabilities for binary classes (Real/Altered).

**Step 4: Model Training**

- **Early Stopping Callback:** Stops training if validation performance stagnates.
- **Metrics Visualization Callback:** Tracks precision, recall, F1-score, and accuracy at each epoch.

**Step 5: Testing and Prediction**

Test images undergo the same preprocessing pipeline. Predictions are based on:

- **Thresholding:** Outputs > 0.5 are classified as "Real," and ≤ 0.5 as "Altered."

**Algorithms and Models**

**1. Data Augmentation:**

Image Data Generator from TensorFlow performs augmentation and normalization.

**2. Convolutional Neural Networks (CNNs):**

The model architecture uses four convolutional layers with increasing filter sizes (32, 64, 128, 256) and ReLU activations to learn spatial hierarchies.

**3. Training Optimizer:**

Adam optimizer dynamically adjusts learning rates to balance speed and convergence.

**4. Evaluation Metrics:**

Precision, recall, and F1-score ensure balanced evaluation for imbalanced datasets.

**5. Preprocessing Pipeline:**

Custom preprocessing with OpenCV and PIL standardizes test images before prediction.

### 3.4 Analytical and Numerical Models

**1. Numerical Model:**

- **Forward Propagation:** Processes input images through convolutional, pooling, and dense layers.
- **Backpropagation:** Updates weights using the Adam optimizer to minimize binary cross entropy loss.

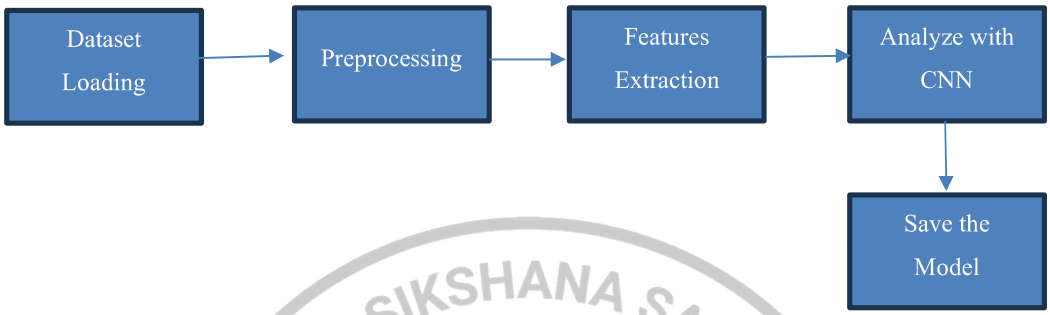
**2. Analytical Models:**

- Fingerprint classification is treated as a **binary hypothesis testing problem**:
  - Null Hypothesis (H0H_0H0): The fingerprint is real.
  - Alternative Hypothesis (H1H_1H1): The fingerprint is altered.

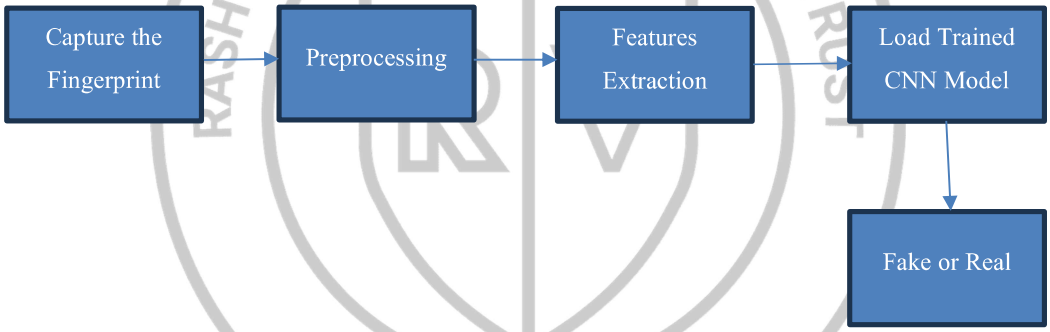
# CHAPTER 4

## Methodology

**Training Phase:**




**Testing Phase:**



**Training Phase:**

**1. Collecting the Dataset**

This phase involves assembling a comprehensive dataset comprising:

- Real fingerprints: These can be sourced from publicly available datasets or captured using fingerprint scanners from volunteers.
- AI-generated synthetic fingerprints: These can be created using advanced generative algorithms, such as GANs (Generative Adversarial Networks), which produce realistic-looking fingerprints.

**2. Preprocessing the Dataset**

Preprocessing is essential for cleaning and standardizing the fingerprint images before analysis. Key steps include:

- Noise Removal: Using filters (e.g., Gaussian blur or median filters) to eliminate random noise in the images.
- Image Resizing: Standardizing all fingerprint images to the same dimensions (e.g., 128x128 pixels) for uniformity.
- Contrast Enhancement: Adjusting brightness and contrast to make ridge patterns clearer.
- Binarization: Converting the image to a binary format where ridges are represented by black and valleys by white.
- Normalization: Ensuring consistent intensity levels across all images to avoid biases during feature extraction.

**3. Feature Extraction**

Feature extraction involves identifying and encoding unique characteristics of the fingerprint, such as:

- Ridges and Valleys: Patterns of raised lines (ridges) and recessed spaces (valleys).

- Minutiae Points: Tiny unique features like ridge endings, bifurcations, and dots.
- Patterns: Broad patterns like loops, whorls, and arches.

**4. Analyze with CNN (Convolutional Neural Network)**

Once the features are extracted, they are processed by a Convolutional Neural Network (CNN), a type of deep learning algorithm ideal for image analysis. The process includes:

- Training Phase:
  - Feeding the preprocessed fingerprint images into the CNN.
  - The CNN consists of layers like convolutional, pooling, and fully connected layers that learn spatial hierarchies of features (from edges to complex patterns).
  - The network adjusts its weights through backpropagation to minimize error and improve its ability to classify real versus fake fingerprints.
- Validation: Testing the model on unseen data during training to ensure it generalizes well.

**5. Saving the Trained Model**

Once the CNN achieves satisfactory accuracy during training, the final model (weights and architecture) is saved. This ensures the model can be reused for future predictions without needing retraining.

**Testing Phase:**

**1. Fingerprint Capture for Testing**

When evaluating a new fingerprint:

- Capture Method: Use a fingerprint scanner or high-resolution camera to acquire a clear image.
- Image Quality: Ensure the image has minimal distortions, proper lighting, and high clarity to facilitate accurate analysis.

**2. Preprocessing for Testing**

The captured fingerprint image undergoes the same preprocessing steps as during training:

- Noise removal, resizing, normalization, and enhancement to prepare it for feature extraction.

**3. Feature Extraction for Testing**

The system extracts key fingerprint features from the preprocessed image using the same method applied in the training phase. This ensures the features are compatible with the trained CNN model.

**4. Loading the Trained CNN Model**

The system loads the trained CNN model, which contains the learned patterns and characteristics required to differentiate between real and fake fingerprints.

**5. Classification: Real or Fake**

The extracted features from the new fingerprint are fed into the trained CNN model. The model performs the following:

- Comparison: Matches the features against patterns it learned during training.
- Decision:
    - If the fingerprint aligns with the characteristics of a real fingerprint, it is classified as "Real Image."
    - If the fingerprint displays signs of AI generation, tampering, or alteration, it is classified as "Altered Image."

# CHAPTER 5

## Project Specifications

### 5.1 Experimental details

The project focuses on detecting **AI-generated Fingerprint** using machine learning techniques. A comprehensive dataset of real and AI-generated images is compiled, followed by feature extraction through pixel analysis, metadata inspection, and frequency domain analysis. Machine learning models, including CNNs and Random Forests, are trained and tested to classify images. Performance is evaluated using metrics like accuracy, precision, and recall, providing insights into the models' effectiveness in distinguishing AI-generated content.

### 5.2 Software & Testing

For machine learning projects, kaggle.com(Software) is an excellent resource; it's particularly appropriate for "AI Generated Fingerprint Image Detection Using Machine Learning." It offers cloud-based notebooks with frameworks like TensorFlow and PyTorch pre-installed, as well as access to big datasets, including fingerprint image data. Model training and testing are accelerated by Kaggle's integrated GPU and TPU support. Researchers can exchange ideas, compete in competitions, and improve models in its collaborative environment. Kaggle's tools are essential for fingerprint detection projects since they provide efficient data processing, feature extraction, and performance evaluation.

An 80:20 split is frequently used to separate datasets into training and testing sets in order to test the "AI-Generated Fingerprint Image Detection Using Machine Learning" algorithm. To verify generalization, the models are tested on the test set after being trained on the training set. Strong performance analysis is ensured by cross-validation methods like k-fold validation. The model's strength is evaluated using key measures such as accuracy, precision, recall, and F1-score. The visualization tools provided by Kaggle aid in result analysis, misclassification identification, and further model improvement to increase detection accuracy.

### 5.3 Result and Discussion

"**AI Generated Fingerprint Image Detection Using Machine Learning**" creates an intelligent system capable of efficiently classifying fingerprint photographs. The uploaded images would be categorized as "Real" if they were taken with authenticity or "Altered" if they were created using artificial intelligence. The developed systems achieve high precision and recall by generating precise models using robust datasets. In order to support security, forensics, and authentication procedures, this solution will be a dependable tool for differentiating between real and artificial intelligence-generated fingerprints.


Fig.5.3.1: Training and Validation Accuracy


Fig.5.3.2: Training & Validation Loss

- 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.

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

Table 5.3.3: Accuracy

- 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.

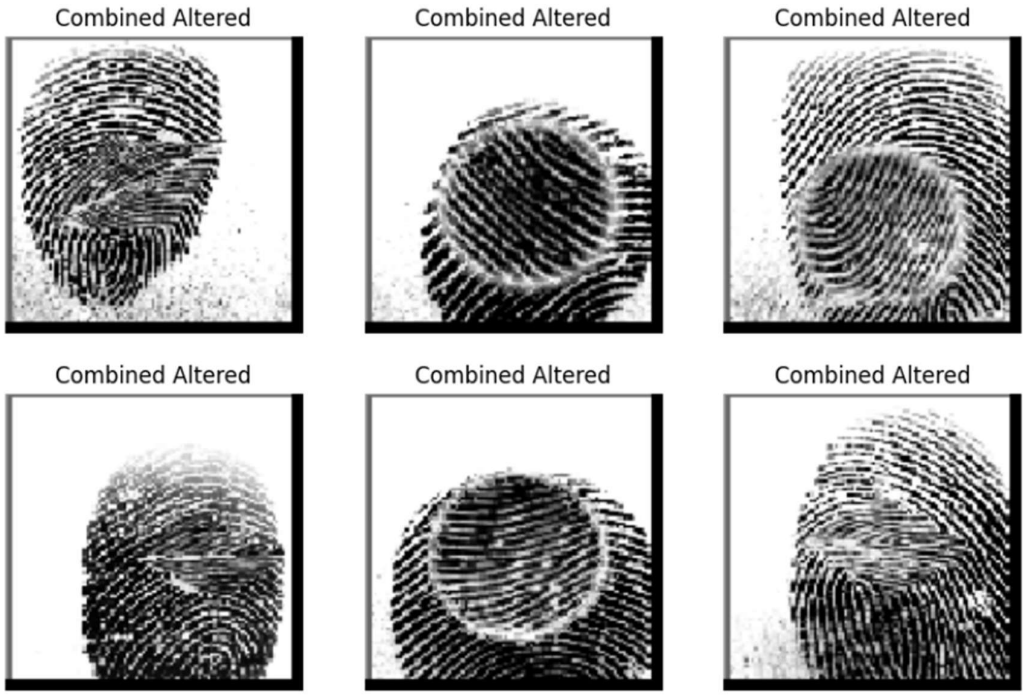
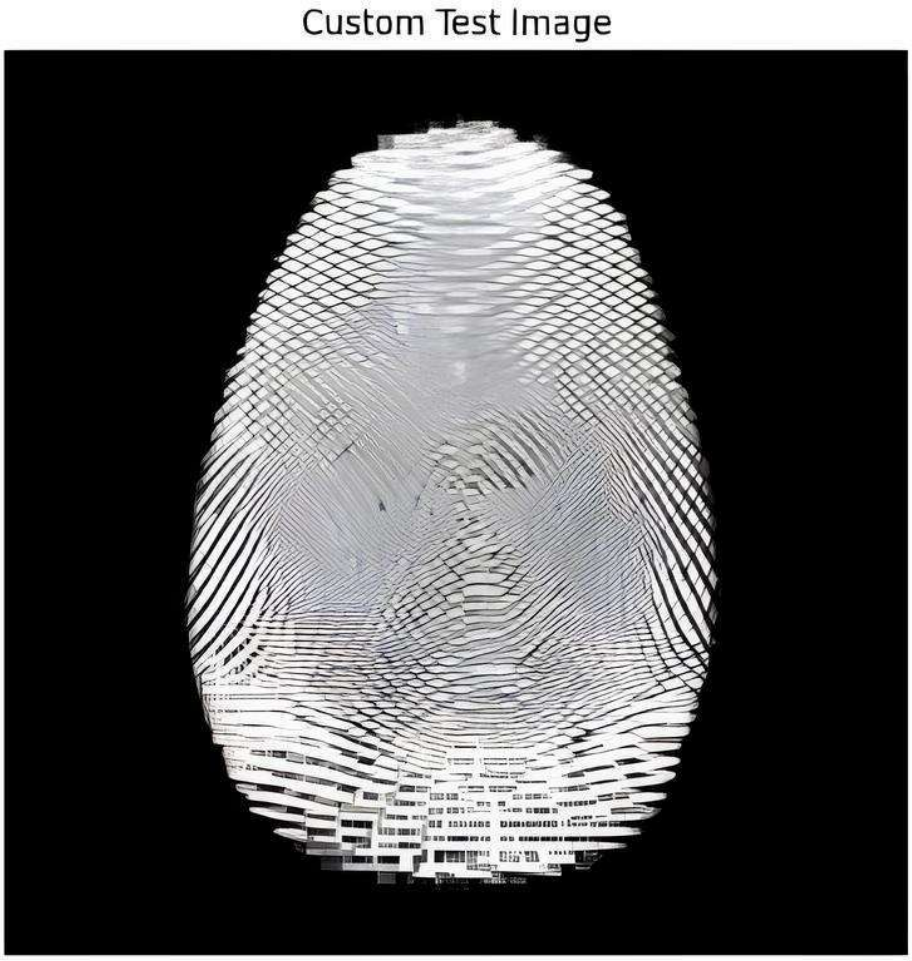



Fig.5.3.4: Altered Fingerprints Image

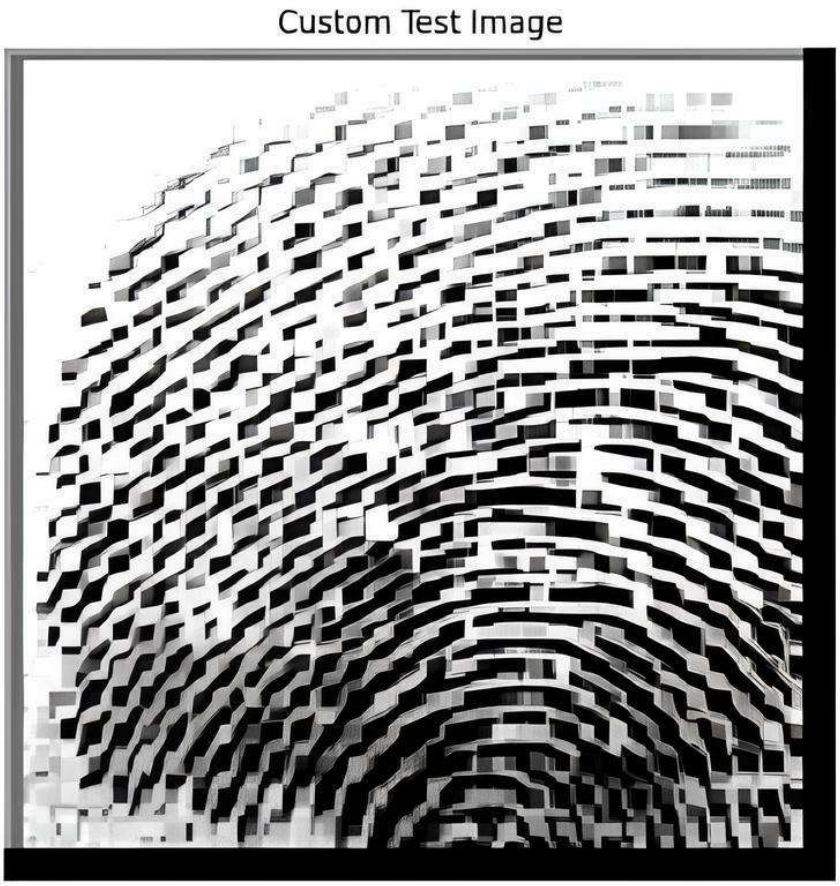

Fig.5.3.5: Real Fingerprints Image




[189]:
```
# Step 7: Classify the Custom Image
result = predict_image(model, custom_image_path)
print(f"The fingerprint is classified as: {result}")
```

```
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 110ms/step
The fingerprint is classified as: Altered
```

Fig.5.3.6: Altered Fingerprint image detected by trained model




```
Step 12.3: Custom single test image displayed successfully!
```

```
[20]:
# Step 12.4: Test the model with the custom image
result = predict_image(loaded_model, custom_test_image_path)
print(f"The fingerprint is classified as: {result}")
```

```
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 119ms/step
The fingerprint is classified as: Real
```

Fig.5.3.7: Real Fingerprint image detected by trained model

# CHAPTER 6

## Conclusion and Future Scope

The project demonstrates the ability to distinguish a fingerprint image from real and those which AI produced by using advanced machine learning. It uses robust algorithms in a system, feature extraction method with effective classification models to attain great precision of identification regarding synthesized fingerprint issu es- the critical security concern associated with biometric systems. This research points out the increasing demand for automated tools to counter AI-driven spoofing attempts and ensure the integrity of biometric authentication.

Future work can include enhancing the adaptability of the model to diverse datasets, improving performance under real-world scenarios, and integrating deep learning techniques for greater accuracy. The system will be made more robust and efficient by the incorporation of real-time detection capabilities, cross-platform validation, and hybrid models that combine both traditional and deep learning methods. Its scalability to large-scale deployments and reduction of computational costs will make it better applied in practice. Overall, the project makes a significant step forward to secure biometric systems against emerging AI-generated threats by safeguarding critical digital infrastructures and contributing to the advancement of more secure and trustworthy biometric authentication systems in the modern digital era.

## 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, pp. 3827-3833, 2024, 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, pp. 1848-1852, 2020, 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, pp. 580-587, 2014, 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, pp. 193 203, 2022, 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, pp. 5495-5502, 2021, 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.
13. 14. 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, pp. 2057-2061, 2017, 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, pp. 895-903, 2019, 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, pp. 1-10, 2018, 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.

## Annexure A: Paper Published Certificates

**Title of the Paper:**

***AI-Generated Fingerprint Image Detection Using Machine Learning***

Certificate for Author 1: Nandan D S

## Annexure B: Front Page of Published Paper

**Title of the Paper:**

***AI-Generated Fingerprint Image Detection Using Machine Learning***

Front Page of the Paper:

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.