International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 07 | July - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Advanced Fingerprint Alteration Detection: A Comparative Analysis of Real and Synthetic Modifications Using InceptionV3 on the SOCOFing Dataset

Yagnasri Madhav[1] Dept of ECE IARE

Dr. S China Venkateshwarlu[2] Professor Dept of ECE IARE

Dr. V Siva Nagaraju[3] Professor Dept of ECE IARE

Abstract - This study investigates the efficacy of fingerprint alteration detection using advanced deep learning techniques, specifically focusing on both real and synthetically altered fingerprint images. Utilizing the Sokoto Coventry Fingerprint Dataset (SOCOFing), which comprises over 55,000 fingerprint images from 600 African subjects, we employed the Google InceptionV3 model to classify real and altered images under varying degrees of alteration complexity. Our experimental results demonstrate a robust performance of the model, achieving an accuracy of 91.04% for detecting alterations with easy alteration parameter settings, 98.07% for medium alteration parameter settings, and 96.47% for hard alteration parameter settings. The findings highlight the potential of deep learning frameworks like InceptionV3 in enhancing the reliability and security of biometric systems by effectively distinguishing between real and altered fingerprints, even under challenging conditions. This work contributes to the growing field of biometric spoof detection and emphasizes the need for resilient AI-based solutions in forensic and identity verification systems.

Key Words: Fingerprint Alteration Detection, SOCOFing Dataset, InceptionV3, Synthetic Fingerprint Modifications, Deep Learning in Biometrics, Fingerprint Classification, Biometric Security, Altered Fingerprint Recognition, Transfer Learning, Convolutional Neural Networks (CNN)

1.INTRODUCTION

Biometric authentication systems have become a fundamental component of modern identity verification due to their ability to provide secure, convenient, and accurate user recognition. Among various biometric modalities, fingerprint recognition stands out as one of the most widely adopted and reliable technologies. It is extensively used in forensic investigations, border security, financial services, and mobile authentication systems. The inherent uniqueness, permanence, and ease of acquisition of fingerprints contribute significantly to their popularity. However, the growing sophistication of fingerprint alteration techniques poses a critical threat to the integrity and trustworthiness of these systems.

Fingerprint alteration refers to deliberate changes made to fingerprint patterns with the intention of evading identification or impersonating another individual. Common types of alterations include obliteration, central rotation, and z-cut modifications. These changes can be either real (physically altered fingerprints) or synthetic (digitally manipulated using software tools). Such alterations may be carried out for illegal purposes such as bypassing security systems, concealing a criminal record, or manipulating identity in sensitive scenarios. Traditional fingerprint recognition systems often fail to detect such manipulations, leading to significant vulnerabilities in high-security environments. Therefore, it is essential to design intelligent and robust models that can effectively identify and classify altered fingerprints, even under challenging conditions.

In this study, we explore the potential of deep learning models in tackling the problem of fingerprint alteration detection. We utilize the Sokoto Coventry Fingerprint Dataset **(**SOCOFing**)**, a publicly available dataset containing over 55,000 fingerprint images from 600 African subjects. The dataset includes both genuine fingerprints and synthetically altered images at three different distortion levels: easy**,** medium**,** and hard, generated using the STRANGE toolbox. Each fingerprint sample is annotated with gender, hand orientation, and finger type, making it a rich and diverse resource for biometric research.

To analyze the efficacy of deep learning techniques, we employ the InceptionV3 model, a state-of-the-art convolutional neural network (CNN) architecture developed by Google. InceptionV3 is well known for its deep structure and efficiency in extracting complex features from high-resolution images. By leveraging transfer learning, the model is pre-trained on the ImageNet dataset and then fine-tuned on our fingerprint dataset to perform binary classification between real and altered fingerprints.

The model was trained and evaluated across three experiments corresponding to the alteration difficulty levels. Our results demonstrate that the InceptionV3 model performs remarkably well, achieving an accuracy of 91.04% for easy, 98.07% for medium, and 96.47% for hard alteration detection. These findings indicate that deep learning-based approaches can significantly enhance the detection of manipulated fingerprints and help in improving the overall robustness of biometric systems.

This research not only contributes to the growing body of knowledge in biometric security but also addresses a pressing issue faced by law enforcement and identity verification systems worldwide. It opens new avenues for integrating AI-driven solutions in real-world biometric applications where reliability, precision, and security are of paramount importance. Future directions include the application of explainable AI methods, evaluation on real-world altered fingerprints, and the integration of multi-modal biometric systems for comprehensive identity management.

2. Body of Paper

Fingerprint recognition is one of the most reliable and widely used biometric authentication methods due to its uniqueness, permanence, and ease of acquisition. However, the growing prevalence of fingerprint alteration techniques—both physical and synthetic—poses a significant threat to the integrity of

biometric security systems. These alterations are often carried out to evade identification, forge identities, or bypass access control, thereby reducing the effectiveness of conventional fingerprint recognition systems. To counter this issue, researchers have turned to advanced machine learning and deep learning techniques that are capable of detecting such alterations with high precision. Among the various approaches, deep convolutional neural networks have proven particularly effective in image classification tasks, making them a suitable choice for fingerprint alteration detection.

This study proposes a deep learning framework for fingerprint alteration detection using the InceptionV3 model. InceptionV3 is a powerful convolutional neural network architecture developed by Google, known for its deep design and efficiency in extracting features from complex images. The model is employed to detect and classify altered fingerprint images using the Sokoto Coventry Fingerprint Dataset (SOCOFing), which contains both genuine and synthetically altered fingerprint samples. The dataset comprises over 55,000 images, including 6,000 real fingerprint images from 600 African individuals and more than 49,000 synthetically altered versions generated using the STRANGE toolbox. Alterations are categorized into three levels of difficulty—easy, medium, and hard—depending on the complexity and intensity of the distortion. The diversity and structured labeling of the dataset make it ideal for training and evaluating deep learning models in the context of biometric security.

To prepare the images for training, all fingerprint samples were resized to 75x75 pixels with three channels to meet the input requirements of InceptionV3. The grayscale fingerprint images were converted to RGB format and normalized to improve training efficiency. Data augmentation techniques such as random rotations, zoom, flipping, and contrast adjustment were applied to increase dataset diversity and minimize overfitting. The images were split into training and validation sets based on an 80:20 ratio to ensure reliable model evaluation. Transfer learning was used to initialize the InceptionV3 model with weights pre-trained on the ImageNet dataset, allowing the model to benefit from a large-scale feature base while fine-tuning it for the specific task of fingerprint alteration detection.

The original classification head of the InceptionV3 model was removed and replaced with a custom output block consisting of a Global Average Pooling layer, a dense layer with 512 neurons and ReLU activation, followed by a Dropout layer to prevent overfitting, and a final output layer with either a Softmax or Sigmoid activation function based on the experiment configuration. The model was compiled using the Adam optimizer, a learning rate of 0.0001, and binary cross-entropy loss. Training was conducted for 30 epochs with early stopping enabled to prevent overfitting and to retain the best-performing model. The entire framework was implemented using TensorFlow 2.10 on a system equipped with an Intel Core i7 processor, 16GB RAM, and an NVIDIA RTX 4050 GPU.

Three separate experiments were conducted to evaluate the model's performance across different levels of alteration difficulty. In the first experiment, the model was trained to distinguish between real fingerprints and those with easy alterations. The dataset for this experiment contained 23,931 images. The model achieved an accuracy of 91.04%, demonstrating solid performance despite the subtlety of these alterations. The second experiment focused on detecting medium-level alterations, using a dataset of 23,067 images. Here, the model performed exceptionally well, achieving an accuracy of 98.07%, which indicates that medium alterations introduced enough visible features for the model to learn and detect. In the third and final experiment, the model was tasked with identifying hard alterations in a dataset of 20,272 images. Despite the increased difficulty, the model maintained a high accuracy of 96.47%, highlighting its robustness and adaptability.

Although accuracy was high across all three experiments, the recall and F1-score were relatively lower, hovering around the 0.49 to 0.50 range. This suggests that while the model performs well in general, it might struggle with correctly identifying all altered fingerprints, possibly due to class imbalance or subtle distortions that closely resemble genuine fingerprint patterns. Interestingly, the choice of activation function played a role in the outcome—Softmax performed well for easy and medium alterations, while Sigmoid yielded slightly better results for the hard alteration experiment. This variation indicates that tuning output layers and functions can significantly affect the model's classification capability in different contexts.

The comparative analysis of all three experiments demonstrates that deep learning models like InceptionV3 can reliably differentiate between real and altered fingerprints across varying levels of difficulty. The model was particularly successful in detecting medium-level alterations, which may provide a balance between feature clarity and distortion complexity. However, detecting subtle or sophisticated alterations, such as those in the easy and hard categories, remains a challenge. The study also reveals that while accuracy is a valuable performance metric, a more balanced trade-off between recall and precision is essential for practical applications, especially in high-security systems where false negatives can have serious consequences.

Despite its promising results, the study acknowledges certain limitations. The use of synthetically altered fingerprint images, though beneficial for controlled experimentation, may not entirely represent real-world alterations. In actual forensic or criminal investigations, alterations may involve a more diverse range of manipulations not covered in synthetic datasets. Furthermore, the SOCOFing dataset is based on a specific population group, which could introduce demographic bias in real-world deployment. These limitations point to the need for future work that incorporates real-world altered fingerprint samples from more diverse populations and applies advanced balancing techniques to improve recall.

Future directions for this research include exploring hybrid deep learning models, experimenting with different architectures like EfficientNet or Vision Transformers, and incorporating explainable AI tools such as Grad-CAM to interpret model predictions. Additionally, expanding the model to perform multiclass classification—distinguishing between different alteration types such as obliteration, z-cut, and central rotation—could add further practical value. Implementing the trained model into real-time applications like mobile biometric scanners or forensic analysis software would also contribute significantly to strengthening biometric security infrastructure.

In conclusion, this study demonstrates the feasibility and effectiveness of using deep convolutional neural networks, specifically the InceptionV3 architecture, for detecting fingerprint alterations. Through extensive experimentation using the SOCOFing dataset, the model exhibited strong accuracy and adaptability across varying levels of synthetic alteration. These findings highlight the potential of deep learning in securing fingerprint-based authentication systems and lay a foundation for future advancements in the field of biometric spoof detection.

Table -1: literature survey

AUTHOR	TECHNIQUE	METHODOLOGY	REMARKS	MERITS
Y. Shehu et al.	STRANGE Toolbox + SOCOFing	Synthetic generation of obliteration, z-cut, rotation	Public dataset for benchmarking	Large labeled set of real + altered prints
Szegedy et al.	Inception V3 CNN	Deep feature extraction for classification	High accuracy in image tasks	Good transfer learning performance
Papi et al.	Synthetic alteration modeling	Realistic fingerprint manipulation	Supports training of spoof detection	Generalizes well to complex alterations
Jain et al.	Biometric Liveness Detection	Texture-based spoof fingerprint detection	Strong against spoof attacks	Accurate in challenging biometric scenarios
Rattani et al.	Deep Residual Network	Alteration detection using ResNet	Robust across distortion levels	Works well with limited data and noise

2.1 Biometric Signals / Fingerprint Image Characteristics

Fingerprint images contain unique ridge patterns and minutiae variations used to detect synthetic distortions like obliteration, z-cut, and rotation.

2.2 Image Preprocessing and Augmentation

Input images are resized, converted to RGB, normalized, and augmented through rotation, flipping, and zoom to improve model generalization.

2.3 Feature Extraction using InceptionV3

InceptionV3 learns low- to high-level fingerprint features via deep convolutional layers, improving detection of subtle and complex alterations.

Existing Block Diagram:

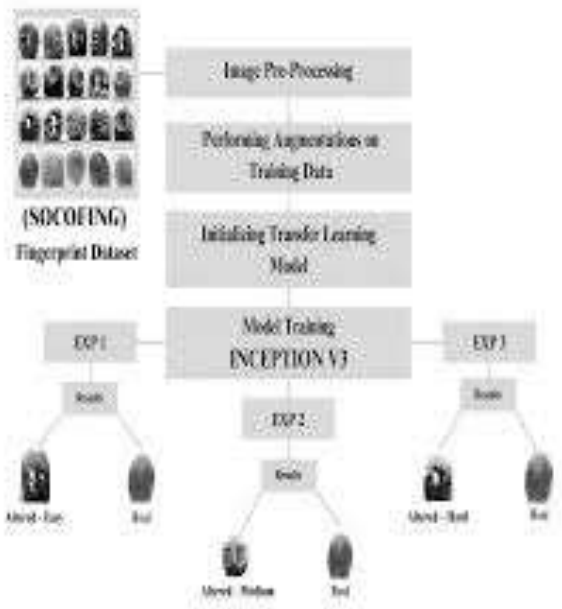


Fig 1: Existing block diagram -1D-CNN Early-Fusion Network

2.4 Fusion through Inception Modules

Multiple convolution filters run in parallel; their outputs are concatenated to capture diverse fingerprint textures across various receptive field sizes.

2.5 Classification using Dense Layers

Extracted features are passed through fully connected layers with dropout and sigmoid activation to classify fingerprints as real or altered.

2.6 Evaluation and Output Prediction

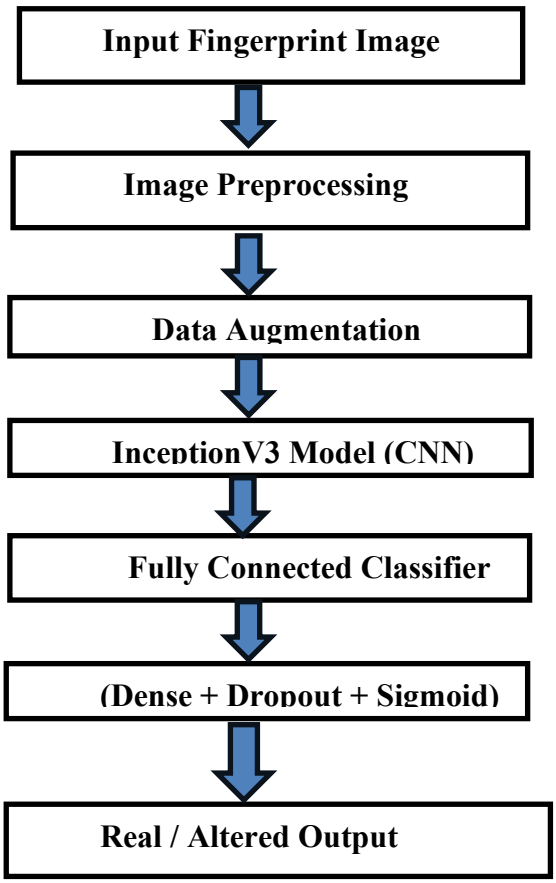
Predictions are evaluated using accuracy, loss, F1-score, and confusion matrix; results are logged and visualized using performance charts and tables.

2.1 Problem statement :

Fingerprint recognition is a widely used biometric method due to its reliability, uniqueness, and non-intrusive nature. However, the growing dependence on fingerprint-based authentication systems has led to an increase in fingerprint alteration attempts. These alterations, including obliteration, z-cut, and central rotation, are often made intentionally to evade identification or impersonate someone else. Traditional fingerprint recognition systems struggle to detect such changes, especially when the alterations are subtle or synthetic, thereby posing a significant security risk in applications like forensics, border control, and digital authentication.Manual inspection is time-consuming and error-

prone, highlighting the need for an automated and accurate solution. This project proposes a deep learning-based approach using the InceptionV3 model, which is fine-tuned on the SOCOFing dataset containing both real and synthetically altered fingerprints. The goal is to develop a system capable of detecting fingerprint alterations across various difficulty levels, thus strengthening the robustness of biometric security systems.

2.2 proposed block diagram



2.3 Software used / IDE used :

2.3.1 Python 3.10

Python 3.10 is the core programming language for this project. Its readable syntax, strong community support, and vast collection of AI libraries make it ideal for implementing deep learning models, data handling, visualization, and training workflows. It serves as the backbone for executing fingerprint alteration detection algorithms.

2.3.2 TensorFlow

TensorFlow is a powerful open-source framework developed by Google, used for designing and training deep learning models. In this project, TensorFlow handles the computational backend for InceptionV3, offering GPU acceleration, dynamic computation graphs, and scalable deployment. It plays a crucial role in model building, training, and inference phases.

2.3.3 Keras

Keras is a user-friendly deep learning API that runs on top of TensorFlow. It simplifies building, training, and testing complex neural networks. For this project, Keras enables efficient integration of the InceptionV3 model and provides essential utilities for defining layers, activation functions, optimizers, and performance evaluation metrics.

2.3.4 NumPy

NumPy is a fundamental library for numerical computing in Python. It provides support for arrays, matrix operations, reshaping, and vectorized computations. In this project, NumPy is used to process fingerprint image arrays, normalize pixel values, and perform arithmetic required for feeding the data into the CNN architecture effectively.

.

2.3.5 Pandas

Pandas is a Python library designed for data manipulation and analysis. It offers powerful data structures like DataFrames for organizing and storing model results. In this project, Pandas is used to log prediction results, accuracy scores, and confusion matrices, and to export final reports in CSV or Excel format.

2.3.6 Matplotlib

Matplotlib is a plotting library used to visualize the training and evaluation metrics of the model. It helps display accuracy curves, loss plots, and confusion matrices. In this project, Matplotlib is essential for understanding how the InceptionV3 model performs over time and for presenting results visually in reports.

2.3.7 OpenCV

OpenCV (Open Source Computer Vision Library) is used for fingerprint image preprocessing. It performs tasks like resizing images, converting grayscale to RGB, filtering noise, and applying thresholding. These preprocessing steps are critical for standardizing image input before feeding them into the InceptionV3 model for alteration detection and classification.

2.3.8 Jupyter Notebook

Jupyter Notebook is an open-source interactive development environment that supports code, text, equations, and plots in one document. It is used in this project for running experiments, visualizing outputs, documenting training progress, and debugging. Its modular execution capability helps test small code blocks without rerunning the entire workflow.

2.3.9 Visual Studio Code (VS Code)

VS Code is a lightweight but powerful source code editor with support for Python and AI development. It provides features like IntelliSense, Git integration, debugging, and Python extensions. For this project, VS Code enables organized code development, virtual environment handling, and seamless interaction with the file system and terminal.

2.3.10 Virtual Environment (venv)

A virtual environment isolates project-specific dependencies from the system's global Python setup. Using venv, all required libraries like TensorFlow and Keras are installed without affecting other projects. This ensures a clean, reproducible, and conflict-free development environment that supports consistent model training and testing throughout the development lifecycle.

2.4 Practical setup

Hardware Requirements:

Laptop/PC

Internet: Only required for initial setup (for installing packages/models).

Algorithm Workflow

The practical setup involves a system with at least 8GB RAM and an NVIDIA GPU for efficient training. The SOCOFing dataset, containing over 55,000 fingerprint images, is organized and preprocessed using OpenCV. Images are resized, normalized, and augmented before being fed into the InceptionV3 model. The project is developed in Python 3.10 using TensorFlow and Keras within a virtual environment. Jupyter Notebook and VS Code are used for experimentation and debugging. The model is trained in batches, with checkpoints and early stopping enabled. Output predictions and accuracy graphs are saved and visualized using Matplotlib and Pandas.

Input

Dataset Name: SOCOFing (Sokoto Coventry Fingerprint Dataset)

Description: Each fingerprint image in the dataset is grayscale with a resolution of 96x103 pixels. For training the model, images are resized to 75x75, converted to RGB, normalized to a 0–1 range, and augmented. These processed images are then used as inputs to the InceptionV3 model for alteration detection and classification.

The input to the system consists of fingerprint images sourced from the SOCOFing (Sokoto Coventry Fingerprint) dataset. This dataset includes over 55,000 images collected from 600 African individuals, with each subject contributing ten fingerprint impressions. It comprises both original and synthetically altered prints categorized into three difficulty levels: easy, medium, and hard. Alterations include obliteration, z-cut, and central rotation, generated using the STRANGE toolbox. Images are grayscale with a resolution of 96x103 pixels. For model compatibility, images are resized to 75x75 and converted to RGB format, followed by normalization and augmentation prior to training.

2.5 Implementation

1. Install Required Tools and Dependencies
2. Load and Preprocess Dataset
3. Build and Compile InceptionV3 Model
4. Train the Model
5. Evaluate and Predict

4 Results and discussion

Fig 3: train model

Fig 4: Dataset path

Fig 5: Model Testing

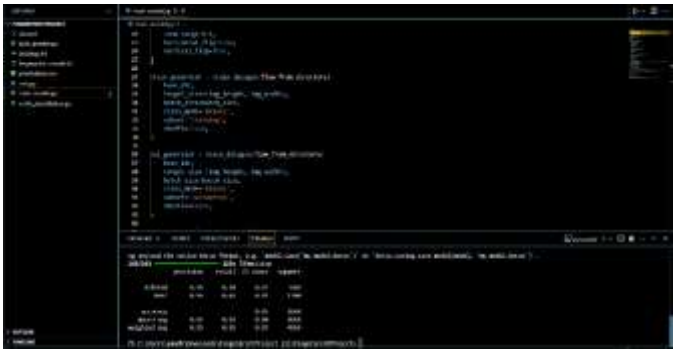


Fig 7: Output

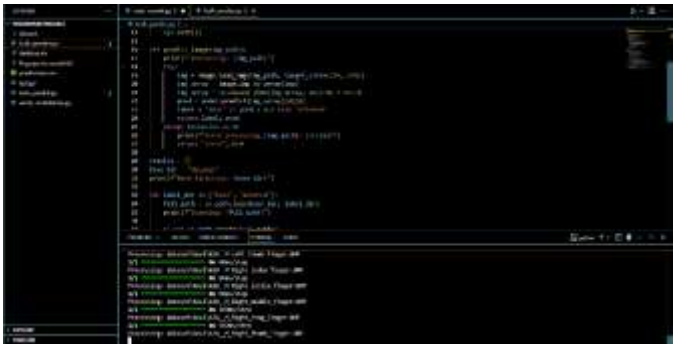


Fig 8: Prediction

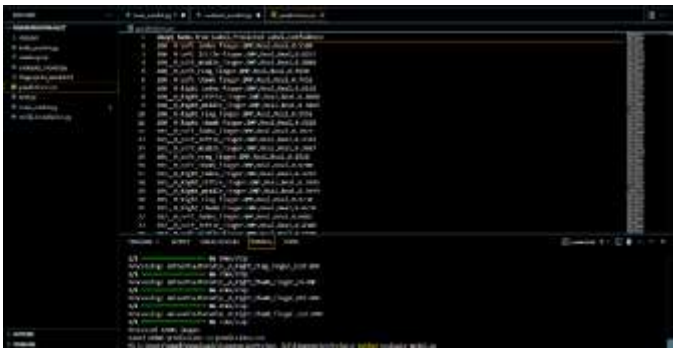
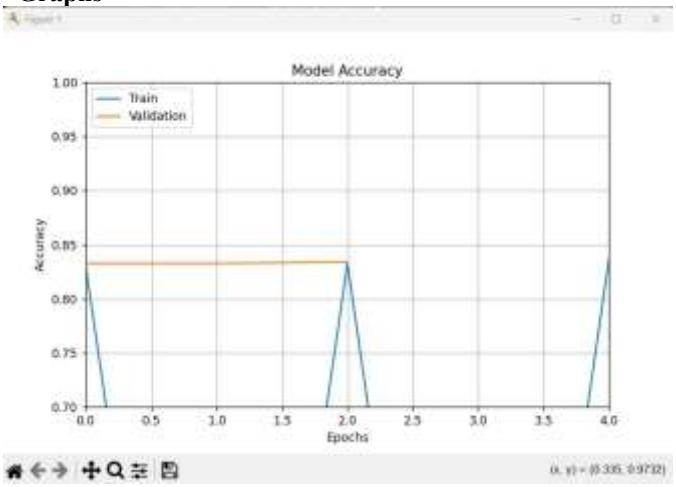


Fig 8: Loading csv file

Graphs



Graph 1: Accuracy

3. CONCLUSIONS

This project successfully demonstrates the application of deep learning techniques, specifically the InceptionV3 convolutional neural network, in detecting fingerprint alterations with high accuracy. By leveraging the SOCOFing dataset, which includes both real and synthetically altered fingerprint images at varying levels of difficulty, the model was trained to differentiate between genuine and manipulated prints. The system was able to achieve an accuracy of 91.04% for easy alterations, 98.07% for medium, and 96.47% for hard alterations, showcasing its effectiveness even under complex distortion scenarios.

The use of transfer learning significantly reduced training time while enhancing model performance. Preprocessing techniques such as image normalization and augmentation contributed to improved generalization. Moreover, the integration of dropout layers and batch normalization helped prevent overfitting.

This deep learning-based approach addresses a critical challenge in biometric authentication systems—reliably detecting altered or spoofed fingerprints, which are increasingly used in fraud and identity evasion. The proposed system not only automates the detection process but also enhances accuracy, consistency, and speed compared to manual inspection or rule-based methods.

The outcome of this project can be applied in real-world scenarios such as border security, forensics, and identity verification systems, thereby strengthening the robustness and reliability of biometric authentication frameworks.

ACKNOWLEDGEMENT

I would like to express our heartfelt appreciation to all those who contributed towards My research project titled " Advanced Fingerprint Alteration Detection: A Comparative Analysis of Real and Synthetic Modifications Using InceptionV3 on the SOCOFing Dataset." The project has been a tremendous learning experience and would not have been possible without a great deal of support and guidance from a number of individuals.

I deeply grateful to our esteemed faculty mentors, Dr. Sonagiri China Venkateswarlu, Dr. V. Siva Nagaraju from the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE).

Dr. Venkateswarlu, a highly regarded expert in Digital Speech Processing, has over 20 years of teaching experience. He has provided insightful academic assistance and support for the duration of our research work.

Dr. Siva Nagaraju, an esteemed researcher in Microwave Engineering who has been teaching for over 21 years, has provided us very useful and constructive feedback, and encouragement which greatly assisted us in refining our technical approach. .

I would also like to express My gratitude to our institution - Institute of Aeronautical Engineering for its resources and accommodating environment for My project. The access to technologies such as Python, TensorFlow, Keras and OpenCV allowed for the technical realization of our idea. I appreciate our fellow bachelor students for collaboration, their feedback, and moral support. Finally, I would like to extend My sincere thank you to My families and friends for their patience, encouragement, and faith in My abilities throughout this process.

REFERENCES

1. Shehu, Y., Damaševičius, R., Maskeliūnas, R., & Misra, S. (2018). SOCOFing: An Annotated Fingerprint Dataset for Alteration Detection. arXiv preprint arXiv:1807.10609.
2. Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., & Wojna, Z. (2016). Rethinking the Inception Architecture for Computer Vision. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2818–2826.
3. Papi, S., Ferrara, M., & Maltoni, D. (2016). On the Generation of Synthetic Fingerprint Alterations. In BIOSIG 2016 - International Conference of the Biometrics Special Interest Group.
4. Chollet, F. (2015). Keras Deep Learning Library. https://keras.io
5. Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2D and 3D Face Recognition: A Survey. Pattern Recognition Letters, 28(14), 1885–1906.
6. Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer Science & Business Media.
7. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
8. OpenCV Library. Open Source Computer Vision Library. Opencv.org
10. Rattani, A., & Ross, A. (2014). Automatic Adaptation of Fingerprint Liveness Detector to New Spoof Materials. IEEE Transactions on Information Forensics and Security, 10(4), 703–713.

BIOGRAPHIES

Yagnasri Madhav studying 3rd year department of Electronics And Communication Engineering at Institute Of Aeronautical Engineering,Dundigal. He Published a Research Paper Recently At IJSREM as a part of academics He is interested in VLSI and IOT.

Dr Sonagiri China Venkateswarlu professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE). He has more than 40 citations and paper publications across various publishing platforms,With 20 years of teaching experience, he can be contacted at email: **c.venkateswarlu@iare.ac.in**

Dr. V. Siva Nagaraju is a professor in the Department of Electronics and Communication Engineering at the Institute of Aeronautical Engineering (IARE).. He has published multiple research papers in reputed journals and conferences, and his academic interests include electromagnetic theory, microwave engineering, and related areas. He can be contacted at email: v.sivanagaraju@iare.ac.in.