The ISC Int'l Journal of Information Security
ISeCure

July 2026, Volume 18, Number 2 (pp. 55–67)
http://www.isecure-journal.org

An Innovative Method for Detecting Double Identity Fingerprints from Non-Contiguous Minutiae-Based Attack Technique

Muhammad Sufyan [1,*], Khushbu Khalid Butt [2] Tahir Alyas [1] Omer Irshad [3] Umer Iqbal [2]

[1] *Lahore Garrison University, Computer Science, Lahore, 54920, Pakistan*
[2] *Lahore Garrison University, Information Technology, Lahore, 54920, Pakistan*
[3] *Lahore Garrison University, Software Engineering, Lahore, 54920, Pakistan*

ARTICLE INFO.

Article history:
Received:
Revised:
Accepted:
Published Online:

Keywords:
Biometric authentication, Fingerprint spoofing, Non-contiguous minutiae, MobileNet, Deep learning, SOCOFing dataset, Lightweight neural networks, Real-time verification, Synthetic fingerprint alterations

Type:

doi:

Abstract

Advanced fingerprint spoofing attacks often threaten biometric authentication systems, such as the presence of non-contiguous minutiae to form a double-identity fingerprint. This research paper offers a deep learning system based on MobileNet to differentiate between authentic and anomalous fingerprints. The SOCOFing dataset (in the public domain) with real fingerprints and synthetically deformed samples at three levels of difficulty (easy, medium, and hard) was experimented with, which is used as a reference point in assessing the performance of spoof detection. In order to enhance the generalization, data augmentation and transfer learning were utilized, which helped in increasing the resilience of the model to different fingerprint modifications. The overall test accuracy of the MobileNet-based model was 88%, which declined with the case of medium and hard alterations, which suggests the inability to detect extremely complicated spoofing patterns. However, the model is efficient and has low computational expense, thus it can form a viable yet lightweight real-time biometric verification architecture. The future research ought to cover more sophisticated architectures, cross-dataset testing, and feature-level analysis in order to enhance the detection of difficult forms of spoofing.

1 Introduction

Biometric systems can easily and exactly authenticate a person's identity; they have become an essential part of verification today. Fingerprint recognition is the system chosen most for all types of applications because it is accurate, less expensive, and people find it easy to use [1, 2].

The whole idea behind fingerprint recognition is that certain points, known as minutiae, at the ends of ridges and the places where they split, are unique to each person and never change [3]. Even so, fingerprint-based systems are not fully protected against different kinds of security risks. The double identity attack is quickly becoming a concern because it allows a fraudulent fingerprint to represent more than one identity [4].

* Corresponding author.
Email addresses: maliksufyan1518@gmail.com, drkhushbukhalid@lgu.edu.pk, Tahiralyas@lgu.edu.pk, Omer.irshad@lgu.edu.pk, Umer.iqbal@lgu.edu.pk
ISSN: 2008-2045

With this type of attack, attackers directly take advantage of weaknesses in the system's representation of fingerprints, bypassing both traditional liveness detection and various spoof materials[5]. In these cases, cyber-attackers may generate phony fingerprint images that seem realistic and meet the matching criteria for diverse individuals, thus putting the Automated Fingerprint Identification Systems (AFIS) at risk. Despite improvements made to protect fingerprint data, many systems still have stored unprotected minutiae, making them vulnerable to attack and fake fingerprints [6].

Studies have revealed that it is possible to counteract existing minutiae and produce templates that allow for imitation or cancellation of biometrics, all while preserving the appearance of authentic features and enabling adversarial matching[7]. Minutiae-based fingerprint matchers depend on the fact that the unexpected arrangement of minutiae indicates a real fault in the ridge structure. Still, these approaches often do not have ways to confirm if the groupings of minutiae make sense in space or tend to be realistic. So, systems could be fooled by carefully prepared composite templates that blend a part of two individuals' fingerprint data to create a false identification [8][9]. If there is no defense in the minutiae templates, a fingerprint database can be compromised by inversion attacks and unauthorized use. It is also suggested that cancelable biometrics may help mitigate such problems [10].

The effects of people having two successful identities are very serious. Not only are access control and identity management systems penalized, but biometric evidence cannot always be trusted in courts. If fingerprints stay unchanged over time, they have long supported large-scale identity management systems[11]. Yet, the possibility of making synthetic fingerprints that can easily deceive these systems puts at risk the whole system of biometric authentication. The use of a fake fingerprint match on official IDs like CNIC in Pakistan and biometric passports in the EU may cause someone's identity to be stolen, and this may result in false court cases and issues with data quality [12].

Whereas conventional spoofing can be found out through hardware or material checks, non-contiguous minutiae-based attacks are harder to spot because they function on the digital side of things. Consequently, attackers can still manipulate fingerprint templates, even in an encrypted form, so new strategies are needed to check and prevent such anomalies [13].

This paper aims to venture into the complexities of double identity fingerprint attacks and understand the mechanisms involved, the consequences for biometric security, and the efficacy of the existing solutions. Based on the review of current research and state-of-the-art technologies, we aim to give an overview of the topic under examination and suggest some research directions to strengthen fingerprint recognition systems against such sophisticated threats.

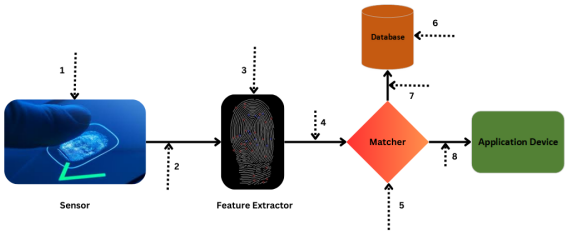

Figure 1. Attacks on Fingerprint

Figure 1 demonstrates several areas where an attacker can compromise a fingerprint recognition system. Attack can happen at the sensor (1) with synthetic fingerprints, in feature extraction (2-3) by eavesdropping on data, at the matcher (4-5) by injecting false features or manipulating comparators, and at the database (6-7) by stealing or corrupting stored templates. Even the application device (8) can be subjected to an attack to abuse the authentication result.

The current paper has three contributions: (1) it shows how a lightweight MobileNetV2-based pipeline, trained on the publicly available SOCOFing dataset, can be fine-tuned to detect non-contiguous attacks against minuteiae-based double-identity biometric authentication; (2) it presents an experimental protocol, where multiple independent experiments are conducted and statistical measures (mean +- standard deviation) are reported to ensure the stability and consistency of the results; (3) it evaluates the efficiency of the model itself: in terms of model size, and inference time This way this work builds upon previous studies on fingerprint-spoof detection (e.g., dual-model networks of VGG16 and ResNet50, feature-fusion approaches of CNN and handcrafted descriptors) by combining accuracy, computational-efficiency, and reproducibility and solving the understudied problem of minutiae-level double-identity attack.

2 Related Work

Fingerprint biometrics are commonly used in identity verification because they are distinct and last for a long time. Still, improved spoofing and other attack methods have made it very challenging for fingerprint recognition systems. The double identity fingerprint attack is a growing problem because it can create

fingerprint images by piecing together the data from two distinct persons' fingerprints.

For more than a hundred years, fingerprints have been used to identify people. In modern systems, there are mostly two steps when using fingerprint recognition. The next stage is to locate the character's points of minutia (endings and bifurcations) and match them with a template in a set database.

Most commonly, minutiae-based systems are used because they can separate individuals very well. Ridge orientation maps, local minutiae descriptors (such as Minutiae Cylinder-Code), and alignment algorithms are commonly used in this part of biometrics [2]. However, they can still be broken if printed or unusual fingerprints are made to match the variations in legitimate prints.

The first method used to spoof biometric security was to make false fingerprints with materials such as gelatin or silicone. Presentation Attack Detection (PAD) methods have been made using texture analysis, deep learning, and multi-spectral imaging [14].

Since image synthesis and adversarial attacks have improved, other more advanced methods were created, such as fingerprint morphing and double identity attacks. This means it is becoming necessary to move beyond physical spoof detection and begin examining major differences in the architecture of the network.

Double identity fingerprinting is the process of making a fake fingerprint that matches both identities on file. Thus, impostors may use different identities to get unauthorized access, which weakens the assumption of biometric systems that every person has a unique biometric trait.

With the rise of digital applications and biometric authentication technologies, the need for reliable verification methods has become essential, and traditional passwords are no longer secure enough to withstand the risks of attack. Fingerprints are one of the most commonly used biometric factors and are not easily borrowed, stolen, or forgotten, as are passwords or RFID cards. But unlike popular belief, fingerprint recognition is not an indomitable method, and the ability to detect fingerprint presentation attack is thus vital [15].

The weaknesses of fingerprint authentication systems have posed serious security issues in high-security-based access control applications, whereas Fingerprint Presentation Attack Detection (FPAD) is a crucial solution for secure authentication. The traditional handcrafted approaches based on features have failed to offer good generalization, and the deep learning approaches have dominated the FPAD field and have performed extremely well in the last decade [16].

Liveness detection for fingerprint impressions is a crucial part of the prevention of unauthorized access and phishing attacks. With the development of unique identification based on biometrics, it has become more accessible, and deep learning technology with computer vision has shown great performance in fingerprint image recognition and detection applications. One recent work suggested a methodology that was based on spatial attention and channel attention models applied in sequence with ResNet convolutions on the LivDet-2021 dataset and tested it against the state-of-the-art CNNs such as DenseNet121, VGG19, InceptionV3, and ResNet50 [17].

The LivDet competition series has been a key to assessing the performance of the PAD fingerprint method, where the contest scenarios and materials were changed every time. LivDet 2019 for the first time featured multi-material combinations, and LivDet 2021 had a new pseudo-consensual method, ScreenSpoof, added to the new fabrics. For LivDet 2023, four datasets were used for two known sensors and two unknown capture devices, thus increasing the difficulty of the existing FPAD approaches for generalization [18].

Fingerprint morphing allows someone to use parts of two different fingerprints to make a combined print that might fool a scanner. In contrast to face morphing, which is a common risk in border security, fingerprint morphing must carefully integrate each set of details, usually to maintain the usefulness of the fingerprint [19].

With non-contiguous techniques, almost all the points from different parts of the fingerprint images are blended to create a single image of the fingerprint. Attackers may pick up more useful points based on ridge flow, location mask, and topological mixture to match two templates and raise the score [20].

It is much more difficult to detect such attacks than contiguous ones since they do not have clear breaks and may appear like normal ridges.

It is only recently that detecting double identity fingerprints created from sparse minutiae has become a challenge. Many techniques have been considered for dealing with this task.

Verifinger and Bozorth systems determine the quality of a fingerprint through the repetition of minute details. Differences in ridge flow, strange angles of the minute features, and variations in the pattern can point to a double identity in these cases [21].

These approaches may still not be able to catch an

attacker who fine-tunes the image to match globally. Reaching the level of knowledge required for detection has pushed researchers in the direction of using machine learning.

Deep learning has made significant progress in fingerprint recognition as CNNs have proven effective in solving the task of visual pattern recognition. Numerous studies have harnessed the promises of CNNs and transfer learning to classify and detect spoofs in fingerprint images drawn from datasets such as SOCOFing.

Researchers have found that CNNs show useful results in handling PAD and spoof detection cases, and suggested the use of a CNN discriminator on real and changed fingerprints to detect small variations in ridge lines and the way minutiae are placed [22].

To address hybrid attacks, researchers extended the model to include scenarios where minutiae are not connected by training it on datasets made using GANs.

In a thesis, Aseel H. Aloweiwi developed a CNN model that achieved 81% accuracy when trained on the SOCOFing dataset in detecting faults in recorded fingerprints. The researchers applied transfer learning to a smaller dataset (ATVS-FakeFingerprint) and realized improved accuracy. This highlights the usefulness of transfer learning in biometric systems that can benefit from access to only limited amounts of labelled data[23].

Another study published in the IIETA Digital Library presented a methodology that combined Gabor filters, HOG, and two machine learning algorithms—Random Forest and Naïve Bayes [24]. Nonetheless, the authors highlighted that enhancing images before analysis and ensuring high-quality fingerprint data contribute significantly to achieving higher accuracy in detecting merged minutiae.

Another study examined distinguishing gender based on fingerprints taken from the SOCOFing dataset. The accuracy rate improved from 77% to 90% as the number of fingers employed for classification by the model increased. However, these results demonstrate the usefulness of fingerprint ID and how robustly CNNs analyze such data to distinguish between individuals[25].

Although the latest frameworks, including the Dual-Model Synergy method dually using VGG16 and ResNet50 in performing PAD tasks [26], or fusion-based models that use CNN features and handcrafted ridge/texture descriptors [27], have demonstrated impressive results on traditional fingerprint spoofing datasets, they do not explicitly consider non-contiguous minutiae-based double-identity attacks. Also, most of them are based on computationally intensive networks, making them unapplicable in resource-constrained or real-time systems. Domain-adaptation methods (e.g., GRU-AUNet) have already started to tackle cross-domain fingerprint spoofing problems, though they, once again, aim at contactless or sensor variability issues and not identity-merging attacks[28]. We do not overlap in that we explicitly consider the problem of double-identity spoofing with a lightweight and efficient model, which can be regarded as a fresh and applicable addition to the biometric security literature.

SOCOFing has become a popular choice among researchers due to its collection of both genuine and fake fingerprints for evaluating security-aware fingerprint classification systems.

These publications, as shown in Table 1, show the pros and cons of using SOCOFing. Distinct fingerprints can be successfully identified using SOCOFing; however, this method sometimes fails when normalized images are insufficient. SOCOFing is an effective resource for evaluating approaches to double identity detection, including situations involving discontinuous minutiae.

Table 1. Comparison of Studies Utilizing the SOCOFing Dataset

Study Title	Methodology	Dataset	Accuracy (%)	Epochs	Notable Findings
Fingerprint Classification Using Transfer Learning Technique	CNN + Transfer Learning	SOCOFing	81	50	Effective for small datasets; improved accuracy on ATVS.
Comprehensive Method for Fingerprint Classification	Gabor Filters + HOG + ML (RF, NB)	SOCOFing	81 (CNN w/o enhancement)	30	Emphasized the importance of preprocessing for better accuracy.
Enhancing Fingerprint Forensics: Gender Classification	CNN-based Gender Classification	SOCOFing	77 (single finger), 90 (multiple fingers)	25	Multiple fingers improve accuracy, but are less practical for real use.

3 Methods

3.1 MobileNet: A Lightweight Convolutional Neural Network for Efficient Image Classification

MobileNet represents a deep learning model created for effective image classification tasks within mobile and edge devices[29]. This network design reduces costs while maintaining its accuracy rates. Depthwise separable convolutions in MobileNet reduce parameter numbers while decreasing computational complexity better than standard AlexNet CNNs.

3.2 Dataset Description

The project employs the SOCOFing Dataset sourced from Kaggle. This dataset collects a set of fingerprint images designed to support fingerprint liveness detection, an indispensable security function that protects against spoofing. The SOCOFing dataset has two prominent categories, namely: Real and Altered, with

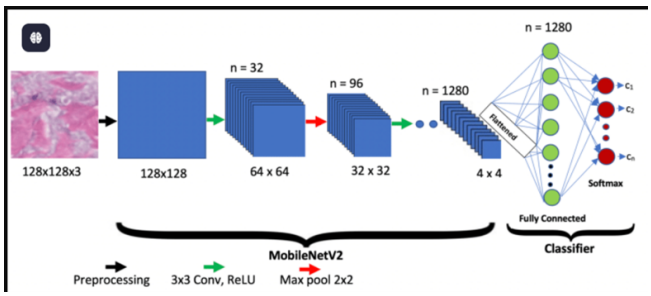

Figure 2. Architecture of MobileNet taken from [30]

an additional three elements within Altered: Altered-Easy, Altered-Medium, and Altered-Hard. Each subclass presents a unique challenge in manipulating fingerprints, which causes great complexity in the detection of life. All images are in the form of BMP (Bitmap File Header), a commonly used file header for raster graphics.

To satisfy the requirements for training as well as for evaluation, the dataset is split purposefully into three subsets: training, validation, and testing. Each subset is given training: 70%, validation: 15%, and testing: 15%. In this way, the model gets a lot of training, validation continues to closely monitor performance along the way, and the final tests are done on unseen examples to test generalization.

3.3 Description of Model

The core of the project's methodology lies in the utilization of a MobileNet architecture, a highly efficient convolutional neural network pre-trained on ImageNet. This pre-training provides the model with a strong foundation of visual feature extraction capabilities, which are further refined through fine-tuning on the specific task of fingerprint liveness detection. Fine-tuning involves adjusting the model's parameters to optimize its performance on the target dataset, thereby enabling it to effectively distinguish between real and altered fingerprints.

Figure 2 describes how MobileNetV2 is used for image classification in a deep learning process. Starting with a 128×128×3 image, the model sends the image through many convolutional layers and pooling operations, which make the spatial size smaller and the number of layers bigger. The feature map is made into a long list of numbers and processed by fully connected layers.

3.5 Key Components of MobileNet Architecture

3.5.1 Dropout Layer

To address overfitting as little as possible, dropout consists of randomly "dropping out" (setting to zero)

3.4 Algorithm For MobileNet

- Data preparation of fingerprint dataset for training and testing.
- Making a Network architecture of five layers for high-level feature extraction.
- Train the dataset to achieve effective convergence and to balance convergence, speed, and stability.
- Using optimization techniques to prevent overfitting, to achieve robustness, and to speed up computation.
- Do an Evaluation and get accuracy, loss, and precision.
- The flowchart of the Algorithm for MobileNet is shown in Figure 3.

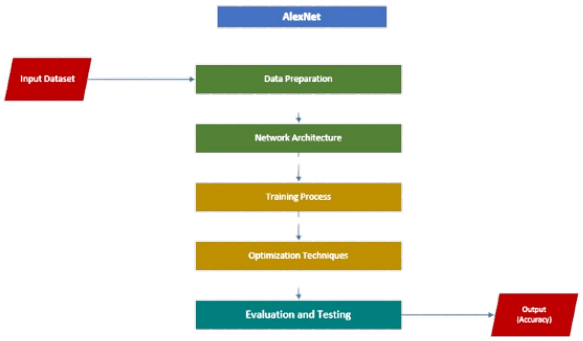

Figure 3. Algorithm of MobileNet taken from[31]

part of the neurons during training. The impact is that the network is forced not to rely on any single neuron, which shapes robustness and redundancy in ways through which the features are learned. In addition, this approach enables the network to capture larger patterns, minimizes the possibility of neurons relying on each other, and enables more robust learning.

For a given input activation h, the output after dropout is:

$$\tilde{h} = r \times h \quad \text{where} \quad r_i \sim \text{Bernoulli}(p) \qquad (1)$$

- r: binary mask vector (same shape as h), with each $r_i = 1$ with probability p and 0 otherwise.
- p: dropout keep probability (e.g., 0.5 for 50%).

To enhance the model's architecture and improve its ability to capture relevant information, several key components are incorporated [32]. Global Average Pooling is employed to reduce the spatial dimensions of the feature maps extracted by MobileNet, facilitating the integration of these features into subsequent layers. Dropout layers, with dropout rates of 0.3 and 0.2, are strategically placed to prevent overfitting, a phenomenon where the model performs well on the training data but poorly on unseen data. These lay-

ers randomly drop out neurons during training, forcing the model to learn more robust and generalized features[33].

3.5.2 ReLU Activation function

Rectified Linear Units (ReLUs) are used extensively in neural networks, and especially in deep learning, due to their simplicity and very important contribution to the performance of the underlying model. It introduces non-linearity to the model, but is very effective with computation.

Mathematically:

$$\text{ReLU}(x) = \max(0, x) \tag{2}$$

Dense layers, also known as fully connected layers, are incorporated to further process the features and generate predictions. A dense layer with 128 neurons and ReLU activation function introduces non-linearity, enabling the model to capture complex relationships within the data. The final output layer consists of 4 neurons, corresponding to the four classes in the dataset (Real, Altered-Easy, Altered-Medium, Altered-Hard), and utilizes softmax activation to produce probability distributions over the classes. This allows the model to assign a probability score to each class, representing its confidence in the classification [34].

3.5.3 Adam Optimizer

The model's training process is guided by the Adam optimizer, a popular optimization algorithm that efficiently adjusts the model's parameters to minimize the loss function. The categorical cross-entropy loss function, well-suited for multi-class classification problems, quantifies the difference between the predicted class probabilities and the true labels. Accuracy, a widely used metric, is employed to evaluate the model's performance by measuring the proportion of correctly classified samples [35].

To further enhance the model's robustness and prevent overfitting, data augmentation techniques are applied during training. These techniques involve transforming the training images in various ways to introduce variations and expand the effective size of the training dataset. In this project, data augmentation includes rescaling pixel values, random rotations, random width and height shifts, and random zooming. These transformations expose the model to a wider range of fingerprint variations, making it more resilient to unseen data and improving its generalization ability.

3.5.4 Input Preprocessing

- Images were resized to 224 × 224 pixels to match the MobileNetV2 input requirement.
- Pixel values were normalized to [0, 1] by dividing by 255.
- No flipping was applied, as horizontal or vertical flips distort fingerprint ridge patterns.

3.5.5 Data Augmentation

- Rotation range: ±10°
- Width shift: ±0.1
- Height shift: ±0.1
- Zoom range: 0.1
- Horizontal and vertical flips: not used

As of now, data augmentation has only been performed on the training set to enhance the model's generalization capabilities. Augmentation was done by randomly rotating between 10 degrees, translating in width and height by 10% each, and varying the zoom by 10%. We didn't use horizontal and vertical flipping as the transformations are not suitable for fingerprint images. The validation and test datasets were only rescaled and did not undergo any augmentation.

3.5.6 Model Architecture

- Base model: MobileNetV2 (pretrained on ImageNet)
- Input shape: (224, 224, 3)
- Fine-tuned layers: top 50 layers
- Dropout rate: 0.3
- Final dense layer: 4 units with softmax activation

3.5.7 Optimizer and Training

- Optimizer: Adam
- Initial learning rate: 1e-4
- Learning rate schedule: ReduceLROnPlateau, factor 0.5, patience 5 epochs
- Batch size: 32
- Epochs: 15

3.5.8 Experimental protocol and reproducibility

In order to be reproducible and determine the stability of results, we did N = 5 independent training runs using different random seeds (10, 20, 30, 40, 50). We used the data split (70%/15%/15%) in terms of train/validation/test as well as input preprocessing (scale to [0,1], resize 224x224) and augmentation (rotation +-10deg, widthheight shift 5, zoom 5). The MobileNet model was optimized with the Adam op-

timizer, learning rate 1e-4, batch size 32. It was decided that a maximum of 15 epochs of training will be available. An Early Stopping approach was used to avoid overfitting and to ensure good generalization by observing the validation accuracy. Training was stopped after a maximum of a few epochs when no improvement was seen in the validation accuracy, and the weights of the model with the highest validation accuracy were reloaded before the training was stopped. For the training images, a rotation range of 10° and width and height shift range of 0.1, and a zoom range of 0.1 were used. No flip around the X or Y axis was used as shown in Table 2. All experiments were performed under the same settings. This strategy guaranteed an efficient train while maintaining the best performance of the model. All main metrics (accuracy, precision, recall, F1) are also reported with mean +- standard deviation per run and per-class results, and normalized confusion matrices are also reported. Code and model.h5 are all found at Github Repo.

Table 2. Data Augmentation Parameters

Parameter	Value
Rotation Range	10°
Width Shift Range	0.1
Height Shift Range	0.1
Zoom Range	0.1
Horizontal Flip	False
Vertical Flip	False

3.6 Metrics

Following the training process, the model's performance is rigorously evaluated on the test set, which contains images that the model has not encountered during training. This evaluation provides an unbiased assessment of the model's ability to generalize to unseen data. A comprehensive set of metrics is utilized to gauge the model's performance:

3.6.1 Accuracy

Measures the overall correctness of the model's predictions.

3.6.2 Loss

Quantifies the error in the model's predictions.

3.7 Confusion Matrix

Provides a detailed breakdown of the model's performance by showing the counts of true positive, true negative, false positive, and false negative predictions for each class [36][37].

The confusion matrix is a table used to evaluate the performance of a classification model by comparing actual vs. predicted labels. It is structured as follows:

$$\mathrm{CM} = \begin{bmatrix} \mathrm{TP} & \mathrm{FP} \\ \mathrm{FN} & \mathrm{TN} \end{bmatrix}$$

where:

- True Positives (TP)
- False Positives (FP)
- False Negatives (FN)
- True Negatives (TN)

3.8 Key Performance Metrics Derived from the Confusion Matrix

3.8.1 Accuracy

Measures the overall correctness of the model:

$$\text{Accuracy} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \tag{3}$$

3.8.2 Precision (Positive Predictive Value)

Measures how many of the predicted positive cases were correct:

$$\text{Precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{4}$$

3.8.3 Recall (Sensitivity or True Positive Rate)

Measures how many actual positive cases were correctly identified:

$$\text{Recall} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{5}$$

3.8.4 F1-Score

Harmonic mean of Precision and Recall:

$$\text{F1-Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{6}$$

3.8.5 Classification Report

Presents precision, recall, F1-score, and support for each class, offering a more nuanced understanding of the model's performance across different classes.

3.8.6 ROC Curve (for multi-class classification)

Visualizes the trade-off between true positive rate and false positive rate for each class, illustrating the model's ability to discriminate between classes [38].

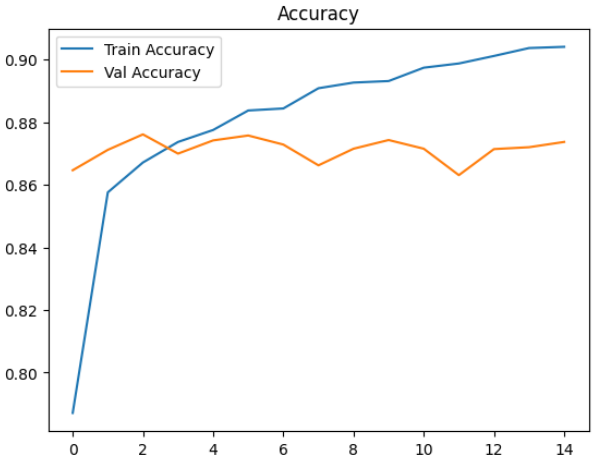

Figure 4. Accuracy chart achieved after training the model

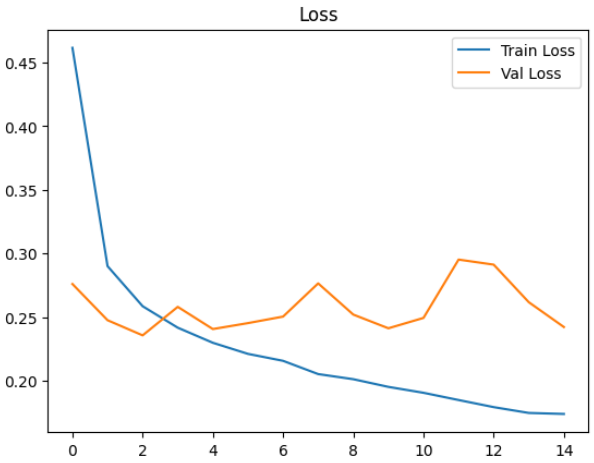

Figure 5. Loss chart achieved after training the model

4 Results

4.1 Environmental Parameters

The Kaggle Notebook environment is used for the project, using a P100 GPU, and it depends on TensorFlow/Keras and Python for the development. Using libraries such as TensorFlow, keras, kagglehub, os, shutil, random, matplotlib, pyplot, seaborn, numpy, and sklearn, the project manages data, develops models, and visualizations.

4.2 Model Evaluation

4.2.1 Training Accuracy and Loss

4.2.2 Accuracy

A test accuracy with a 5 runtime was

- 0.8713527917861938
- 0.8613455295562744
- 0.8665300011634827
- 0.8705087900161743

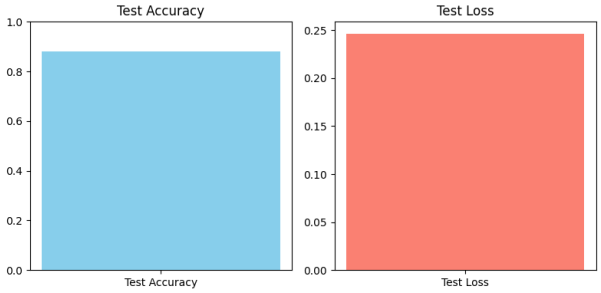

Figure 6. Testing Accuracy and Loss Chart

- 0.8795514702796936

also Mean Accuracy: 0.8699 and Std Dev: 0.0060 were recorded, indicating the overall success of the model in fingerprint image classification for authenticity/tampering.

4.2.3 Loss

Test loss 0.2463 recorded indicates the performance of the model on minimizing prediction errors.

4.2.4 Confusion Matrix

By analyzing the confusion matrix, we could view the model's predictions for each class in detail, such as indices of true positives, true negatives, false positives, and false negatives. The confusion matrix analysis showed that most misclassifications were between the Altered-Medium and Altered-hard classes. This observation indicates that these classes are close in ridge distortions and structural properties and hence hard to distinguish. The Real and Altered-Easy classes, on the other hand, had significantly high classification accuracy because of their unique fingerprint patterns. The results suggest that further research is needed to enhance the feature extraction process for fingerprints that are highly distorted. By way of this analysis, we could discuss the behavior of the model in different classes and identify areas for further improvement as shown in Figure 7.

4.2.5 Classification Report

The classification report presented precision, recall, F1-score, and support for all classes, thus providing the evaluator an opportunity to analyze the model's performance for each of the categories. The metrics demonstrated information about the performance of the model on different classes, allowing the model to be targeted for alterations to improve its accuracy as shown in Table 3. The test accuracy of the model was found to be 88% in 5 runs. Per-class recall values were [Altered-Easy=0.99 +- 0.02, Altered-Hard=0.77 +- 0.03, Altered-Medium=0.81 +- 0.02, Real=0.99

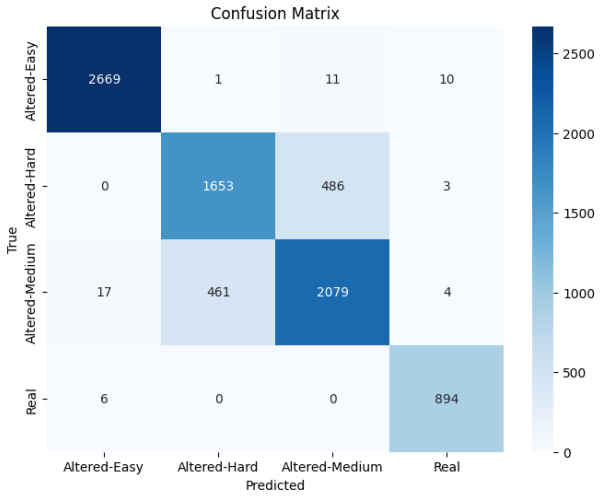

Figure 7. Confusion Matrix obtained after Testing

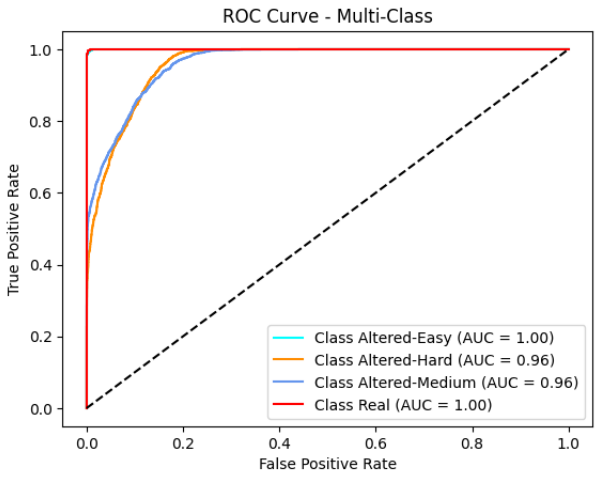

Figure 8. ROC Curve

Table 3. Classification Report for Fingerprint Class Detection

Class	Precision	Recall	F1-Score	Support
Altered-Easy	0.99	0.99	0.99	2691
Altered-Medium	0.81	0.81	0.81	2561
Altered-Hard	0.78	0.77	0.78	2142
Real	0.98	0.99	0.99	900
Accuracy			**0.88**	**8294**
Macro Avg	0.89	0.89	0.89	8294
Weighted Avg	0.88	0.88	0.88	8294

+- 0.02]. The hard alteration class had lower recall as demonstrated by the normalized confusion matrix as shown in Figure 7, which was expected, as the difficulty increased. The Total Trainable Parameters were 3,360,580, 38.64 MB of model file, and 62.87 ms of an average inference time per image on P100.

4.2.6 ROC Curve (Multi-class)

The ROC curve supported the discriminative capabilities of the model to assess the true difference between the real and synthetic fingerprints. By combining AUC values for each class, we were able to quantify the model's effectiveness, which further attests to its ability to identify live fingerprints as shown in Figure 8.

The results of the ROC analysis show very good discrimination results at each fingerprint class. The Real and Altered-Easy classes had an AUC of 1.00, representing almost perfect separation from the other classes. Even more complex and heavily altered fingerprints achieved both an AUC of 0.96 in both Altered-Medium and Altered-Hard classes, yet they are still relatively easier to classify than the simpler classes. In conclusion, these findings are in line with the findings of the proposed MobileNet-based framework, which performs very accurately and consistently in recognizing real and altered fingerprint images, as shown in Table 4

Table 4. AUC Scores for Fingerprint Class Detection

Class	AUC
Real	1.00
Altered-Easy	1.00
Altered-Medium	0.96
Altered-Hard	0.96
Average	**0.92**

5 Discussion and Comparison

This paper has tested a MobileNet-based model to detect non-contiguous minutiae alterations in the SOCOFing fingerprint dataset. In general, the model was excellent in both the Real and Altered-Easy classes, suggesting that light or simple modifications could be detected using the transfer learning. Nevertheless, the fact that the accuracy of the Altered-Medium and Altered-Hard groups is smaller implies that it has significant drawbacks that must not be overlooked. Such patterns are normally more complex changes, e.g., ridge perturbations, more faithful synthetic perturbations, or partial obliteration, that might not be fully represented by MobileNet. As such, the present results cannot be seen as the fact that the model is resistant to any kind of advanced alteration or spoofing.

Another reason is that of the SOCOFing dataset in itself. The distorted fingerprints in SOCOFing, though being very popular, are artificially produced by a set of predetermined distortion algorithms. Though these synthetic changes can be experimented with under control, they may not be a true representation of what happens in reality, including physical abrasion, chemical modification, deliberate ridge transplant, or sensor noise behaviour. As a result, the results might not correspond to the functionality of real-world systems, and cross-dataset validation is crucial before implementation.

In spite of these shortcomings, the model has two outstanding strengths. The first one is that MobileNet offers lightweight inference, which means that it can be used in a system with limited hardware capabilities, including edge devices or embedded biometric systems. Second, the training pipeline is simple and computationally efficient, and it can allow quick experimentation and may also be used in real-time fingerprint authentication systems.

These findings also indicate a number of areas of improvement. Recently, MobileNetV3, EfficientNet-Lite, and MobileOne were shown to achieve good performance in the area of biometric recognition and presentation attack detection. To enhance efficiency, MobileNetV3 uses a neural architecture search and a squeeze and excitation model [39]. EfficientNet-Lite achieves a balance between performance and efficiency by applying compound scaling [40], while MobileOne adopts structural reparameterization for deployment in real time [41]. The above architectures have not been tested in this work, but are good directions for further research and could be used to further enhance the identification of complex fingerprint alterations.

All in all, the model exhibits good baseline performance on the simple and moderately altered fingerprints, but more improvements are needed to handle the highly complex alteration attacks and guarantee the generalizability to synthetic datasets.

Here are two research works compared with this research work that all use the same dataset (SOCOFing (Sokoto Coventry Fingerprint Dataset)) to classify fingerprints, so that one can compare the techniques and results used.

The first work, Fingerprint Classification Using Transfer Learning Technique, is a CNN trained with Transfer Learning, which involves fine-tuning a pre-trained model with fingerprint data. It was found that the longer the training, the higher the accuracy, even though it has been trained for 50 epochs, yielding an accuracy of 81%, which is not a sign of low performance!

In the second study, Comprehensive Method for Fingerprint Classification, a more traditional hybrid approach is used by extracting texture using Gabor Filters and shape features with a HOG (Histogram of Oriented Gradients), which are then given as input for classical machine learning models such as Random Forest and Naive Bayes. They report an 81% accuracy, which is actually for their baseline CNN without enhancements, and trained for 30 Epochs. The point of this study is that they demonstrate that well-architected traditional features can be competitive to deep-learning baselines.

This research, called An Innovative Method for Detecting Double Identity Fingerprints, takes a novel approach and applies a lightweight deep learning architecture, originally developed for mobile and resource-constrained systems, to the problem of double identity fingerprint detection. It was also found to have the highest accuracy of 87% in fewer epochs, 15, than either of the other three studies. This shows the efficiency and effectiveness of MobileNet for fingerprint classification tasks.

Overall, the Table 5 shows that the MobileNet achieved better results than the CNN with Transfer Learning and the hybrid traditional approach, with a much lower training time. It indicates that the training time is not the most important aspect of the architecture and that lightweight architectures, such as MobileNet, can produce better results even if they perform fewer calculations.

Table 5. Comparison of Methods for Fingerprint Classification Using the SOCOFing Dataset

Study Title	Methodology	Dataset Used	Accuracy (%)	Epochs
Fingerprint Classification Using Transfer Learning Technique	CNN + Transfer Learning	SOCOFing	81	50
Comprehensive Method for Fingerprint Classification	Gabor Filters + HOG + ML (RF, NB)	SOCOFing	81 (CNN w/o enhancement)	30
An Innovative Method for Detecting Double Identity Fingerprints from Non-Contiguous Minutiae-Based Attack Techniques	MobileNet	SOCOFing	87	15

6 Conclusion and Future Work

The Transfer learning model known as MobileNet was used to identify both genuine and false altered individual fingerprints in the SOCOFing dataset. The dataset was separated into four classes. Real images, Altered-Easy, Altered-Medium, and Altered-Hard. To train the model dataset was split into 70% for Training, 15% for Validation, and 15% for Testing. Data Augmentation was used to improve generalization while preserving the natural characteristics of biometric data. After training the MobileNet model over 15 epochs, the model was found to be 88% in general accuracy, thus showing that lightweight architectures can be used to classify unaltered and slightly modified fingerprints. Nevertheless, the decline in performance in the case of medium and hard alteration levels suggests that more advanced spoofing patterns have not yet been easy for MobileNet. As such, the outcomes can be viewed as an encouraging benchmark instead of an all-purpose answer to non-contiguous minutiae attacks of high complexity.

The results indicate that further research on three dimensions should be conducted: (1) testing on various real-world datasets to enhance the generalizability, (2) testing innovative architectures, including MobileNetV3, EfficientNet-Lite, or hybrid CNN-

Transformer models, and (3) combining conventional feature-based fingerprint analysis with deep learning. Future studies that consider these factors could result in more valid systems of detection in order to deal with a wide spectrum of alteration methods.

In short, although the suggested approach has a potential in resource-constrained biometric systems, further refinement and cross-dataset testing are needed before it is possible to be deployed in real operational settings.

7 Data Availability Statement

The dataset used in this study, the SOCOFing fingerprint dataset, is publicly available on Kaggle at the following link: Kaggle.

8 Funding

No external funding was received for this research.

9 Conflicts of Interest

The authors declare no conflict of interest regarding the publication of this work.

10 Ethics, Consent to Participate, and Consent to Publish Declarations

Not applicable. In this paper, publicly available and anonymized fingerprint images (SOCOFing dataset) were used. No human subjects or subjects of interest were recruited, and no personally identifiable information was gathered.

11 Code Availability Statement

The source code to be used to train and test the MobileNet-based fingerprint classification model, including preprocessor and augmentation scripts as well as plotting script, will be shared publicly at Github Repo, when it is published.

References

[1] A. Jain, Lin Hong, and R. Bolle. On-line fingerprint verification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19(4): 302–314, 1997. .

[2] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer London, 2 edition, 2009. ISBN 9781848822535. . URL https://doi.org/10.1007/978-1-84882-254-2.

[3] S. Pankanti, Salil Prabhakar, and Anil Jain. On the individuality of fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24:1010– 1025, 09 2002. .

[4] Carsten Gottschlich and Stephan F. Huckemann. Separating the real from the synthetic: Minutiae histograms as fingerprints of fingerprints. *IET Biometrics*, 3(4):291–301, April 2013. . URL https://doi.org/10.1049/iet-bmt.2013.0004.

[5] Arun Ross, Jidnya Shah, and Anil K. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29 (4):544–560, May 2007. . URL https://doi.org/10.1109/TPAMI.2007.1004.

[6] Patrizio Campisi. *Security and Privacy in Biometrics*. Springer London, 2015. ISBN 9781447167215. . URL https://doi.org/10.1007/978-1-4471-6722-2.

[7] Cai Li and Jiankun Hu. Attacks via record multiplicity on cancelable biometrics templates. *Concurrency and Computation: Practice and Experience*, 26, 06 2014. .

[8] Jun Feng and Anil K. Jain. Fingerprint reconstruction: From minutiae to phase. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(2):209–223, February 2011. . URL https://doi.org/10.1109/TPAMI.2010.59.

[9] Kai Cao and Anil K. Jain. Learning fingerprint reconstruction: From minutiae to image. *IEEE Transactions on Information Forensics and Security*, 10(1):104–117, January 2015. . URL https://doi.org/10.1109/TIFS.2014.2368356.

[10] V. S. Baghel and S. Prakash. *Digital Image Security*. CRC Press, 2024.

[11] Soweon Yoon and Anil K. Jain. Longitudinal study of fingerprint recognition. *Proceedings of the National Academy of Sciences*, 112(28):8555–8560, 2015. . URL https://doi.org/10.1073/pnas.1417220112.

[12] Shi Xuanbin, Jun Feng, Jie Zhou, and Yilong Luo. Detection and rectification of distorted fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 37(3):555–568, March 2015. . URL https://doi.org/10.1109/TPAMI.2014.2353647.

[13] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, January 2001. . URL https://doi.org/10.1147/sj.403.0614.

[14] Emanuele Marasco and Arun Ross. A survey on antispoofing schemes for fingerprint recognition systems. *ACM Computing Surveys*, 47(2):1–36, November 2014. . URL https://doi.org/10.1145/2656334.

[15] Konstantinos Karampidis, Minas Rousouliotis, Euangelos Linardos, and Ergina Kavallieratou. A comprehensive survey of fingerprint presenta-

tion attack detection. *Journal of Surveillance, Security and Safety*, 2:117–161, 2021. .

[16] Anuj Agarwal et al. Deep learning based fingerprint presentation attack detection: A comprehensive survey. *arXiv preprint arXiv:2305.17522*, 2023.

[17] Abdulaziz A. Alshdadi et al. Enhancing fingerprint liveness detection accuracy using deep learning: A comprehensive study and novel approach. *Journal of Imaging*, 9(8):158, 2023. .

[18] Hailin Li and Raghavendra Ramachandra. A survey on deep learning techniques for fingerprint presentation attack detection. *Sensors*, 26(4), 2026. ISSN 1424-8220. . URL https://www.mdpi.com/1424-8220/26/4/1283.

[19] Sai Venkatesh, Raghavendra Ramachandra, Karthik N. Raja, and Christoph Busch. Face morphing attack generation & detection: A comprehensive survey. *IEEE Transactions on Technology and Society*, 2(3), September 2021. . URL https://doi.org/10.1109/TTS.2021.3110099.

[20] Michele Ferrara, Riccardo Cappelli, and Davide Maltoni. Detecting double-identity fingerprint attacks. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 5(4):476–485, 2023. . URL https://doi.org/10.1109/TBIOM.2023.3258442.

[21] Kai Cao and Anil K. Jain. Automated latent fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41 (4):788–800, April 2019. . URL https://doi.org/10.1109/TPAMI.2018.2855026.

[22] Haoxiang Zhang, Raghavendra Ramachandra, Karthik N. Raja, and Christoph Busch. Generalized single-image-based morphing attack detection using deep representations from vision transformer. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pages 1510–1518. IEEE, 2024.

[23] A. H. Aloweiwi. Fingerprint classification using transfer learning technique. Master's thesis, Montclair State University, New Jersey, 2021. Available at DIGITAL COMMONS.

[24] F. M. Jasem, I. T. Ahmed, and B. T. Hammad. A comprehensive method for fingerprint classification based on gabor filters and machine learning. *International Information and Engineering Technology Association*, 4(6):1775–1782, December 2024.

[25] A. Spanier, D. Steiner, N. Sahalo, and Y. Abecassis. Enhancing fingerprint forensics: A comprehensive study of gender classification based on advanced data-centric ai approaches and multi-database analysis. *Applied Sciences*, 14(1): 417, 2024. . URL https://doi.org/10.3390/app14010417.

[26] Debanjan Roy, Abhishek Bhowmick, Faria Ahmed, Md Jahid Hossain, and Md Mahfuzur Rahaman. Dual-model synergy for fingerprint spoof detection using vgg16 and resnet50. *Journal of Imaging*, 11(2):42, 2025. .

[27] Ricardo Rodrigues, Jason Jermyn, and Stephanie Schuckers. Dyffpad: Dynamic fusion of convolutional and handcrafted features for fingerprint presentation attack detection. *IEEE Transactions on Information Forensics and Security*, 18: 3505–3518, 2023. .

[28] Yifan Xu, Shiqi Liu, Yan Fang, and Zheng Wang. Gru-aunet: A domain adaptation framework for contactless fingerprint presentation attack detection. *arXiv preprint arXiv:2504.01213*, 2025.

[29] A. Kumar, D. Dembla, S. Tinker, and S. B. Khan. *Handbook of Deep Learning Models for Healthcare Data Processing-Disease Prediction, Analysis, and Applications*. CRC Press, 2025.

[30] Metin Akay, Yong Du, Cheryl Sershen, Minghua Wu, Ting Chen, Shervin Assassi, Chandra Mohan, and Yasemin Akay. Deep learning classification of systemic sclerosis skin using the mobilenetv2 model. *IEEE Open Journal of Engineering in Medicine and Biology*, PP:1–1, 03 2021. .

[31] S. Belaqziz, S. E. Hajjami, H. Amellal, R. Lahmyed, L. Koutti, B. Abdellah, and I. U. Khan. *Smart Applications of Artificial Intelligence and Big Data*. CRC Press, 2025.

[32] H. L. Gururaj, F. Flammini, V. R. Kumar, and N. S. Prema. *Recent Trends in Healthcare Innovation*. CRC Press, 2025.

[33] Z. Li, B. Gong, and T. Yang. Improved dropout for shallow and deep learning. arXiv preprint arXiv:1607.01799, 2016. URL https://arxiv.org/abs/1607.01799.

[34] A. M. Javid, S. Das, M. Skoglund, and S. Chatterjee. A relu dense layer to improve the performance of neural networks. In *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, June 2021.

[35] Z. Zhang. Improved adam optimizer for deep neural networks. In *2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)*. IEEE, June 2018.

[36] A. Arias-Duart, E. Mariotti, D. Garcia-Gasulla, and J. M. Alonso-Moral. A confusion matrix for evaluating feature attribution methods. In *Proceedings of the 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, June 2023. URL https://www.researchgate.net/publication/

373134015_A_Confusion_Matrix_for_Evaluating_Feature_Attribution_Methods.
[37] P. Nandal, M. Dahiya, M. Singh, A. Dagur, and B. Kumar. *Progressive Computational Intelligence, Information Technology and Networking*. CRC Press, 2025.
[38] H. Dong. *Data Analytics in Finance*. CRC Press, 2025.
[39] Andrew Howard et al. Searching for mobilenetv3. *Proceedings of ICCV*, 2019.
[40] Ming Tan and Quoc Le. Efficientnet: Rethinking model scaling for convolutional neural networks. *ICML*, 2019.
[41] Pavan Kumar Vasu et al. Mobileone: An improved one millisecond mobile backbone. *CVPR*, 2023.

Muhammad Sufyan The Author was born in Jhang, Pakistan, in 2002. He received the degree of B.S. in computer science from Lahore Garrison University, Lahore, in 2025. His research interests include biometrics, deep learning, and fingerprint recognition systems. He has worked on projects related to smart traffic management systems, image classification, bone fracture detection, crop disease detection, and biometric security.

Khushbu Khalid Butt The author received her B.S. (Hons) in Computer Science from Government College University Lahore, Lahore, Pakistan, in 2014. She also won a scholarship to go to Huazhong University of Science and Technology to study in China for her M.S. program in 2015, where she finished in 2017, and studied Mandarin Chinese along with networking security. The same year, she was awarded a second scholarship, this time to study her PhD at the same university, focusing on image encryption, and she finished her studies in 2023. From 2021 to 2022, she served as a lecturer at Lahore Garrison University and resumed her role as Assistant Professor upon completing her PhD. She has published over 15 articles and co-authored articles in highly respected international journals and conferences. She is interested in research related to network security, image encryption, cryptography, and Information security.

Tahir Alyas (Senior Member, IEEE) received his Ph.D. in Computer Science in 2018 and currently serves as the Director ORIC and Associate Professor of Computer Science at Lahore Garrison University. He is an Oracle Certified Cloud Infrastructure Architect with research interests spanning AI, ML, Cloud Computing, Cloud Security, Federated Learning, XAI, Blockchain, and IoT systems. He has published 50+ Papers in Q1/Q2 international journals, including Scientific Reports, IEEE Access, CMC, Sensors, and Applied Sciences, and continues to lead research in intelligent and secure computational frameworks.

Omer Irshad is an Assistant Professor at Lahore Garrison University (LGU), a Ph.D. holder in Computer Science with a rich background in academic and professional pursuits in the field of data science and software engineering. His primary research areas are genetic data integration and modeling, semantic data modeling, and advanced computational techniques for complex biological and semantic data analysis. He has published and co-authored several research papers in good-quality journals, which are contributing to these fields. Outside of the academic realm, he has a few years of experience in software industry, which enables him to connect theory with practice. His research focus is on novel data modelling approaches that enable efficient knowledge modelling, knowledge integration, and knowledge-based decision making. This is expertise in a variety of multidisciplinary fields, and has an important impact on research and industry.

Umer Iqbal was born in Gojra, Punjab, Pakistan, and obtained his Bachelor's Degree in Mathematics from Government College University Faisalabad (2008-2012) and his M.S. Degree in Mathematics from HITEC University (2012-2014), with a Gold Medal. After obtaining his PhD in Information Technology from the University Tun Hussein Onn Malaysia in 2018, he took up the position of Assistant Professor at Riphah International University from 2018 to 2022. He served as a Product Manager at Techrydes, bringing industry experience in product strategy, software development management, and coordinating stakeholders to the table to connect the dots between academia and the real world from 2022 to 2024. He returned to Riphah International University, Faisalabad Campus, in June 2024 as an Associate Professor and to Lahore Garrison University on July 1, 2025, as Head of the Department of Information Technology and Assistant Professor. He has published and co-published over 21 research papers in international journals and conferences in the fields of Data Mining, Neural Networks, Network Security, Machine Learning, and Artificial Intelligence.