Comprehensive Fingerprint Recognition Utilizing One Shot Learning with Siamese Network

by

Sara Milham Zaman
19101141
Md. Abir Hasan
18201019
Md. Rafid Sadat
22341053
Md. Abrar Haque
19101648

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
January 2023

© 2023. Brac University
All rights reserved.

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Sara Milham Zaman

19101141

Md. Abir Hasan

18201019

Md. Rafid Sadat

22341053

Md. Abrar Haque

19101648

Approval

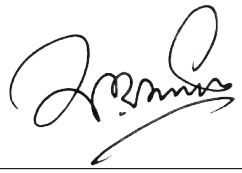
The thesis/project titled "Comprehensive Fingerprint Recognition utilizing One Shot Learning with Siamese Network" submitted by

1. Sara Milham Zaman (19101141)
2. Md. Abir Hasan (18201019)
3. Md. Rafid Sadat (22341053)
4. Md. Abrar Haque (19101648)

Of Fall, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January 19, 2023.

Examining Committee:

Supervisor:
(Member)



Faisal Bin Ashraf

Lecturer
Department of Computer Science and Engineering
Brac University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD

Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD

Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

Detailed Fingerprint investigation has been a dominant law enforcement tool which is utilized to distinguish suspects, settle crimes and violations for over 100 years. Moreover, gender classification from fingerprints is a vital step in forensic anthropology in order to identify a criminal's gender and reduce the list of suspects. A novel approach of machine learning (ML) which is One Shot Learning has been introduced in this report for identification of persons which will implement the Siamese learning approach for training fingerprint samples by using the triplet loss. One Shot Learning has shown to be efficient because it reliably performs with only one labeled training example and one or a few training sets. Moreover, by using Transfer Learning with EfficientNetV2S an accuracy of 99.80%, 99.73%, 97.09%, 99.66%, 98.61% for identification of person, gender, hand, finger and detection of forge fingerprints has been achieved on the Sokoto Coventry Fingerprint Dataset.

Keywords: Fingerprint; One Shot Learning; Siamese learning; Machine Learning; Transfer Learning; Triplet loss; EfficientNetV2S ; SOCOFing Dataset.

Dedication

All praise in the name of the Almighty, we show our eternal gratitude to our creator for giving us guidance, wisdom and giving us a healthy life. We dedicate this book to the Almighty Allah.

And last but definitely not the least we want to dedicate our thesis to our adoring parents. Without our parents' ongoing support, it might not be possible. We owe a debt of gratitude to them for sacrificing their comfort for our well being. It is also dedicated to our teachers, friends and to our well wishers who motivated us in our ways and prayed for our success.

Acknowledgement

First and foremost, glory be to the Great Allah, with whose help we were able to finish writing our thesis without too many setbacks.

Second, we deeply appreciate our thesis supervisor Mr. Faisal Bin Ashraf for continuously encouraging and guiding us during the last year, and also for being there for us whenever we needed him even though he was not in Bangladesh. Working under his supervision has been very enjoyable and we have learned and grown a lot.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this era of modern technology, the need to authenticate any system is paramount and the implementation of authentication through bio-metrics is being developed progressively. With the advent of IoT and digitization, the approach of identifying individuals is becoming more and more important. Therefore, arises the need for fingerprints, palm prints, facial recognition and more approaches. But to learn about them, we should at least learn the procedural implementations of ideas that gave output to such authentication methods. Bio-informatics, bio-metrics are the terms inter-related with each other as well as with fingerprint identification.

1.1 Bio-informatics

The world is a diverse place getting enriched with the introductions of many species discovered as days are passing by. With the discovery of new lives, it is an untold necessity to store information about them. However, with the growing number of species, the number of data sets storing such information is getting larger, resulting in the need of utilizing various computational methods that can address this issue.[57] Thus, came the idea known as Bio-Informatics. This concept includes biological data along with both computer science and information technology. With the combined efforts put up by three scientific fields, the problems with data complexity and others were addressed.This bio informatics deals with data that are gathered through biometric means or biometric data. These data require AI to handle properly[23].

1.2 Brief on Biometrics Technology

Biometric technologies are derived from the concept of Bio-informatics. In many ways, bio-informatics is the broader term and biometrics is dependent on this ideology as biometric deals with physical traits of an individual. Biometric technologies are popular in term of digitized and autonomous authentication system. The approach is able to uniquely identify an individual person, taking into account the unique characteristics of a person for instance their behavioral, as well as psychological traits [6].Biometric technologies verify a person uniquely and anonymously by connecting their biometric pattern, personal information and behavioral traits to the individual's biometrics. This way the person can be identified through a

digital process[3]. Thereby, it is quite understandable why the process is related to computers and such digital approaches. Biometric technologies include methods like collecting a person's fingerprint, palm-print, facial structure and more to uniquely identify an individual. Such statistical technique gives out the identification as a form of digitized data which is used in the authenticated process. In our paper, the focus is on fingerprint recognition which has the most unique features and varies from person to person.

1.3 Fingerprint Recognition

Utilization of an individual's fingerprint in terms of unique identification is not a later technology, to the contrary, the method is being using for decades in various sectors. The grounds behind the strengths of fingerprint lie behind the physical structure of our fingers. For decades, through scientific investigation and microscopic visualization, the fact that each finger contains different pattern of ridges and furrows has been revealed. Moreover, the magnificence of each person has different patterns (actually, no two person in the entire world do not have similar fingerprints, even identical twins have different fingerprint patterns) can statistically identify any person and detect their identity[1], [31]. Moreover this form of bio-metric technology has a widespread of uses as well. For instance, in context of Bangladesh, bio-metric fingerprints have been associated with driving licenses, passports, NIDs, offices, medical centers, attendance in various academic institutions, verifying ownership, transactions, withdrawal process, smart devices, smartphones, laptops, personal computers, home security installation and many more. Fingerprint has been the most valuable digital data which can derive a person's identity, financial information and other sensitive necessary information as well. Using fingerprint identification, many criminals have been identified, or at least, the process of finding criminals has been easy. In police investigations, the ability to identify a person's gender can easily narrow down the elaborate process of narrowing down the identification process. It goes without saying that fingerprint identification in this regard has been a much needed helping hand as through fingerprint identification, the gender of a person can be identified easily and with luck, all the digital information of a criminal associated with their fingerprint is traceable as well [12], [42].

1.4 Brief On the Aim of Our Research

Since fingerprint is associated with various digital accessories, it's also easy to exploit loop holes of the technology through spoof fingerprinting. Hence, falling these data into wrong hands can cause massive danger to an individual[34]. Besides, methods for finding the data involves large data sets and complexity, which requires strong methods. In our paper we have shown methods used by other researchers throughout the years using deep convolutional neural network, RT method and so on, However, in our paper we will be proposing a method combining the technology of one shot machine learning as well as Siamese learning network. One shot learning method can extract data while eradicating the complexity of any form of data sets. Besides, even if the data sets lack in features, the algorithm will work fine. The implemen-

tation of Siamese learning model will help the data sets training phase. Using the one shot method, the the large data set, no matter how complex, can easily be incorporated since one shot simplifies the verification process. Moreover, the Siamese network will handle input similarities and make sure the output is accurate. By implementing these methods successfully, an individual person's gender and other relevant information can be derived from the recognition of fingerprints which will help in tackling fingerprint spoofing and help in other sectors like the forensic process, medical authentication and more. By implementing mentioned procedures, we will try to validate, verify and ensure privacy through fingerprint recognition while proposing a cost effective system which can be implemented in various sectors.

1.5 Research Problem

Among many scientific technological inventions, Artificial Intelligence allow a machine to imitate the learning process of humans without being unequivocally customized every single time. In order to detect and identify the distinct characteristics which make an individual different from others, Machine learning offers some novel approaches to solve difficult bio-metric problems which provides top notch accuracy for bio-metric identification. Fingerprint is one of the most effective biometric modalities because of the convenience and robustness of this feature. However, a study [32] found that the number of verification steps is proportional to the database's size. Thus to deal with this issue, One Shot Learning has been used in this paper. If testing is done with few sample images then the system will acquire better efficiency as this One Shot Learning model not only utilizes small labeled samples but also this framework easily gets adapted with new samples which are not studied earlier [55]. Additionally, to upgrade and refine and handle computational expenses, Siamese Network is being incorporated along with One Shot Learning. Thus, the main purpose of using Siamese Network is to address Neural networks for having a strong knowledge of similarity learning [44].

1.6 Research Objectives

To develop a detailed recognition of fingerprints using one shot learning which will handle and classify massive data sets and reduce the computation expenses utilizing the Siamese network, is the main objective of our proposed paper. Using the Siamese network, we will train our data set and for testing we will use a novel architecture which is one shot learning in order to do the fingerprint classification. The problems that will be addressed from this research paper are:

Bio-metric Validation: Bio-metrics is a viable innovation utilizing which human's Behavioral and physiological attributes are identified [4]. One of the fascinating applications of bio-metric modality is to identify the distinct features of fingerprints which are not easily changeable. To identify an individual voice, gender, fingerprint, footprint are the discriminant features [31]. Meanwhile, among those discriminant features, fingerprints play a vital role for identifying the distinctive features. In this paper, we will propose a model which will identify gender, hand, finger and forge fingerprints with a high accuracy.

Security: The need of bio-metric authentication for any security purpose is very vital and fingerprint is the most extensively used bio-metric modality [42]. Our model will assist in differentiating and classifying gender on the basis of the fingerprint and the distinctiveness of the fingerprint features will help to limit the time to recognize a suspect. Additionally fingerprint identification is one of the most well grounded identification processes which is acceptable in law. Thus, this model will be very useful for the forensic investigators to shorten the suspect list in a short amount of time and accelerate the identification process. Moreover, with our proposed model, it will be able to identify forge fingerprints precisely and thus improve security system

Verification: Fingerprinting is the widely used identification sector because of the robustness in comparison with the traditional methodologies. The distinct features of fingerprints help to distinguish between the age and gender of an individual [1]. In order to speed up forensic investigation, reduce the threat of forging, authentication of mobile devices, home security system the verification of fingerprinting is very vital. Moreover, industries and companies are getting digitalized day by day and by using One Shot Learning we can easily identify the employee and also simply add new employees in the database without training the whole model all over again.

Cost Effectiveness: Verification is the need of any protected framework and one of the most frequently used verification systems. One of the most useful features of fingerprint detection using one shot learning is cost effectiveness. This proposed model will guarantee feature extraction, high accuracy of identification and easy decision making which can be applied to large data sets of images in a short period of time [51]

Chapter 2

Literature Review

Verification is the need of any protected framework and as discussed earlier, to be able to investigate criminal offenders, Fingerprint detection has significant importance. Among many of the investigating and detection techniques, One Shot Learning will give better interpretation and accuracy in detecting gender and fingers of the hand. However, a number of past papers have implemented different machine learning algorithms to classify and recognize an individual's unique palm and finger patterns which also gave a moderate accuracy. Thus in order to perceive scope of further research some of the research papers have been summarised below:

2.1 Related Work

Among many of the biometric modalities, Fingerprint is the most widely used. It has been more than a century since people use fingerprints for identification. Fingerprints are eccentric patterns that are not changeable [31]. As fingerprints of a person are a unique marker, this biometric modality is one of the best techniques for tracking crime offenders.[42]. Moreover, to shortlist the suspects of crime, gender classification by taking fingerprints is one of the best proven methods in many researches. So detailed fingerprint identification will help the crime department to decrease the counterfeiting threat [5]. The authors of [45] in their research paper proposed CNN and Transfer learning in order to identify the fingers classification, hand and gender. Their proposed model because of the promising result was used in SOCOFing corpus. Their model learns the features for gender classification with CNN and by the incorporation of transfer learning the CNN classifier works faster [15]. With the implementation of both CNN and transfer function, the model learns the feature for classification by taking fingerprint image information into consideration to provide precise results [detailed identification]. Precisely, this paper utilizes ResNet model that is trained on ImageNet which acts like a source domain and then adjust the model to the domain of classification of fingerprints. However, the proposed model achieved around 75.2% accuracy for the classification of gender and around 76% accuracy for fingers classification which need to be improved. The accuracy result for the identification of the hand is very high which is around 93.5%. Thus there's a scope for improvement in the classification of gender and hand.
Many studies were conducted in order to upgrade the identification and classification of fingerprints since biometrics is one of the most effective technologies for identifying behavioral characteristics in order to authenticate [4]. In [61], few shot learning

palm-print acknowledgment algorithms with the implementation of Meta-Siamese Network have upgraded the exactness and robustness of identification results to a better accuracy by implementing only few images for testing. Because of using few shot learning and testing few images for palm print recognition, investing huge amounts of time to label and train samples were resolved. To ensure personal security and for gathering individuals' palm print which will split the data set with the purpose of training and testing was also corrected by the utilization of few shot learning. Therefore, the authors of [61] proposed a few shot learning by implementing Meta-Siamese Network for palm-print recognition in a small sample of data. To construct the proposed model, the image data set is split into a training and testing set in 1:1 ratio randomly. In order to evaluate, the model used 15 distinct unconstrained and constrained subsets for the recognition task. Then the images are resized and incorporated into networks. The whole experiment was conducted using the PyTorch framework. After the experiment, the results for different settings exceed around 99%. So, the main purpose of this article was to train a classifier using few shot learning in order to identify a few labeled images in the testing phase for each of the categories. However, if the classifier using the conventional optimization algorithms was directly trained because of the shortage of labeled data, the model would have faced over-fitting issues and the model would not have gained acceptable results. That is why meta learning was proposed [30]. The model proposed by the authors of [61] have outperformed all other methods of the state of the art and set a benchmark for palm-print database for both constrained and unconstrained databases.

A variety of biometric recognition systems are being used in the identification sector because of the convenience and robustness of using those identification systems due to the guaranteed high accuracy results. However, these systems are also not spared from the baleful attacks. These attacks faced by the system are of two types, direct attack and indirect attack [28]. The most common attack is the direct attack because no information is needed to do the attack. However, to recognize the fingerprint sensor device with simple and subtle handy tools are done. Conversely, the indirect attack requires extensive knowledge regarding the system's module. That is why researchers had keen interest to build a system which can evaluate liveness of fingerprints and detect any spoofing activities and provide optimal solutions. Alqahtani and Zagrouba [51] in their paper aimed to review different research papers which differentiate original and altered fingerprint images utilizing different ML algorithms and have also tried to scrutinize different schemes. In order to be able to differentiate between real and fake images, the most crucial thing is to understand the features of the image. Nevertheless each feature has different characteristics proposed by different studies [43]. On the basis of general features, fingerprint can be split into three levels which are Global level, Local level and detail level [41]. On the basis of some specific metrics, the comparison between different data-sets were made. To improve accuracy, a combination of various data-sets were utilized in the training period. The output of this research work have found that the SVM was extensively utilized as a classifier. Moreover, BFIF, LPQ are the extracted features in nearly all of the cases. Additionally the data-sets LivDet2013, LivDet 2011 were implemented in the training and testing phase in most of the reviewed research papers than other data-sets.

One of the systems that engage directly with the user, who will be given a diversified

database every day, is the system that automatically detects the anthropometric fingerprint. This necessitates optimizing the system to manage the process to match users' expectations, such as quick processing time, near-perfect accuracy, and no errors in the real process. It is paper-based on developing fingerprint classification on the singular feature and mainly focuses on improvising the execution of an automatic fingerprint detection module. Fingerprint classification is a multi-class classification issue in which unsupervised learning is used and the fingerprints (labels) are chosen as the entered data for supervised training of a multi-classifier. The Random Forest and Support vector machine are two ML algorithms used to train the module. The proposed fingerprint identification method is based on RF and SVM algorithms. Betterment of picture pre-processing methods with CNN technology, and computer vision techniques are combined. This improves the quality of the processing system's input images.[48]

Fingerprint classification is a functional method for reducing the number of candidate fingerprints in an automatic fingerprint recognition system's matching stage (AFIS). We present a tentative attempt at solving the traditional fingerprint classification problem using the new depth neural network technology in this study. While processing images and computer vision are two disciplines where deep learning algorithms are used. Using three hidden layers the stacked sparse autoencoders (SAE) in the database(NIST-DB4), reach 91.4 percent accuracy by employing simply the orientation field as an identification feature for the four-class problem. Then, for fuzzy classification, two classification probabilities are utilized, which can significantly improve classification accuracy. In actuality, however, people are continuously looking for ways for the betterment of categorization accuracy without increasing costs. A fuzzy classification is a powerful tool for increasing classification accuracy. In this paper, a novel model is mentioned of neural network and fuzzy classification to improve accuracy.[39]

Personal identity is increasingly required in a wide range of applications, spanning from security to commerce. Biometric-based identifying methods have been shown to overcome the weaknesses of traditional security systems. Bifurcation and termination of the ridge The RF, Multilayer Perceptron, Radial Basis Functions, and Naive Bayesian machine learning methods are trained and tested using minutiae features. Automatic Recognition of Fingerprints (AFR). AFR typically handles three processes: enrollment, identification, and authentication. Calculations of ridge terminating and ridge bifurcation emplacement, type, and orientation are required for fingerprint recognition utilizing minutiae characteristics. The performance of four states of ML Algorithms utilized in AFR for Personal detection is investigated and evaluated in this study.[27]

The respected authors Arslan and Yorulmaz [33] stated that biometric systems are commonly used in conjunction with other authentication methods to enhance security and are considered a decent option. In biometric recognition systems, a controlled and secure platform is the primary goal of biometric recognition methods. Even so, storing the data in an environment with the greatest amount of safety is vital to the recognition system using the characteristic. During the process of biometric recognition, the techniques of machine learning are implemented for not only the extraction of characteristics but also for a variety of other purposes. The researchers provided a few instances of these diverse functions including the liveness identification of biometric modalities, the classification of biometric data sets for

inspecting as well as carrying out the process of diversification, the advancement of statistical method used for the biometric authentication system, an improvement in performance as well as accuracy in the advanced approaches and so on [29], [10],[19], [22]. Throughout the course of this procedure, the authors cleared that the most significant flaws are the capacity of the biometric traits, the defense attributes feature of biometric modalities and the difficulties that arise when utilizing biometric applications [11]. The authors cleared that, in order to create a safe platform for biometric identification, two essential components need to be taken into consideration. The article suggests, that the information recorded during the application process can be saved in a safe way. When an application is being used, security holes that could be found should be kept to a minimum. The alternative method, known as a biometric cryptosystem, is utilized as the key. The biometric information is encapsulated using the key. However, the key itself requires reshaping using a distinct set of supplementary data [19], [20], [22],[16], [17], [21], [25]. Developing machine learning methods that are able to measure more accurately and achieving more biometric recognition success are the most important aspects of the application under development. Furthermore, fingerprint recognition systems have the broadest range of applications among biometric techniques.

Arun and Sarath focused on the issue of gender classification through the use of fingerprint images in [18]. Following the success of an attempt to discover the differences between fingerprint scans using machine learning, the researchers decided to try the fingerprints at gender recognition. They are able to generate a reliable diversifying method for gender featured vector patterns by making use of SVM that was trained with a set of photos consisting of 150 males and 125 females [8]. The fingerprint, which is the replication of the epidermis on a fingertip and is created when a finger is rubbed against a flat surface, is the most widely used form of biometric recognition. In addition, the authors stated that the Ridge density, RTVTR and the white line numbers in a fingerprint image all work together to help determine a person's gender [18]. The ratio between ridge and valley thickness as well as the density of the ridge is an important attribute which determines a person's gender from fingerprint photos. Additionally, all that is needed to enhance a fingerprint is the input image and some intermediate stages implemented on the pictures to acquire the ultimate result [2]. Support vectors are pieces of input data that determine the boundaries between input classes in SVM and SVM's performance is heavily dependent on the kernel [7]. Additionally, prior to determining the projection profile, the fingerprint picture is binarized as a preparatory method. In conclusion, the outcomes of the studies showed that the proposed system, which has an accuracy of ninety-six percent, has the potential to be applied as a prime candidate in the field of a clinical anthropology. The work that needs to be done in the future includes including new elements into the training and classification process, such as counting the number of white lines, and evaluating how well the new system performs in comparison to the one that was suggested.

Among many of the fingerprint image features, singular point plays a vital role in authentic feature extraction.To be able to deduce successful fingerprint detection and indexing more accurately and precisely, definitive and efficient singular point extraction needs to be done. In order to achieve this goal, the study [46] proposed a deep learning architecture for singular point detection using one shot learning from a fingerprint image. This proposed model comprised of three things for instance three

stacked hour glass, Macro-Localization-Network along with Micro Regression.Using three distinct databases, the model has been run on with the goal of achieving a significant result. Therefore it has been found that this model achieves an optimistic result than most other state of the art models. Among many of the biometric features, Fingerprint is the most mature trait. However, the detection of fingerprints from a huge data-set and to identify the right individual to whom this trait should belong is a difficult task to carry out. Since the identification process includes a number of verification processes which need to be run on all the existing fingerprints of the data-set, this approach is hugely computationally rigorous and the verification processes quantity has a proportional relation to the size of the data-set which is enormous [32]. Thus if the size of the database increases, the number of verification processes will increase and ultimately result in worse system performance. So to improve the system, the authors of this article proposed a strategy that pre-filters the database for generating a pre-determined length nominee batch where size of the set is small and the set of fingerprints have high probabilistic guarantee for high hit rate. This method is known as indexing [47]. This Indexing method needs singular points for a successful recognition of fingerprint and so to detect the singular point, a CNN Model undergoing a training phase which includes 'Two step end to end' training. So after taking a fingerprint data as an entry, the model would output the pin-point location of the the image's singular point. Therefore, the proposed work not only implemented a novel architecture of CNN which detected singular point of fingerprint from scratch which did not have any pre-trained weight, but it also used in-house data-set to bring a promising result and authenticate the proposed model. Babikir Adam and Sathesh [58] in their paper tried to find the liveness detection of fingerprints . They differentiated between the machine learning approach (using SVM classifier) and Ridge Let Transformation (RT). In the paper, hardware modules, software processing algorithms and previous training or capturing of physique moments are mentioned to acquire the sign of live moments at present. These ideas proved to assist in obtaining better results. Although the paper differentiated with the RT approach, their proposed approach still used RT for the extraction of image procedure. The liveness detection part relied on the classifier approach where the approach has a single and ensemble classifier approach. Overall, the model was tested over 50,000 images and obtained 90.34% accuracy.

Lothai and Bong [40] researched about the Bit-plane method of fingerprint identification. They paired bit-plane with POC to get a better result while occupying less storage space for the fingerprint extraction. In there they mainly compared their model with the existing minutiae based fingerprint recognition. In their method, they implemented multiple methods for the whole process. For the ROI or region of interest of fingerprint, they used blob analysis method for detecting ROI.They further implemented image alignment of the fingerprint and image cropping of ROI fingerprint image cropping. Later they utilized Fourier transform for the enhancement of images. Furthermore, bit plane is used for feature extraction of the fingerprint image and POC was used for matching the fingerprints.In their process, the bit plane was selected based on the average highest recognition rate. With the additional help of imposter and genuine similarization, the fingerprint identification process has been evaluated. In terms of putting the accuracy into tangible values, the ROC curve has been utilized. The approach implemented by the authors offered greater storage management and it complemented the challenge of further racing storage

capacity used by grayscale image. By implementing bitplane extraction approach and compression techniques, this compression of size of image has been achieved[14]. From the study, we also came across a point that for different bioinformatic features, the bit planes hase various roles. But, due to the uniqueness of the fingerprint, the process was a bit complicated. [36]. To address this problem, POC method was applied as POC doesn't consider minutiae extraction[9]. The report also included pre POC functions, used for the pattern reorganization and image process. These functions create multiple wide peaks and a single peak whose maximum is difficult to spot.[24]. However, POC still outperform them. The authors compared their method with other methods using FVC2002-Db1a and FingerDos dataset where they achieved 81.16% and 89.78% accuracy respectively.

2.2 Paper Review Summary Table

The table below contains the focus points of the referenced papers that has been discussed for the implementation of our research work:

Title of Paper	Year of Publication	Size of the Dataset	Accuracy Status	Algorithms used	Strong Point	Weak Point
[45]	2018	6000	75.2%	Convolutional Neural Network, Transfer Learning	1.CNN learns the features to distinguish between genders, 2.Gender, Hand and Finger classification	1.Training very deep CNN's, 2.Accuracy of gender and finger classification is very low.
[61]	2021	Few labeled Images	up to 100%	Few Shot Learning, Meta Siamese Network	1.MNS with baseline methods can have accuracy up to 100% , 2.Small training set, 3. Works best for both constrained and unconstrained databases	1. Dataset was not large and labelled.
[51]	2020	Multiple Datasets of different sizes were used	Not Available	Comparison of different algorithms like Support Vector Machine, Deep learning, KNN, NN from	1.Comparison of different research papers to compare real and fake fingerprint by applying different machine learning algorithms, 2.Comparison of different anti spoofing techniques from different research papers	1.No novel approach or no new model was implemented only a comparison of different research papers have been shown
[46]	2019	800, 800, 30,000	98.75, 97.50%, 92.72%	One Shot Learning, CNN, Macro Localization Technique, Micro Regression Network	1.Novel CNN architecture has been introduced, 2.Tested on standard dataset and in-house dataset	1.Four stacked hourglass networks where low accuracy was found.
[48]	2019	3	95.5%	Computer Vision algorithms, SVM algorithm, RF algorithm.	1.Reduce the number of comparisons in automatic fingerprint recognition systems with large databases, 2.High accuracy rate.	1. Often give an error due to of the low-quality input image.
[39]	2016	Not Available	91.4%	Classification-algorithm	1.Focuses on classification accuracy	1.Poor quality or ridge structure because of the wrong classification.
[27]	2015	Not Available	Not Available	RF algorithm, Naïve Bayesian algorithm, Machine Learning algorithm	1.Investigate and evaluate of ML algorithm in automatic fingerprint recognition for personal identification.	1.No security and protection from the pretenders.
[54]	2020	Not Available	Not Available	ML algorithm	1.Focuses on methods that overcome the necessity of huge amount of data	1.Complex model
[33]	2016	Huge dataset	Various Accuracies	Biometric, machine learning, SVM, ANN, GMM, KNN, NB, HMM, LDA, LBP, PCA	1.High accuracy rates for each and every feature, 2.Informative datasets.	1. Use of too many algorithms
[18]	2011	150 male and 125 female subjects. Total image 275	96%	SVM, Radial basis function RTVTR, Ridge Density.	1.High Accuracy	The database was not large.
[58]	2021	Over 50,000	90.34%	SVM, Single and Ensemble Classifier	1.Gives better performance in Fingerprint detection than image recognition method with RT due to ensemble classifier . 2.Use of dataset augmentation to improve accuracy. 3.Obtaining highest accurate detection result through hardware module 4.Obtaining better results through software processing algorithms.	1.SVM was previously used in a research paper making it an existing method. 2.To provide accurate identification, the approach still relied on RT for image feature extraction. 3.Is not that practical for all the forms of spoof fingerprinting materials. 4.Single and Ensemble classifiers have different strengths. 5.Gives lower accuracy while using unknown materials for spoof detection. 6.Only the single classifier can show accuracy for unknown materials.
[40]	2017	FVC2002-Db1a FingerDos	81.16% 89.78%	Modified Blob Analysis Dimension Reduction Fourier Transform POC	1.Image size reduction method 2.Each bit level gives scope to wider recognition area 3.Use of POC for low quality fingerprint identification 4.This model saves storage and increases data transmission rate	1.Faces difficulty in fingerprint recognition due to unique minutiae 2.Poc can be easily affected by fingerprint's displacement

Table 2.1: Paper Review Summary

Chapter 3

Methodology

In this section, we will implement different models of transfer learning on our dataset[45] in order to identify the person and classify gender, hand, finger and also to identify types of alteration.

3.1 ResNet Model

Residual-Network are one of the most popular and efficient frame works in terms of genearating higher accuracy while keeping both complexity of deep layered networks and the training errors of such networks at a minimum rate. Resnet frameworks are extremely efficient , as a sign of the success, we can see that [35] had won 1st place on the ILSVRC-2015 classification task where the framework was operated on the ImageNet dataset [35] .Image-classification, localisation and detection of object as well as reduction of computational expenses are inclusive of the use cases of the said framework [35] . In traditional directed deep networks, the features and the classifiers/labels are generally incorporated through a multilayer fashion, where increasing of the stacked layers denotes the enrichment of the features [26] . However, problems arises when more layers are added, resulting in saturation of accuracy, increment of training error.
The Figure 3.1 shows the continuation of a network where additional layers are added, and with each added layer, we have to perform convolution operations in each layer. Here in the Figure3.1 we take input X, pass it through the weight layer for the convolution operation and after that we pass the result to ReLU activation function. We do this for each layer. The problem here is that, when the network becomes very deep, it becomes very complex to do this kind of operations, and it starts giving out wrong results, resulting in higher error, making an user demotivated to increase the depth.
However that's where residual networks, Like Resnet50,Resnet34 etc. shines in. Instead of performing direct connection, we can feed the neural networks with skipped connections. The idea behind skipped connections is that, it will simply try to find the difference between the input and the outlet, with the help of a residual block.
Here in the Figure3.2, residual network, the input x is added to the F(x). Here the shortcut/skipped connections simply perform identity mapping where the output of the shortcut connection is added with the result of the stacked multi-layer, while adding zero parameter or complexity by the skipped connections [35] . Following this formula, Resnets can successfully address the problems of degrading results with

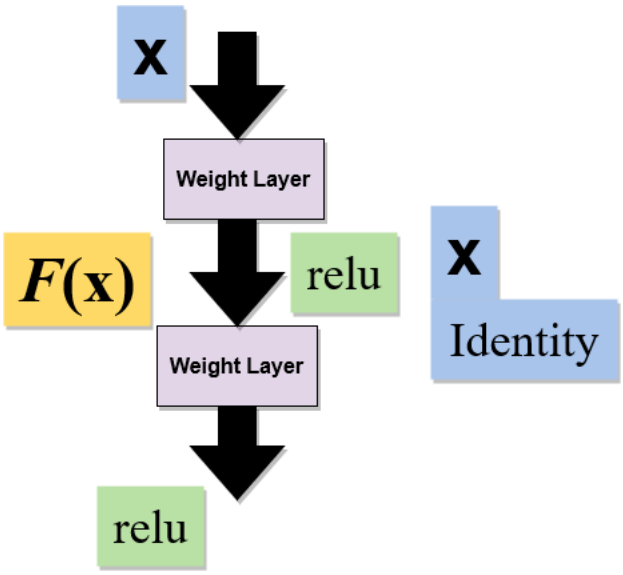


Figure 3.1: Direct Network

added layers, hence faster convergence, better accuracy and efficient performance with extensive deep layers.To keep in mind, for residual networks, the input and the output have to have similar dimensions. If there is a discrepancy between the dimensions, we can follow the equation .

$$Y = F(x, W_i) + W_s x \tag{3.1}$$

Performing this linear projection, W, through the shortcut connection, the dimension can be matched for input x and output y [35] .

3.1.1 ResNet-50

Resnet 50 is a type of residual network, a part of transfer learning models, that aims to increase the accuracy of a network with very deep layers, while keeping the training error minimum. The formulation of the Resnet50 network tries to connect the residual function with respect to the layered inputs.The distinct feature of ResNet-50 is that this model skips 3 layers through shortcut connection.
Resnet50 is a residual-net framework that contains the following layers :

1. 48 layers of Convolution
2. 1 layer of Maxpool
3. 1 layer of Average pool

And they all connect to the fully connected layer that gives out the output. Besides, Resnet50 model can dishout a floating point operation of $3.8*10^9$.
The architecture can be summarized with the help of the following table for a 7*7,64 convolution with a stride/step size of 2 along with 3*3 maxpool having stride size of 2 .

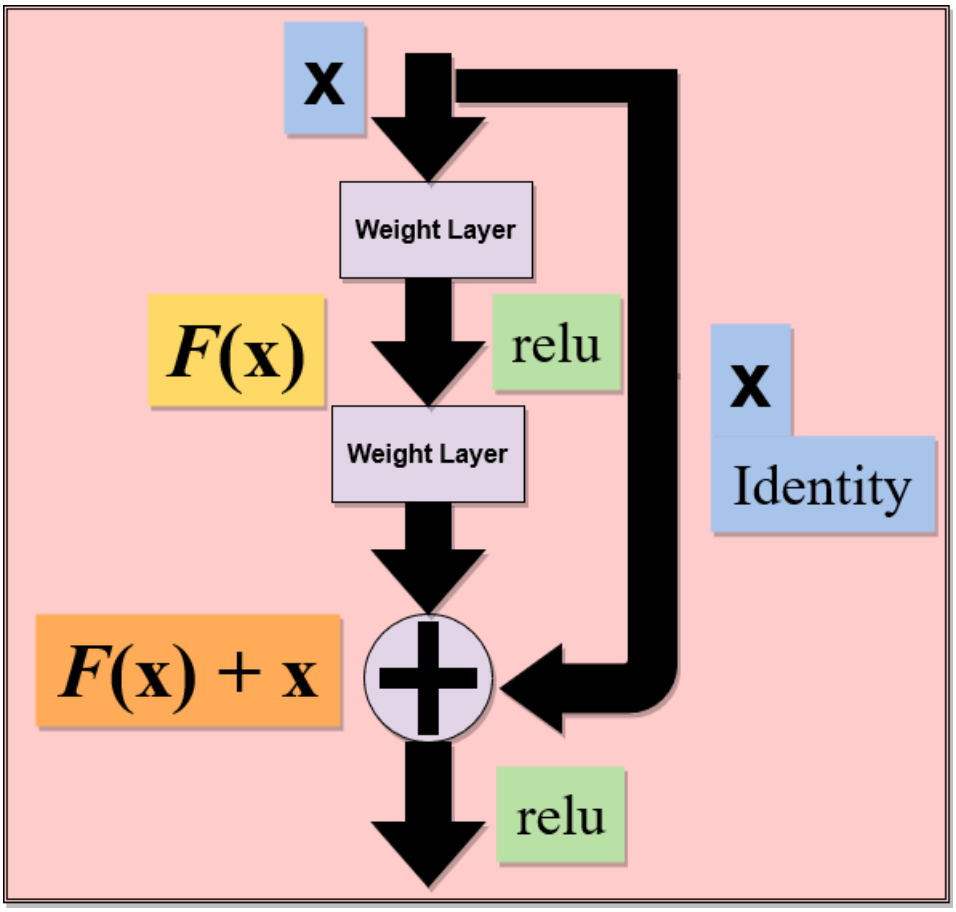


Figure 3.2: Residual Network

From the Figure3.3 we can extract the following informations

1. **1 layer of**, 64 different 7*7 kernels where stride is 2. We also have a 3*3 max pool with stride of 2
2. **9 layers**, where we have repetition of 3 of each, 64 different 1*1 kernels, 64 different 3*3 kernels and 256 different 1*1 kernels.
3. **12 layers**, where we have repetition of 4 of each, 128 different 1*1 kernels, 128 different 3*3 kernel and 512 different 1*1 kernels.
4. **18 layers** , where we have repetition of 6 of each, 256 different 1*1 kernels, 256 different 3*3 kernels and 1024 different 1*1 kernels.
5. **9 layers**, where we have repetitions of 3 of each, 512 different 1*1 kernels, 512 different 3*3 kernels and 2048 different 1*1 kernels.
6. **1 layer** of average pool along with a fully connected layer which contains a number of 1000 nodes as well as a softmax function.

Layer Name	Output Size	50-layer
conv1	112*112	7*7,64, Stride 2 3*3 max pool, Stride 2
conv2_x	56*56	[1*1,64] *3 [3*3,64]*3 [1*1,256]*3
conv3_x	28*28	[1*1,128] *4 [3*3,128]*4 [1*1,512]*4
conv4_x	14*14	[1*1,256] *6 [3*3,256]*6 [1*1,1024]*6
conv5_x	7*7	[1*1,512] *3 [3*3,512]*3 [1*1,2048]*3
	1*1	Average pool, 1000-d,fc , Softmax
FLOPs		3.8*10^9

Figure 3.3: Resnet50 information

The full Resnet-50 architecture Figure3.4 collected from [64] is shown below. This helps better understand the whole network. Here, the shortcut connections skipped 3 layers and there is a ReLU used for activating the function. At the end there is a average pool as well as the whole network is connected with the fully connected layer.

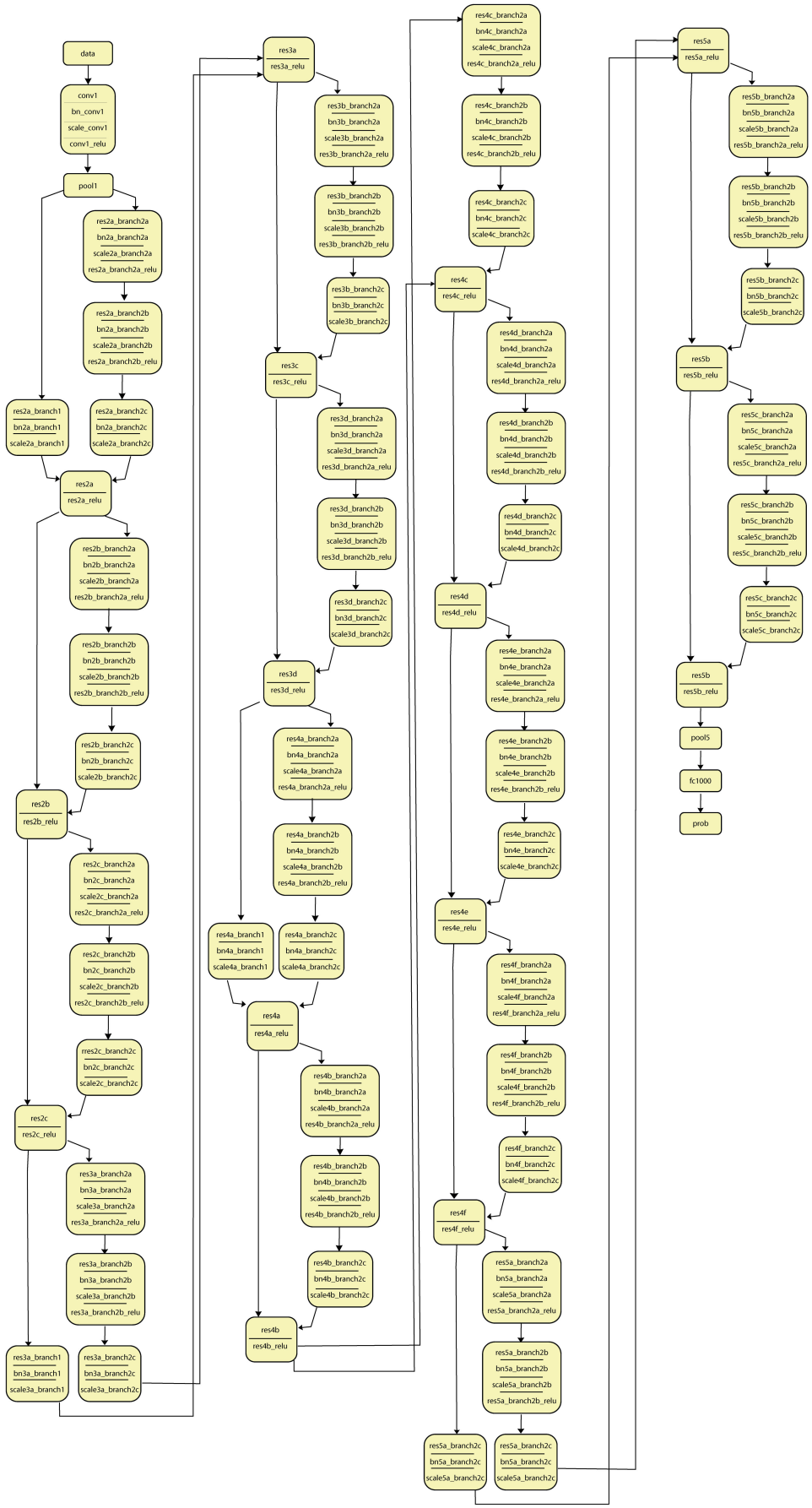


Figure 3.4: ResNet 50 Architecture

3.1.2 Resnet-34

Resnet34 is another residual-net framework that contains the following layers :

1. 32 layers of Convolution
2. 1 layer of Maxpool
3. 1 layer of Average pool

And they all connect to the fully connected layer that gives out the output. Besides, ResNet-34 model can dishout a floating point operation of $3.6*10^9$[35].
Like other residual networks, ResNet34 also aims to improve the accuracy and outputs a solution to the vanishing gradient problem that forbids a deeper network. The idea with the ResNet-34 is that, this model creates a shortcut connection which skips 2 layers, allowing the gradient surf smoothly. The idea here is that, the model should be able to predict ,H(x),any of the predecessor functions. The formula looks like ,

$$F(x) + x = H(x) \tag{3.2}$$

Where the pre-requiem of the learning states that, F(x) should be equivalent to zero [35].
The architecture can be summarized with the help of Figure3.6 for a 7*7,64 convolution with a stride/step size of 2 along with 3*3 maxpool having stride size of 2.

Layer Name	Output Size	34-layer
conv1	112*112	7*7,64, Stride 2 3*3 max pool, Stride 2
conv2_x	56*56	[3*3,64] *3 [3*3,64]*3
conv3_x	28*28	[3*3,128] *4 [3*3,128]*4
conv4_x	14*14	[3*3,256] *6 [3*3,256]*6
conv5_x	7*7	[3*3,512] *3 [3*3,512]*3
	1*1	Average pool, 1000-d,fc , Softmax
FLOPs		3.6*10^9

Figure 3.5: Resnet34 Information

From the table we can extract the following informations

1. **1 layer of**, 64 different 7*7 kernels where stride is 2. We also have a 3*3 max pool with stride of 2
2. **6 layers**, where we have repetition of 3 of each, 64 different 3*3 kernels 64 different 3*3 kernels.
3. **8 layers**, where we have repetition of 4 of each, 128 different 3*3 kernels 128 different 3*3 kernels.
4. **12 layers**, where we have repetition of 6 of each, 256 different 3*3 kernels
5. 256 different 3*3 kernels.
6. **6 layers**, where we have repetition of 3 of each, 512 different 3*3 kernels 512 different 3*3 kernels.
7. **1 layer** of average pool along with a fully connected layer which contains a number of 1000 nodes as well as a softmax function.

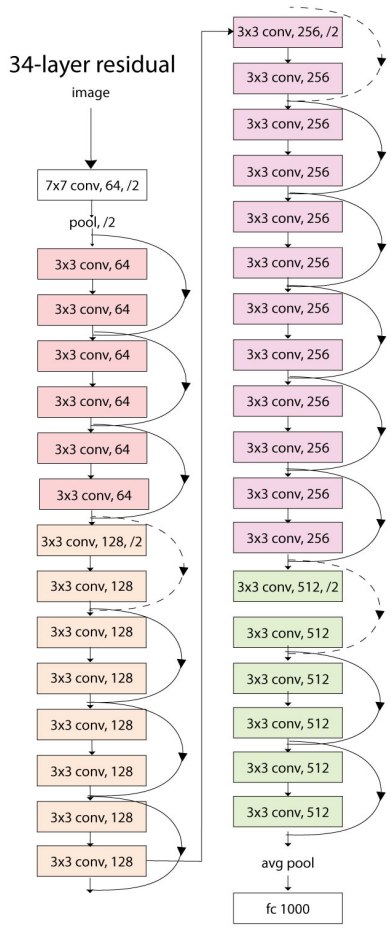


Figure 3.6: Resnet34 Fragment

This is the architecture of a Resnet34 model from Figure3.6, that helps better understand the whole network. Here, the shortcut connections skipped 2 layers and there is a ReLU used for activating the function. At the end there is a average pool as well as the whole network is connected with the fully connected layer.

3.2 EfficeientNet-V2s

EfficientNet V2 is an improved version of the already existing EfficientV1 [50] family models(B0-B7). By improved it means that EfficientNetV2s can have better performance in terms of training agility as well as parameter efficiency [63]. The model solves the problem of accuracy drop during the increment of image size while training for the sake of boosting up the training. By proposing a method of adaptive regularization adjustment called progressive learning, the reduction of accuracy can be optimized.
The pre-existent, EfficientNetV1 family had some drawbacks for instance slower training when the image size is large, slower depth-wise convolution,scaling producing sub-optimal results and so on [50]. The improved EfficientNeV2 family models, like the one we are using EfficientNetV2s, not only solves the above mention boundaries of the previous family, but also has a training speed which is 4 times faster while having a parameter size which is actually 6.8 times lighter[63].
To achieve this success, the model has been composed of training aware Neural Architecture Search aka NAS and scaling. The stage-based factorized space, for NAS search, includes MBConv FusedMBConv [53] convolutional operation types. Moreover, 3*3, 5*5 kernel sizes with an expansion ratio of 1:4:6 are also inclusive. It's noteworthy that the V2 models are based on the original V1 models which allows the newer model to reuse the similar channel sizes, enabling a smaller space suitable for the appliance of reinforcement learning and random search if the network is elaborated[50][63]. Moreover, v2 models optimize the search space by pruning minor/unused operations like pooling or skipping. The desired output can be defined by the following weighted product,

$$A.S^{w}.P^{v}. \tag{3.3}$$

Here A denotes accuracy, S denotes step time and P denotes parameter size with w= -0.07 and v=-0.05 [63]. NAS paired with scaling, achieves a greater throughput in terms of speed and parameter efficiency.
To address the drop of accuracy and slower training of the previous version, the problem has been solved by implementing progessive training as already mentioned, which was based off the curriculum learning [13]. This progressive training allows training large scale images with rapidness and higher precision[63].
The effectiveness of EfficientNetv2s is marvelous. This model got top-1 accuracy with 87.3 percent on the ImageNet (pre-trained on ImageNet21k) ILSVRC2012. Moreover, the parameter efficiency was 83.9 percent on the same dataset. Furthermore, the model was able to hit up to 11times faster training speed as well as 6.8 times better parameter efficiency on CIFAR,Cars etc. dataset besides ImageNet [63].

As for the architectural design of the EfficientNetV2s, the models use both MB-

Conv and FusedMBConv[53][63][50]. Besides, the model manages less memory access overhead by utilizing a smaller expansion ratio. Moreover, 3*3 smaller kernel sizes are designated into this model. However, more layers are inserted to make up for the deducted receptive field due to the utilization of smaller sized kernels. Further, EfficientNetV2s optimizes the parameter size and the overhead by pruning the final stride-1 stage, existing in the V1 model[63].
The detailed structural information is shown in the Figure3.7 .

Stages	Operator	Stride	Channels	Layers
0	conv3*3	2	24	1
1	Fused-MBConv1 , k3*3	1	24	2
2	Fused-MBConv4 , k3*3	2	48	4
3	Fused-MBConv4 , k3*3	2	64	4
4	MBConv4, k3x3, SE0.25	2	128	6
5	MBConv6, k3x3, SE0.25	1	160	9
6	MBConv6, k3x3, SE0.25	2	256	15
7	Conv1x1 & Pooling & FC	-	1280	1

Figure 3.7: EfficientNetV2s Information

From the Figure3.7, we can extract the following informations

1. **Initial Stage** : Composed of 2 strides, 24 channels, and conv3*3 altogether forms 1 layer.
2. **1st Stage** : Composed of 1 stride, 24 channels, and Fused-MBConv1 with k3*3 altogether forms 2 layers.
3. **2nd Stage** : Composed of 2 strides, 48 channels, and Fused-MBConv4 with k3*3 altogether forms 4 layers.
4. **3rd Stage** : Composed of 2 strides, 64 channels, and Fused-MBConv4 with k3*3 altogether forms 4 layers.
5. **4th Stage** : Composed of 2 strides, 128 channels, and MBConv4 with both k3*3 and SE0.25, altogether form 6 layers.
6. **5th Stage** : Composed of 1 stride, 160 channels, and MBConv6 with both k3*3 and SE0.25, altogether form 9 layers.
7. **6th Stage** : Composed of 2 strides, 256 channels, and MBConv6 with both k3*3 and SE0.25, altogether form 15 layers.
8. **Final stage** : concludes with 1 layer consisting of 1280 channels as well as conv1*1, pooling and a FC.

The architecture of EfficientNetV2s, comprising both MBConv and Fused-MBConv is shown in Figure3.8 below[53][63].

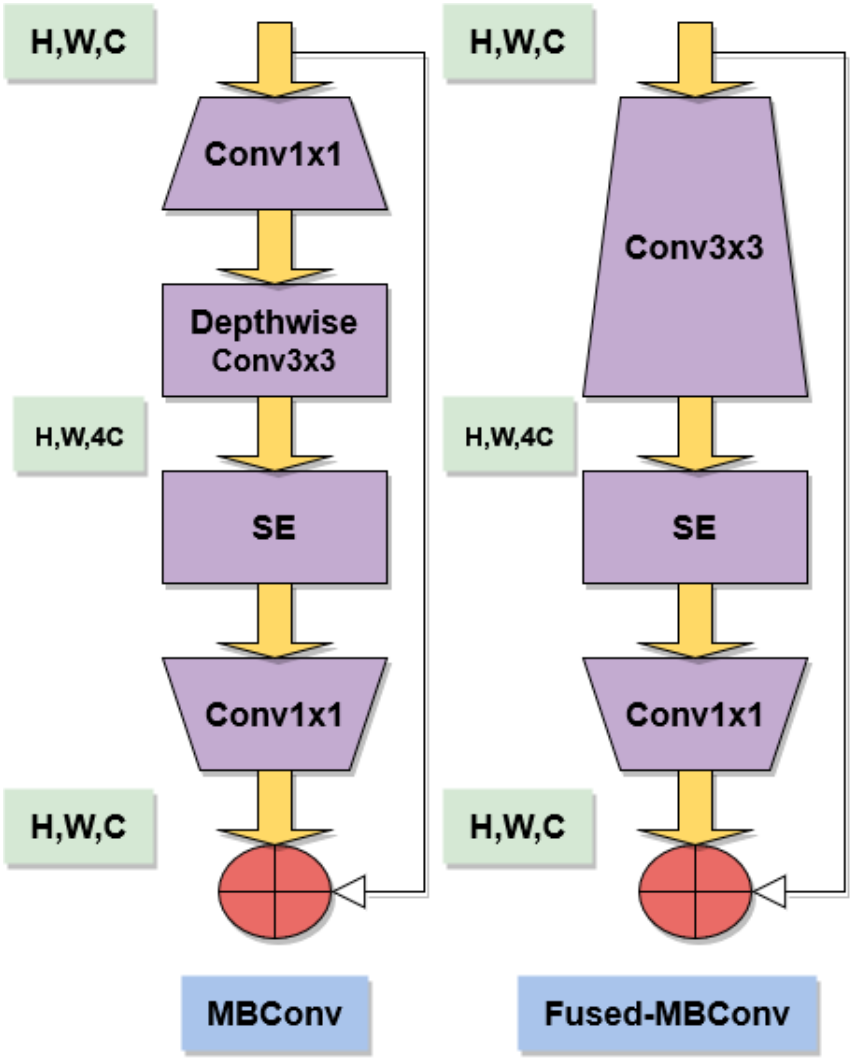


Figure 3.8: EfficientNetV2s Architecture

3.3 RegNet-Y32GF

RegNet is low dimensional design space with a simple parameterized, containing simple regular networks that aims to deliver working simple and fast networks for a variety of floating operations. The RegNet model is tested to produce 5 times faster performance on GPUs that the EfficientNetV1[50] models[56].
RegNet design space combines the positive directions of both NAS and manual design to parameterize network population where RegNet adopts attributes such as interoperability,semi-automated procedures.With the target of advancing the quality, the model initializes a progressive design pattern where it aims to improve an simple and unconstrained design space. The process summarising is inclusive of elevation towards population level, directed through distribution estimates and symmetrical to the manual design level[49][56].
Determining the breadths and depths of the stages through a quantized linear function, the RegNet design space gives ease in terms of interpretation while having a vast amount of better models. To make the RegNet design, AnyNet structure has been used as a baseline, while considering the architectural skeleton of ResNet. To do so, log uniform sampling has been utilized to generate best AnyNet family mod-

els among which the best one will be selected for the RegNet design space. Taking into account the Error empirical distribution Function (EDF), for calculating the n number of models with errors with the following formula,

$$F\ (e)\ =\ \frac{1}{n}\sum_{i=1}^{n} 1\left[e_i\ <\ e\right] \tag{3.4}$$

Where F(e) denotes the AnyNet model that has an error lower than e [49][56]. Observing the accuracy gains based on inputting various values of four parameters in the selected AnyNet model, similar trends and set of equations was generated which helped best fitting the RegNetY32 model with the initial width w0, slope parameter wa, quantization parameter wm, network depth D as well as group and bottleneck ration g and b [56].
Following 3 equations which produces depth and width, the RegNet architecture can be constructed.

1. Parameterized widths Equation : Calculating possible width u, while inputting wa and w0, where j is positive and lesser than d.

$$u_j = w_0 + w_a \cdot j \tag{3.5}$$

2. Parameterized Blocks Equation : Calculating possible block size s, while inputting u, w0 and wm.

$$u_j =\ w_0.w_m^{s_j} \tag{3.6}$$

3. Quantized Widths Equation : Calculating quantized widths w, while inputting rounded value of s as well as amking sure w can be divided by 8.

$$u_j =\ w_0.w_m^{[s_j]} \tag{3.7}$$

4. By taking the unique values of d, we calculate the final width list w.

5. Correcting the incompatible w due to the bottleneck ratio, we will check the multiplicity of group g by the width list w.

Finally , inserting the obtained values into the ResNetX architecture, we will find one part of the RegNetY32 model,RegNetX, as RegNetY models pair up squeeze and excitation layers with the[56].

From the Figure3.9 we can get a visualization of the addition of SE layer in the residual block.

1. Here SE layer is added into the network after each 3*3 convolutional layers of ResNet architecture.

2. Zooming into the SE block, we find a new parameter, q denoting the se ratio along with two 1*1 convolutional layers.

Thus, finally adding the new parameter q with the found parameter of RegNetX, RegNetY32 model is finally generated. It can be written as

$$RegNetY32GF = RegNetX + SE\text{[56]}. \tag{3.8}$$

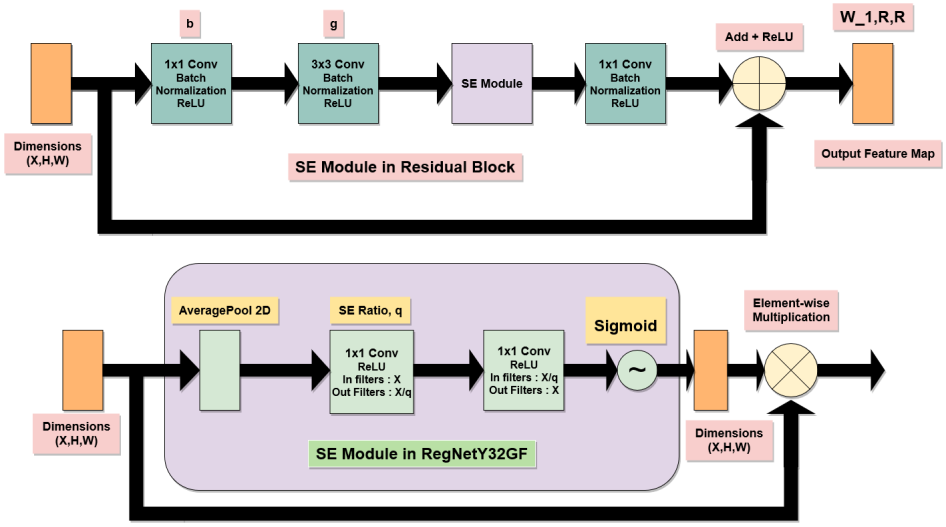


Figure 3.9: RegNetY32GF Architecture

3.4 Inception-V3

For the purpose of optimizing the deep learning networks more efficiently, Inception-V3 was discovered back in 2015. The model consisted of 42 layers where it proposed an array of techniques that made it stand out than it's predecessor, Inception V1 and V2. While the V3 model proposes a much deeper network in comparison to its previous version, the deepness does not compromise the speed in anyway. This results in a higher accuracy in a computational cost-effective manner [38]. The modifications done to this models does wonders in it's performance. Inception V3 factorizes larger convolutions into smaller ones which allows the model to have a 28 percent relative gain. Moreover, due to this factorization, we have seen a reduction in computational cost with the deducting numbers of parameters [38]. Secondly, with the goal of the factorizing the model even more as well as making it more efficient, Asymmetric convolutions are used here. This technique costs 33 percent less in terms of similar amount of input and output filters [38]. Thirdly, to tackle the problems of vanishing gradient as well as improving the convergence of a large neural networks, Inception V3 uses auxiliary classifiers to act as a regularize which assists in producing higher accuracy towards the final stages of training. Lastly, instead of using average and max polling for the grid size reduction, Inception V3 expands the networks filters by activation dimensions. By implementing various techniques and modifications, Inception V3 is a much reliable model producing only 4.9 percent Top-5 error [38]. The outline of the Inception V3 is shown below.
From Figure 3.10 we can see the detailed outline of the Inception V3 model [38].

Type	Patch/ Stride Size	Input Size
Conv	3x3/2	299x299x3
Conv	3x3/1	149x149x32
Conv Padded	3x3/1	147x147x32
Pool	3x3/2	147x147x64
Conv	3x3/1	73x73x64
Conv	3x3/2	71x71x80
Conv	3x3/1	35x15x192
3 x Inception	Module 1	35x35x288
5 x Inception	Module 2	17x17x768
2 x Inception	Module 3	8x8x1280
Pool	8 x 8	8x8x2048
Linear	Logits	1x1x2048
Softmax	Classifier	1x1x1000

Figure 3.10: Inception V3 Model

The illustration of the model cam be seen from Figure 3.11 [38].

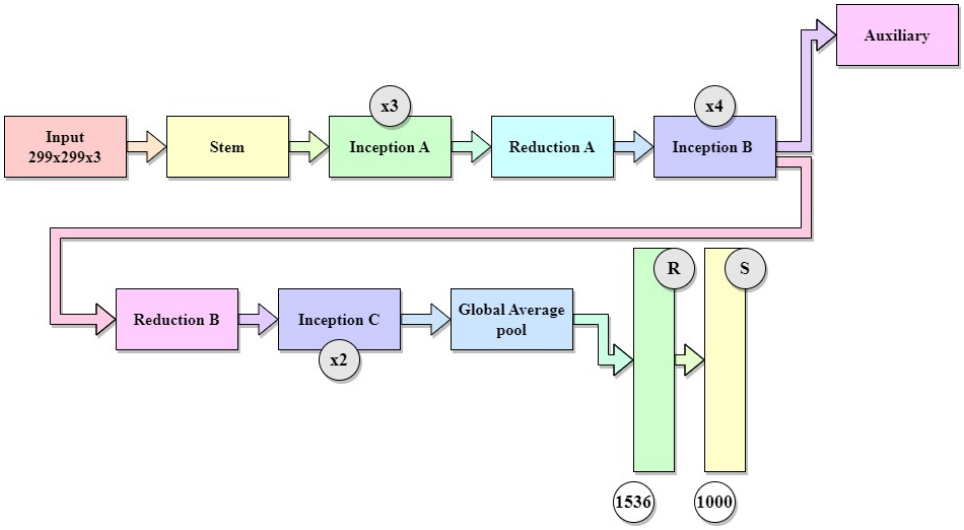


Figure 3.11: Inception V3 Model

3.5 One Shot Learning

While performing image-processing tasks, traditional deep convolutional network faces several issues. Traditional deep CNN requires a lot of labeled image data for each classes, which in many cases may not be available. Moreover, in order train for a specific class, a lots of images of that particular class must be given which is another expensive task. Furthermore if we are to add any new class or remove existing class or any sort of alteration, the network has to retrained. These are

some issues that occurs frequently in forensic departments or even in offices where the number of classes are dynamic. This makes both gathering data and retraining over and over again becomes very expensive for any organization. Therefore we choose one shot learning where only one sample image is needed for learning new or unseen objects. Traditional convolutional network trains input images using soft-max activation and produced output based on predicted probability distribution in a vector size in par with the number of classes. However, One shot learning does not do that. Instead the network take only one reference image, one test image and uses Siamese network to compare the two images and lastly generate a similarity output that shows how the test image is similar or dissimilar with the reference image. This turns the classification problem into a difference evaluation problem. Siamese neural network uses a triplet loss function where it is trained on three types of images. The network is trained on an anchor image, a positive image which is a slightly altered image of the reference or anchor image and lastly a negative image which is a completely different image. The network then compares the features of both images with respect to the reference image. The parameters for the neural network is tuned in such a way where the encoding values of the anchor and positive image is close . On the contrary the encoding values of the anchor and negative is very far apart. This is how Siamese neural network uses triplet loss function to evaluate the distance of the features of two input images , the reference image and the test image, provided into the one shot learning based network.Below Figure-3.12 shows the procedure of Triplet Loss function.

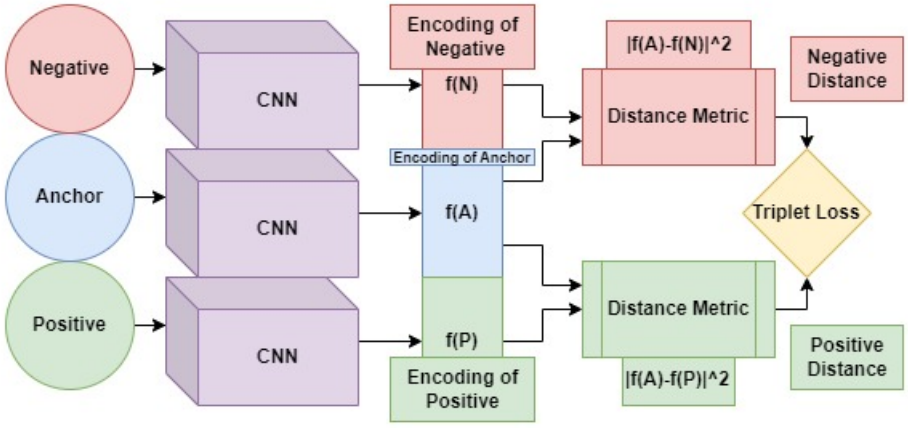


Figure 3.12: Triplet Loss Function

The similarity then uses a threshold value to determine whether the reference image and test image belongs to the same person person on not Fig[3.12] . In our case, the threshold value is 0.75 meaning if the similarity score gives us a value lower than 0.75, our model will say that the test belongs to the reference fingerprint image and the person is matched. It will otherwise not match.
Lastly, the Siamese neural network uses Sigmoid function to provide the output value between 1 and 0. If the output value is 1 or closer to 1 , then it denotes that the reference and the test image are of the same object. If it's 0 then it denotes that

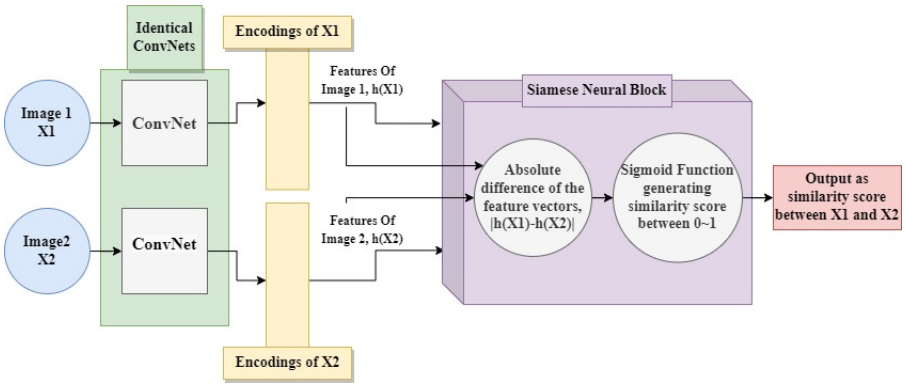


Figure 3.13: One-Shot Learning Model

both the images have very less similarity Figure-3.13. This is how using just a single reference image of an object we can generate similarity with other test objects and classify them. In this way the network does not need to train for dynamic classes as the network deals with the difference evaluation. Moreover, for an object or class to identify, the network only requires one reference image into it's database compared to traditional deep CNN. There in person identification issues, specially in terms of fingerprint recognition, to identify a person only one sample of his registered fingerprint is sufficient to identify him. This will help a lot in forensic and bio metric divisions where there is not always sufficient data to identify a person. However, implementing one shot solves that problem in a cost effective manner.

Chapter 4

Dataset

4.1 Dataset Description

For our thesis, we have utilized the Sokoto Coventry Fingerprint Dataset, in short **SOCOFing**, which is a specialized fingerprint based dataset useful for fingerprint recognition based works [45]. The dataset is composed of the information taken from 600 different adult African individuals who are all aged over 18 years reportedly [45]. There are a total of 6000 fingerprints containing pairs of thumbs,forefingers,long fingers,ring fingers and little fingers of a single individual's left and right hands. Implementing STRANGE framework[37], realistically synthesized altered fingerprint pictures were generated which produces three different tiers of alterations in regards to obliteration, Z-cut and central rotation[45]. The altered images obtain a resolution of more than 500 dbi. Moreover, the numbers of altered images can be ranged from (with respect to parameter settings),

1. **Easy :** 17,934 images
2. **Medium :** 17,067 images
3. **Hard :** 14,272 images.

Hamster plus(**HSDU03P™**) and SecuGen(**SDU03P™**) sensors were operated on the realtime impressions and collected the original images, each images obtaining a resolution of 1x96x103 (gray x width x height)[45]. A sample image of SOCOFing dataset is illustrated in the Figure4.1 below.

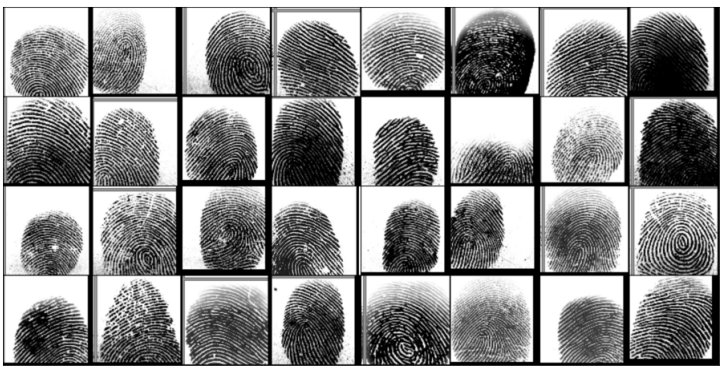


Figure 4.1: SOCOFing Sample

4.2 Data Classification

4.2.1 Training Set

The dataset which are used to form an experience for the models to learn a behavior or pattern is called training dataset that is to know about the features and fit a model accordingly.

4.2.2 Validation Set

The dataset which are used to form an experience for the models to learn a behavior or pattern is called Validation dataset.

4.2.3 Testing Set

A dataset can be divided into training set and validation set. Utilizing this validation set, models are trained to get improved performance.

4.2.4 Visualization

In order to prepare a dataset suitable for model training, a dataset has to be fragmented into three sets such as training set, validation set and testing set. This preparation can be visualized below.

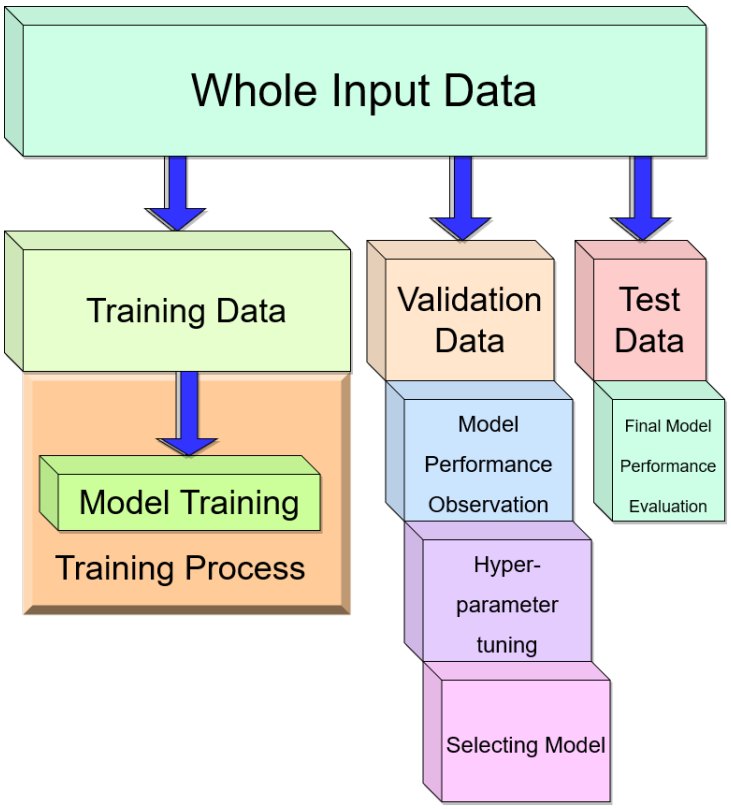


Figure 4.2: Dataset division for training purpose

4.3 Preprocessing for Model Implementation

In order to implement the CNN models, data needed to be preprocessed. This will ensure that the data used for the models don't have any inconsistencies.

4.3.1 Data Segmentation

The main purpose of this research is to make a model which will detect the person's ID, gender, hand, finger and also real and altered fingerprints. For this purpose, the data are divided firstly into two target classes, gender and finger class. Inside the finger class the hand (Left/Right) and finger type (Thumb/ Index/ Little/ Middle/ Ring) are included. Therefore, the gender target class has 6000 images with Male Finger images consisting of 4770 images and Female Finger images consisting of 1230 images. Moreover, both the left and right thumb, index, middle, little, ring finger each class have 600 images. Moreover, for each person's there are total 600 ID assigned as well which is utilized in classifying person's ID. Moreover, there are three types of altered images which gives us a total of almost 55 thousand altered fingerprint to identify whether the fingerprint is altered or real.

4.3.2 Data Augmentation

To make the models versatile, the models need to overcome the drawback of overfitting. Since models tend to memorize the data instead of establishing relationship because of the overfitting nature. Thus the aim of the models is to increase the amount of data by creating new data points in order to mitigate the overfitting nature and form generalized relationship better.

Resize pixels:

In order to decrease the complexity of dealing with large sized pixels, the images were scaled down to 96×96 . Moreover, the models implemented in this research paper used 96×96 pixels.

Reflect:

The reflection is used to ensure that the transition of outputs will occur smoothly to improve the performance of the implemented models.

Random Crop:

Since in the images our object of interest are not always entirely visible in the image, random crop creates random subset of original image to help the model learn and generalize better.

Chapter 5

Result Analysis

5.1 Model Analysis

In order to analyze, the results of the implemented models various performance metrics have been used to interpret the result. A brief discussion have been done below regarding those matrices:

5.1.1 Confusion Matrix

A confusion matrix is a performance assessment matrix of $N \times N$ size used mainly on classification models which assists to visualize the performance of the models implemented. This confusion matrix is also know an error matrix. Here the target class is denoted by N. A brief discussion on the terms used in the confusion matrix have been done below:

• **True Positive, TP** : The actual value and the predicted value are same where both the values were positive

• **True Negative, TN** : The actual value and the predicted value are same where both the values were negative

• **False Positive, FP** : The predicted value was positive however the actual value was negative

• **False Negative, FN** : The predicted value was negative however the actual value was positive

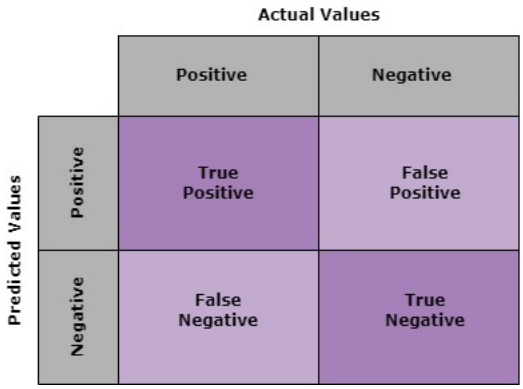


Figure 5.1: Confusion Matrix

5.1.2 Accuracy and Loss

Accuracy and Loss are the performance measuring functions mainly used for classification models. Accuracy measures how precisely the model is working. whereas loss function measures how poorly the model is functioning. Accuracy is measured in percentage whereas Loss is measured based on the addition of errors for both training and validation sets for each of the sample.

$$Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \tag{5.1}$$

5.1.3 Precision, Recall and F1 Score

In order to identify the performance and effectiveness of the model, precision and recall are a must. The proportion of relevant examples among the retrieved instances is known as precision. Precision is also known as positive predictive value. It mainly gives insight of how many of the affirmative identifications were actually accurate. However, the proportion of relevant instances that were retrieved is known as recall. It is also known as sensitivity. Recall gives an idea about what percentage of real positives were successfully identified.

$$Precision = \frac{TP}{TP + FP} \tag{5.2}$$

$$Recall = \frac{TP}{TP + FN} \tag{5.3}$$

A machine learning evaluation metric called the F1 score assesses a model's accuracy. It combines a model's precision and recall ratings. How many times a model correctly predicted throughout the full dataset is determined by the accuracy score.

$$F1Score = \frac{2{*}Precision{*}Recall}{Precision + Recall} \tag{5.4}$$

5.2 Accuracy and Loss measurement of Training Sets Versus Validation Sets

5.2.1 Training Accuracy

Training accuracy detects how effectively the model is training the data.

5.2.2 Validation Accuracy

Validation accuracy measures how well the model is adjusting to new dataset.
If the training accuracy and validation accuracy are identical then it can said that the model has not been overfitted. However, if the validation accuracy is lower than training accuracy then it can be deduced that the model has been overfitted to the training dataset.

5.2.3 Training Loss

Training Loss is a measurement metric to detect how much error the model has made in order to fit the training data.

5.2.4 Validation Loss

Validation Loss is a measurement metric which is calculated after each epoch to validate the performance of the implemented model.
Similarly, if the value of training loss and validation loss are close to equal then it can be deduced that the model is working efficiently. However, if the validation loss value is higher than the training loss then the model shows the sign of overfitting.
To differentiate between the implemented models, it is necessary to analyze the results after training and testing the implemented models. To evaluate the performance of the implemented models, a comparison table is shown below based on the test accuracy, test loss, number of parameters, wall time.At first we tested on two target classes Gender and Hand so two different tables are shown :

Models	Number of parameters	Wall Time	Test Accuracy	Max Accuracy at Epoch Number
ResNet34	25567032	11min 23s	84.43%	23rd
ResNet50	21797672	22min 27s	82.50%	18th
RegNet_Y_3_2GF	19436338	48min 21s	82.19%	22nd

Table 5.1: Result analysis of hand and finger detection of the models

From table 5.1 it can be seen that the test accuracy of ResNet34 is highest of about 84.43% which depicts that this model can detect hand (Left/Right) and finger (Thumb/Index/Middle/Ring/Little) efficiently compared to other implemented models. However, RegNet_Y_3_2GF has the least accuracy rate of 82.19%
Additionally, wall time measurement is another evaluation metric which gives us an insight regarding the time complexity and computational cost of the implemented models. From the table 5.1 we see that ResNet34 takes least time of 11 minutes also gives the highest accuracy rate whereas RegNet_Y_3_2GF takes highest time of about 49 minutes but also provides the least accuracy among all of the implemented models.

Models	Number of parameters	Wall Time	Test Accuracy	Max Accuracy at Epoch Number
ResNet34	25567032	12min	84.43%	16th
ResNet50	21797672	23min 56s	82.24%	18th
RegNet_Y_3_2GF	19436338	50min 15s	84.95%	21st

Table 5.2: Result analysis of gender identification of the models

Here, Resnet50 has the least accuracy rate of 82.24% for gender identification compared to other models and RegNet_Y_3_2GF has the highest accuracy for gender classification which is 84.95%.
Finally, the wall time measurement of ResNet34 is 12 minutes which is minimum amongst the implemented models whereas RegNet_Y_3_2GF takes highest time of about 50 minutes compared to other implemented models.

5.2.5 Result Analysis using Graphs

The implemented models have given satisfactory results. However, the models can't still be labeled as good classifier because overfitting might be an issue when the implemented models get unseen data. Thus in order to make sure that the models are not overfitted, the graphs of training loss, validation loss and validation accuracy are shown below:

ResNet34

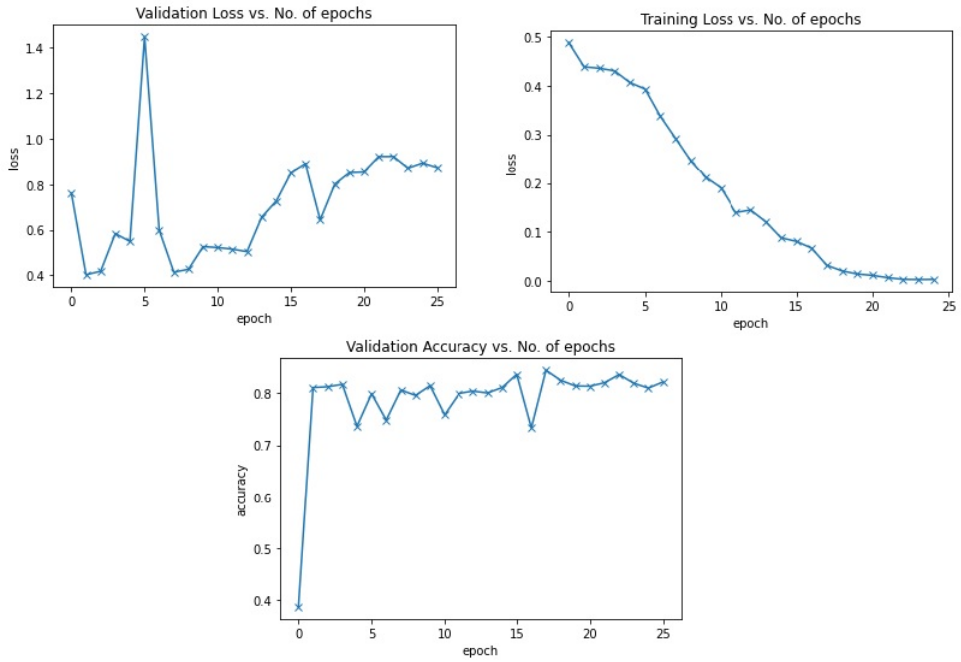


Figure 5.2: Training, Validation loss and Validation Accuracy graph of gender detection

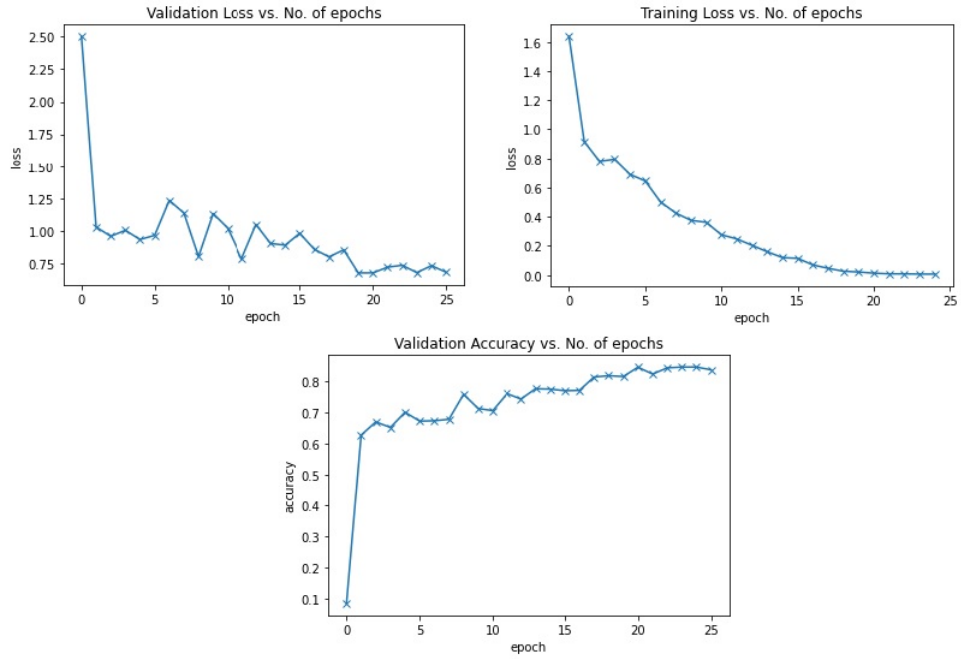


Figure 5.3: Training, Validation loss and Validation Accuracy graph of Hand and Finger identification

ResNet50

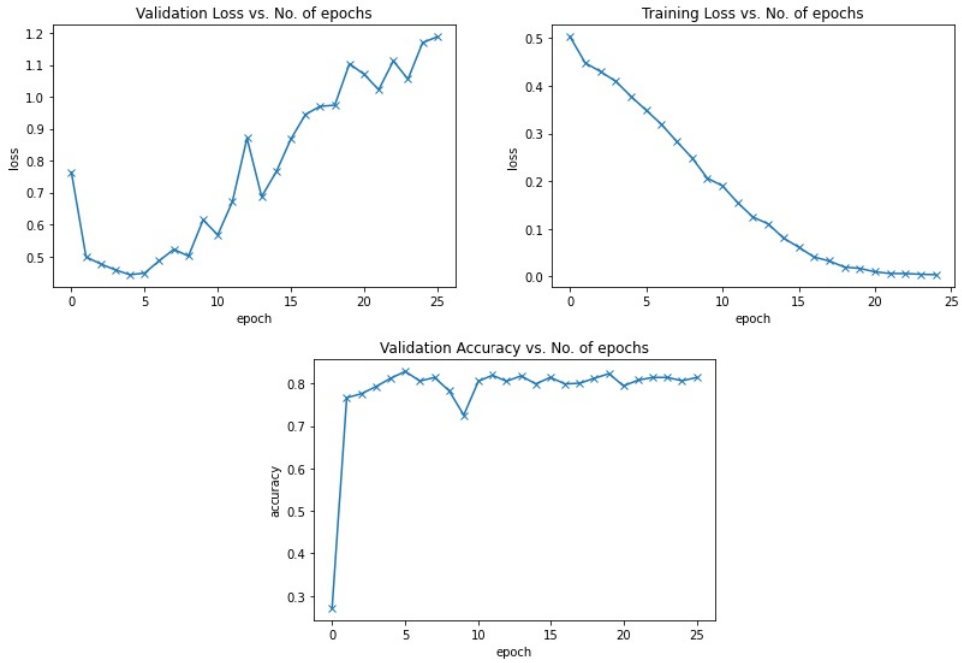


Figure 5.4: Training, Validation loss and Validation Accuracy graph of gender detection

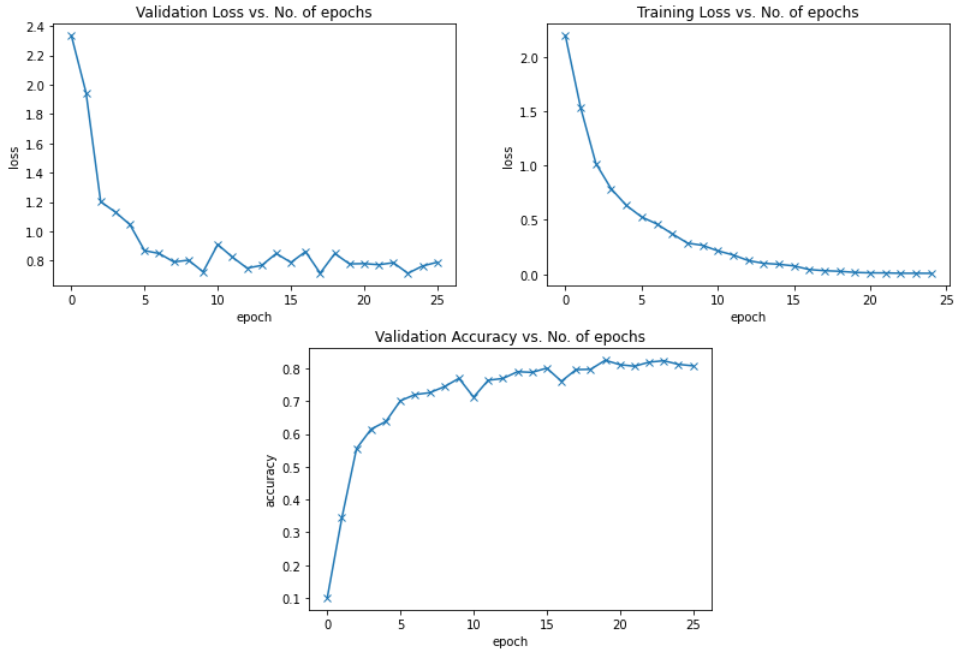


Figure 5.5: Training, Validation loss and Validation Accuracy graph of Hand and Finger identification

RegNet_Y_3_2GF

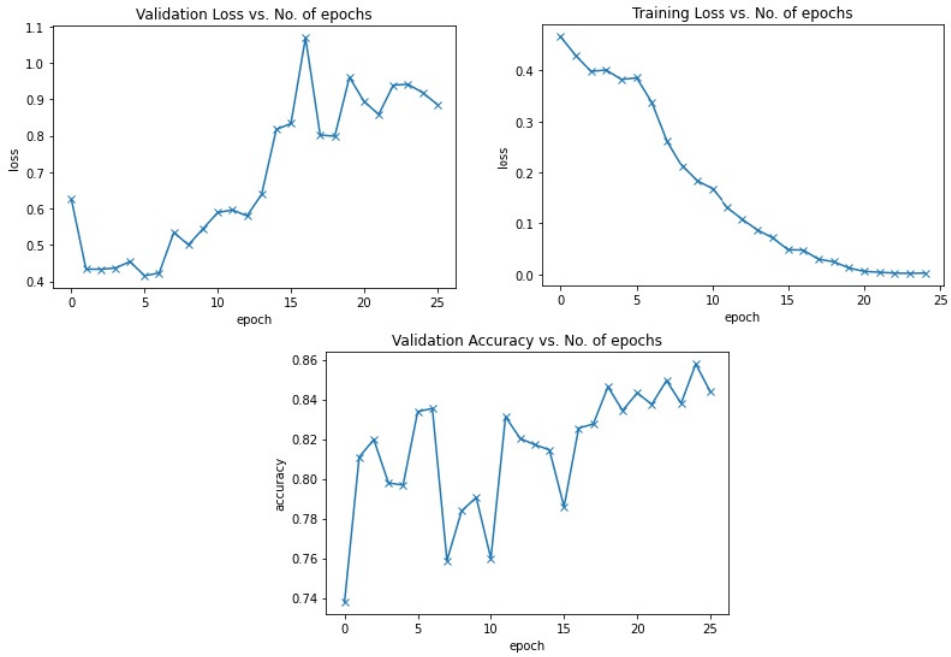


Figure 5.6: Training, Validation loss and Validation Accuracy graph of gender detection

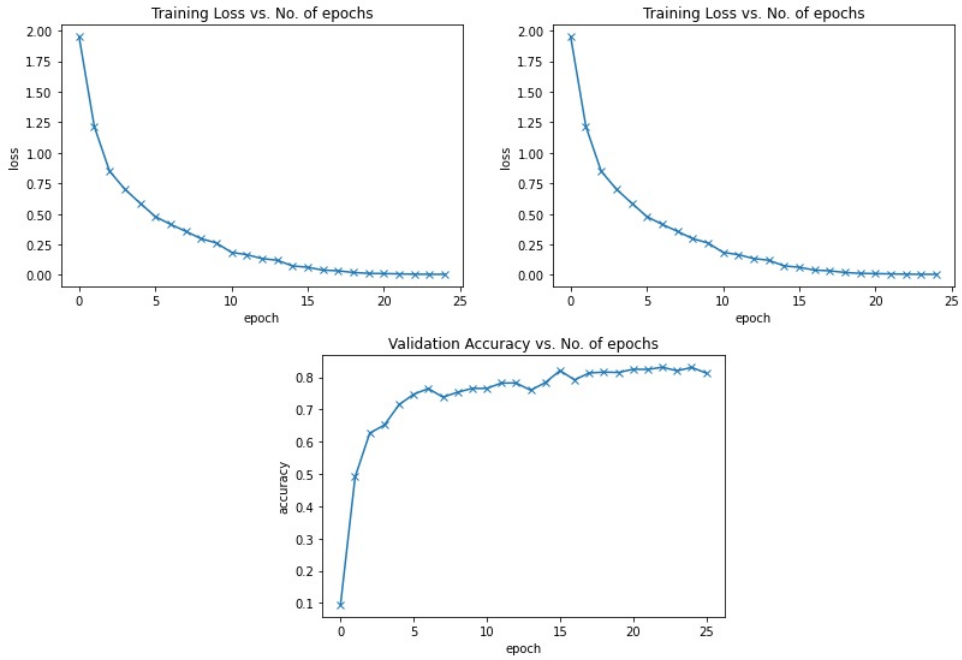


Figure 5.7: Training, Validation loss and Validation Accuracy graph of Hand and Finger identification

EfficientNet_V_2_S

Classification report

From the above graphs it can be seen that the implemented models have not given that much accuracy and also there are overfitting cases. In order to solve the problem, we have further implemented EfficientNet_V2_S and got high accuracy and the overfitting case has been solved too. Thus for classifying gender, hand, finger and identification of person we will use EfficientNet_V2_S. Classification reports after using EfficientNet_V_2_S have been shown below:

	precision	recall	f1-score	support
accuracy			0.9980	5527
macro avg	0.9982	0.9979	0.9978	5527
weighted avg	0.9982	0.9980	0.9980	5527

Figure 5.8: Classification report for Person class

	precision	recall	f1-score	support
0	0.9874	0.9919	0.9896	1107
1	0.9980	0.9968	0.9974	4420
accuracy			0.9958	5527
macro avg	0.9927	0.9944	0.9935	5527
weighted avg	0.9958	0.9958	0.9958	5527

Figure 5.9: Classification report for Gender class

Here, 0 represents female images and 1 represents male images

	precision	recall	f1-score	support
0	0.7365	0.7733	0.7545	300
1	0.9870	0.9841	0.9855	5227
accuracy			0.9727	5527
macro avg	0.8617	0.8787	0.8700	5527
weighted avg	0.9734	0.9727	0.9730	5527

Figure 5.10: Classification report for Hand class

Here, 0 represents left hand images and 1 represents right hand images

	precision	recall	f1-score	support
0	0.9963	0.9982	0.9972	1087
1	0.9963	0.9954	0.9959	1093
2	0.9946	0.9982	0.9964	1104
3	0.9955	0.9928	0.9941	1110
4	1.0000	0.9982	0.9991	1133
accuracy			0.9966	5527
macro avg	0.9965	0.9966	0.9966	5527
weighted avg	0.9966	0.9966	0.9966	5527

Figure 5.11: Classification report for Finger class

Here, 0 represents index finger images, 1 represents little finger images, 2 represents middle finger images, 3 represents ring finger images and 4 represents thumb finger images.

	precision	recall	f1-score	support
0	0.9015	0.9300	0.9155	600
1	0.9914	0.9876	0.9895	4927
accuracy			0.9814	5527
macro avg	0.9464	0.9588	0.9525	5527
weighted avg	0.9817	0.9814	0.9815	5527

Figure 5.12: Classification report for Alteration class

Here, in our main dataset there are total 6000 images and for the alteration class there are more than 6000 images. The first 6000 images are not altered so if the index is less than 6000 label is set to 0 and if index is more than 6000 label is set to 1.
An overall table has been shown below where the accuracy, precision, recall and epoch value have been shown at which we got the highest accuracy:

	Person	Gender	Hand	Finger	Alteration
Accuracy	99.80%	99.73%	97.09%	99.66%	98.61%
Precision	99.82%	99.73%	97.12%	99.66%	98.61%
Recall	99.80%	99.73%	97.07%	99.66%	98.61%
Epoch	28	49	22	31	36

Graphs

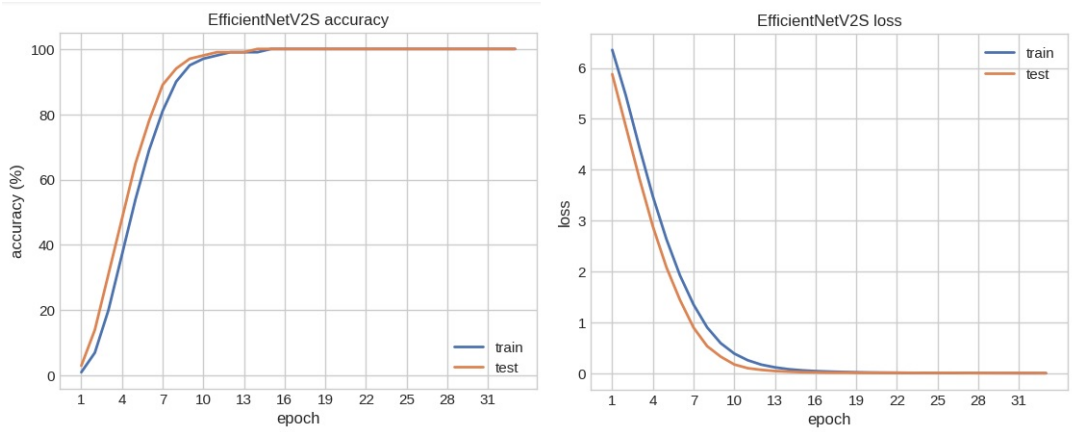


Figure 5.13: Graph for Person class

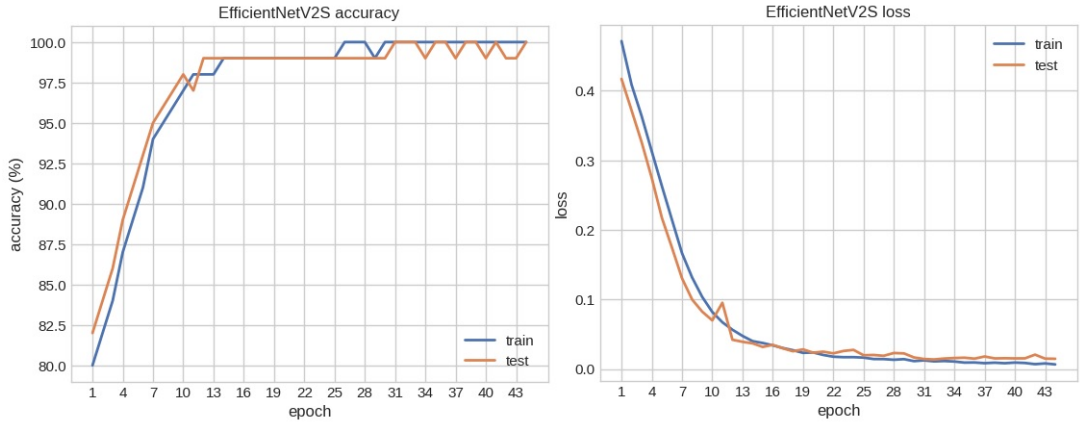


Figure 5.14: Graph for Gender class

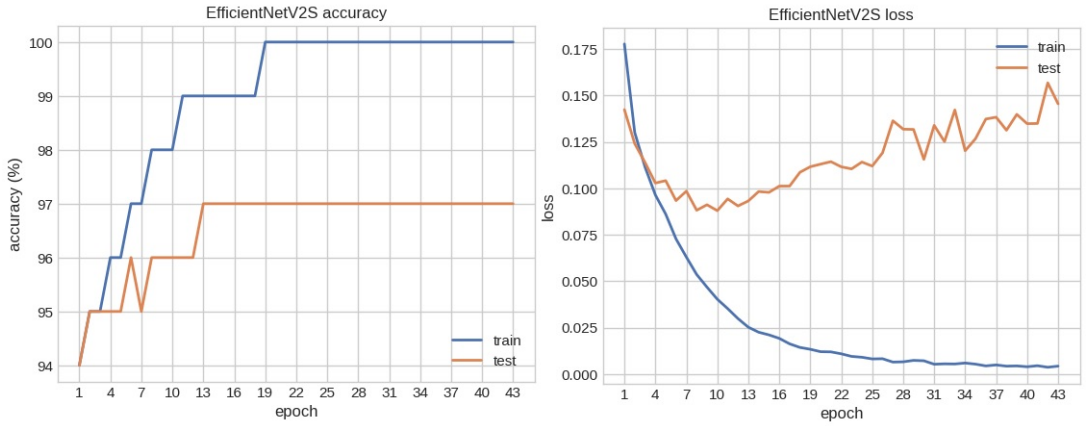


Figure 5.15: Graph for Hand class

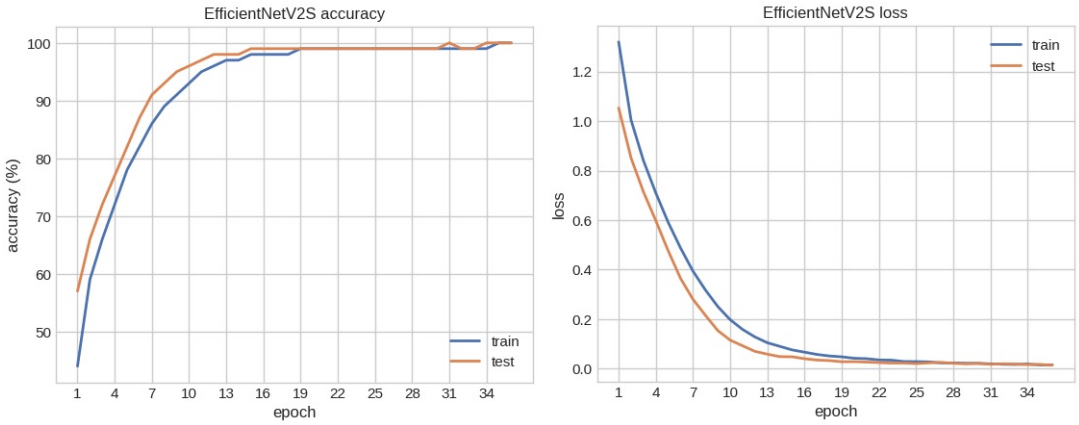


Figure 5.16: Graph for Finger class

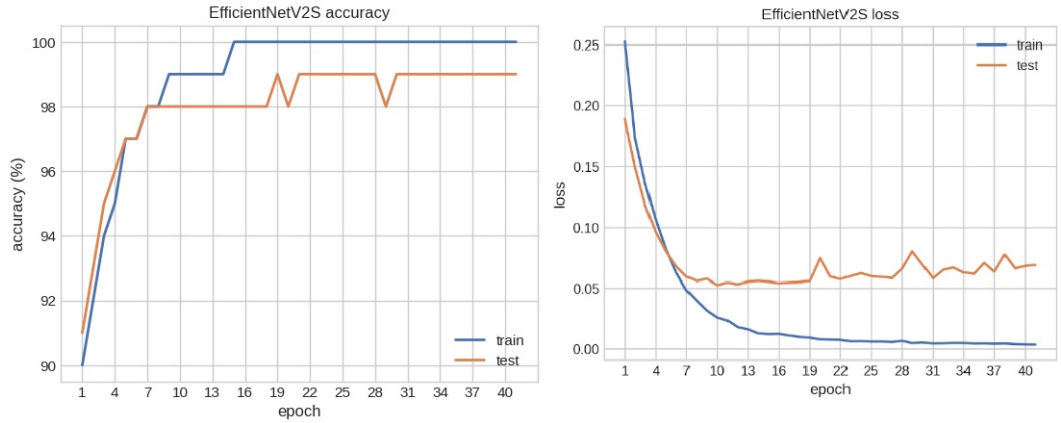


Figure 5.17: Graph for Alteration class

5.3 Analysis of result of One Shot Learning

The main purpose of using one shot learning is to get rid off the hassle of re-training the whole model again when a new entry has to be done in the database. That is why just for person identification, one shot learning has been implemented for training the dataset because new labels will be there if a new entry has to be done. For training the model, the triplet function has been used. However, for the case of gender, hand and finger classification there is no need to apply one shot learning as no new labels are there except for the already declared ones. The working principle of one shot learning is it measures the distance between the pixels and compare the result with the threshold value. For the Socofing Dataset, the threshold value is set to 0.75. If the measured distance of the input image is equal or less than the threshold value then it refers that the image is already there in the database whereas if the measured distance is more than the threshold value then a new image has been put which is not present in the dataset. Then as the main model InceptionV3 has been used.

To scrutinize the result of one shot application on the dataset, a comparison has been done with the images of same person and the image of different person.

For the same person's fingerprints, the measured distance is 0.438806 which is less

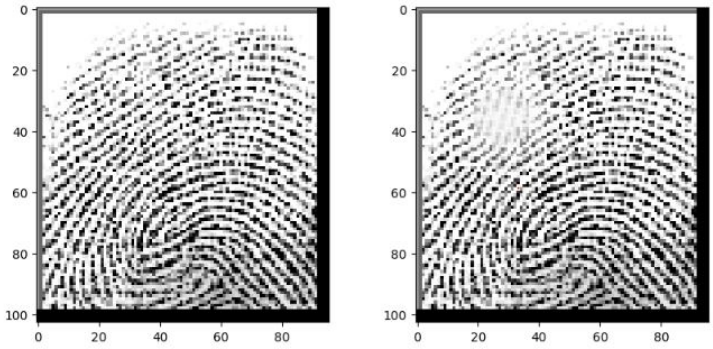


Figure 5.18: Fingerprints of same person

than the threshold value. Thus it can be said that the both fingerprints belong to the same person.

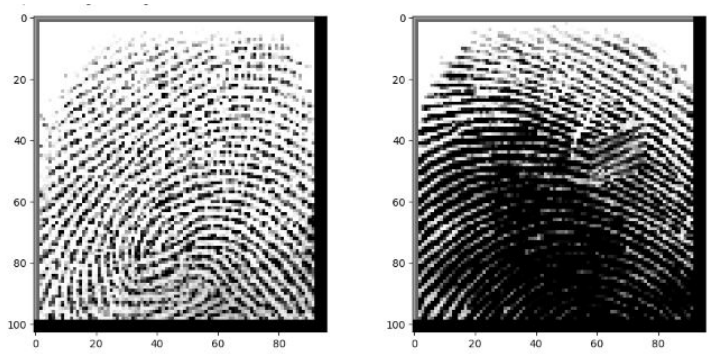


Figure 5.19: Fingerprints of different person

For the different persons fingerprints, the measured distance is 1.0990736 which is more than the threshold value. Thus it can be said that the both fingerprints belong to different person.
Now to check the performance of one shot learning on the dataset, more than 100 random images have been picked and matched with the results of one shot learning.

	precision	recall	f1-score	support
0	0.9608	0.8448	0.8991	58
1	0.8657	0.9667	0.9134	60
accuracy			0.9068	118
macro avg	0.9132	0.9057	0.9062	118
weighted avg	0.9124	0.9068	0.9064	118

Figure 5.20: Classification report of One Shot Learning

Here 0 represents two different images and 1 represents same images.

5.4 Comparison Of Other Works With Ours On SOCOFing Dataset

A lot models have been working on the SOCOFing dataset for the purpose of Fingerprint identification recently. We have compared our result with several works done between 2018-2021. Each work focused on identifying one or more classes which are identification of person, gender, hand , finger and altered and/or fake images. However, our work featured the identification of person as it is a key class in our One Shot learning model. The below Figure5.21 can be helpful to illustrate the comparison of results of our works with the works of [62],[59],[65],[52],[60] and [45] .

Title-Publication Year (Authors Last Name)	Accuracy				
	Person	Gender	Hand	Finger	Altered and/Or Fake Images
Detailed Identification of Fingerprints Using Convolutional Neural Networks-2018 (Shehu, Garcia , Palade & James)	N/A	75.2%	93.5%	76.72%	N/A
Fingerprint Identification using Modified Capsule Network-2021 (Sing, Bhisikar,Satakshi,Kumar)	N/A	99%	99%	99%	N/A
Fingerprint Classification Using Transfer Learning Technique-2021 (Aliweiwi)	N/A	N/A	N/A	N/A	1st Model: 99.4% 2nd Model: 97.5%
Integrated Different Fingerprint Identification and Classification Systems based Deep Learning-2022 (Oleiwi, Abood , Farhan)	N/A	99.96%	99.93%	99.9%	N/A
Single Architecture and Multiple task deep Neural Network for Altered Fingerprint Analysis-2020	N/A	92.52%	97.53%	92.18%	Fakeness : 98.21% Alteration : 98.46%
Fingerprint Alterations Type Detection and Gender Recognition Using Convolutional Neural Networks and Transfer Learning-2021 (Kataria,Gupta,Kaushik,Chaudhury,Gupta)	N/A	83.07%	N/A	N/A	Alteration : 98.50% Alteration Detection: 94.84%
Comprehensive Fingerprint Recognition Utilizing One Shot Learning with Siamese Network (Our Model)	99.8%	99.73%	97.09%	99.6%	98.61%

Table 5.3: Comparison of works done on SOCOFing Dataset

5.5 Conclusion and Future Directives

Utilization of fingerprints in terms of bio-metric validation, security and verification is ,as mentioned already, one of the most popular bio-metric systems. In our paper, we have depicted one shot learning that addresses several ongoing issues, if standard methodologies are followed. Through the implication of one shot learning using Inception V3, we demonstrated that our implication does not require additional retrain for each time the quantity of input images is changed. This is possible because One Shot Learning does not concern with the classification problem, rather our system proposes difference evaluation between the features of two input images, a reference image already stored and a new/altered/similar test image. Instead of inputting multiple images for a specific class , our implementation requires only one reference image stored into the database. It then compares another test image and lastly produces a similarity report. This hassle of not retraining for dynamic classes as well as providing a large quantity of input images is possible due to one shot learning utilizing Siamese Neural Network. In our work, we have utilized a Triplet Loss function to train the Siamese Neural Network and allowed the network to tune the parameters to identify the correct images. Thus using Siamese Neural Network, our method is able to correctly identify the test fingerprint images. In our work, we have tested our designed system on a labeled dataset based on SOCOFing dataset. To measure the success of accurate classification based on the similarity report, we have generated an accuracy where our design showed above 90 percent accuracy. Besides the implementation of One Shot Learning we recognized Person's ID, Person's Gender, Person's Hand, Person's Finger and lastly Person's Altered fingerprint ; from a person's fingerprint with very high accuracy using EfficientNetV2s. Our classification report for the above mentioned classes showed an almost perfect accuracy number. To conclude, based on our work done , we can predict that using our one shot learning model will largely reduce the network complexity as our model requires only one sample fingerprint of a person. Moreover, our model does not require retraining the network due to change in classes allowing the organizations to implement the model in a very cost-effective manner. Besides, our high classification accuracy can ensure a very accurate identification of an unknown person which is very crucial in forensic and medical environments. Especially in terms of criminal cases where getting lots of sample fingerprints is an issue, our system can very efficiently solve that problem with very limited resources. Our implementation greatly strengthens the popular fingerprint verification system in a very cost effective manner ensuring highest utility and security.In the future, we want to implement our model on other biometric applications as well. We are looking forward to implement one shot learning to identify breathing of a person as breathing pattern is unique for each person. We also want to differentiate between healthy and unhealthy breathing based off that.

Bibliography

[1] H. Cummins, W. J. Waits, and J. T. McQuitty, "The breadths of epidermal ridges on the finger tips and palms: A study of variation," *American journal of Anatomy*, vol. 68, no. 1, pp. 127–150, 1941.

[2] V. N. Vapnik, "An overview of statistical learning theory," *IEEE transactions on neural networks*, vol. 10, no. 5, pp. 988–999, 1999.

[3] G. Levin, "Real world, most demanding biometric system usage," *Proc. Biometrics Consortium*, vol. 2, pp. 14–15, 2001.

[4] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.

[5] J. Picard, C. Vielhauer, and N. Thorwirth, "Towards fraud-proof id documents using multiple data hiding technologies and biometrics," in *Security, Steganography, and Watermarking of Multimedia Contents VI*, SPIE, vol. 5306, 2004, pp. 416–427.

[6] J. Wayman, A. Jain, D. Maltoni, and D. Maio, "An introduction to biometric authentication systems," in *Biometric Systems: Technology, Design and Performance Evaluation*, J. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds. London: Springer London, 2005, pp. 1–20, ISBN: 978-1-84628-064-1. DOI: 10.1007/1-84628-064-8_1. [Online]. Available: https://doi.org/10.1007/1-84628-064-8_1.

[7] N. Acır, "A support vector machine classifier algorithm based on a perturbation method and its application to ecg beat recognition systems," *Expert Systems with Applications*, vol. 31, no. 1, pp. 150–158, 2006.

[8] R. Jayadevan, J. V. Kulkarni, S. N. Mali, and H. K. Abhyankar, "A new ridge orientation based method of computation for feature extraction from fingerprint images," *Transactions on Engineering, Computing and Technology*, vol. 13, pp. 201–206, 2006.

[9] J. Zhang, Z. Ou, and H. Wei, "Fingerprint matching using phase-only correlation and fourier-mellin transforms," in *Sixth International Conference on Intelligent Systems Design and Applications*, vol. 2, 2006, pp. 379–383. DOI: 10.1109/ISDA.2006.253866.

[10] M. Dabbah, W. Woo, and S. Dlay, "Secure authentication for face recognition," in *2007 IEEE Symposium on Computational Intelligence in Image and Signal Processing*, IEEE, 2007, pp. 121–126.

[11] J. Galbally Herrero, J. Fierrez, and J. Ortega-Garcıa, "Vulnerabilities in biometric systems: Attacks and recent advances in liveness detection," -, 2007.

[12] M. Sudesh Gungadin, "Sex determination from fingerprint ridge density," *Internet Journal of Medical Update*, vol. 2, no. 2, 2007.

[13] Y. Bengio, J. Louradour, R. Collobert, and J. Weston, "Curriculum learning," in *Proceedings of the 26th annual international conference on machine learning*, 2009, pp. 41–48.

[14] H. Kikuchi, K. Funahashi, and S. Muramatsu, "Simple bit-plane coding for lossless image compression and extended functionalities," in *2009 Picture Coding Symposium*, 2009, pp. 1–4. DOI: 10.1109/PCS.2009.5167351.

[15] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Transactions on knowledge and data engineering*, vol. 22, no. 10, pp. 1345–1359, 2009.

[16] B. Acharya, M. D. Sharma, S. Tiwari, and V. K. Minz, "Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem," *Procedia Computer Science*, vol. 2, pp. 242–247, 2010.

[17] A. Nagar, K. Nandakumar, and A. K. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates," *Pattern recognition letters*, vol. 31, no. 8, pp. 733–741, 2010.

[18] K. Arun and K. Sarath, "A machine learning approach for fingerprint based gender identification," in *2011 IEEE Recent Advances in Intelligent Computational Systems*, IEEE, 2011, pp. 163–167.

[19] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Systems with Applications*, vol. 39, no. 7, pp. 6562–6574, 2012.

[20] B. Prasanalakshmi, A. Kannammal, B. Gomathi, K. Deepa, and R. Sridevi, "Biometric cryptosystem involving two traits and palm vein as key," *Procedia Engineering*, vol. 30, pp. 303–310, 2012.

[21] A. M. Canuto, F. Pintro, and J. C. Xavier-Junior, "Investigating fusion approaches in multi-biometric cancellable recognition," *Expert Systems with applications*, vol. 40, no. 6, pp. 1971–1980, 2013.

[22] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," *Expert Systems with Applications*, vol. 40, no. 5, pp. 1888–1901, 2013.

[23] T. Can, "Introduction to bioinformatics," in *miRNomics: MicroRNA Biology and Computational Analysis*, Springer, 2014, pp. 51–71.

[24] L. Cozzella and G. S. Spagnolo, "Phase-only correlation function by means of hartley transform," 2014.

[25] C. Rathgeb and C. Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters," *Computers & Security*, vol. 42, pp. 1–12, 2014.

[26] M. D. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," in *European conference on computer vision*, Springer, 2014, pp. 818–833.

[27] A. Ali, R. Khan, I. Ullah, A. D. Khan, and A. Munir, "Minutiae based automatic fingerprint recognition: Machine learning approaches," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, IEEE, 2015, pp. 1148–1153.

[28] R. Jain and C. Kant, "Attacks on biometric systems: An overview," *International Journal of Advances in Scientific Research*, vol. 1, no. 07, pp. 283–288, 2015.

[29] H. Kaur and P. Khanna, "Gaussian random projection based non-invertible cancelable biometric templates," *Procedia Computer Science*, vol. 54, pp. 661–670, 2015.

[30] C. Lemke, M. Budka, and B. Gabrys, "Metalearning: A survey of trends and technologies," *Artificial intelligence review*, vol. 44, no. 1, pp. 117–130, 2015.

[31] V. Nıdlová and J. Hart, "Reliability of identification based on fingerprints in dual biometric identification systems," in *Applied Mechanics and Materials*, Trans Tech Publ, vol. 752, 2015, pp. 1040–1044.

[32] K. Tiwari and P. Gupta, "Indexing fingerprint database with minutiae based coaxial gaussian track code and quantized lookup table," in *2015 IEEE International Conference on Image Processing (ICIP)*, IEEE, 2015, pp. 4773–4777.

[33] B. Arslan, E. Yorulmaz, B. Akca, and S. Sagiroglu, "Security perspective of biometric recognition and machine learning techniques," in *2016 15th IEEE international conference on machine learning and applications (ICMLA)*, IEEE, 2016, pp. 492–497.

[34] K. Cao and A. K. Jain, "Hacking mobile phones using 2d printed fingerprints," *Michigan State University, Tech. Rep. MSU-CSE-16-2*, 2016.

[35] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[36] T. Z. Lee and D. B. Bong, "Analysis of bit-plane images by using principal component on face and palmprint database," *Pertanika Journal of Science and Technology*, vol. 24, no. 1, pp. 191–203, 2016.

[37] S. Papi, M. Ferrara, D. Maltoni, and A. Anthonioz, "On the generation of synthetic fingerprint alterations," in *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*, IEEE, 2016, pp. 1–6.

[38] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Jun. 2016.

[39] R. Wang, C. Han, and T. Guo, "A novel fingerprint classification method based on deep learning," in *2016 23rd International Conference on Pattern Recognition (ICPR)*, IEEE, 2016, pp. 931–936.

[40] F. Francis-Lothai and D. B. Bong, "A fingerprint matching algorithm using bit-plane extraction method with phase-only correlation," *International Journal of Biometrics*, vol. 9, no. 1, pp. 44–66, 2017.

[41] L. Ghiani, D. A. Yambay, V. Mura, G. L. Marcialis, F. Roli, and S. A. Schuckers, "Review of the fingerprint liveness detection (livdet) competition series: 2009 to 2015," *Image and Vision Computing*, vol. 58, pp. 110–128, 2017.

[42] J. Sheetlani, R. Pardeshi, *et al.*, "Fingerprint based automatic human gender identification," *Int. J. Comput. Appl*, vol. 170, no. 7, pp. 1–4, 2017.

[43] J. J. Engelsma, K. Cao, and A. K. Jain, "Raspireader: Open source fingerprint reader," *IEEE transactions on pattern analysis and machine intelligence*, vol. 41, no. 10, pp. 2511–2524, 2018.

[44] A. He, C. Luo, X. Tian, and W. Zeng, "A twofold siamese network for real-time object tracking," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 4834–4843.

[45] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, "Detailed identification of fingerprints using convolutional neural networks," in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2018, pp. 1161–1165. DOI: 10.1109/ICMLA.2018.00187.

[46] G. Arora, R. R. Jha, A. Agrawal, K. Tiwari, and A. Nigam, "Sp-net: One shot fingerprint singular-point detector," *arXiv preprint arXiv:1908.04842*, 2019.

[47] P. Gupta, K. Tiwari, and G. Arora, "Fingerprint indexing schemes–a survey," *Neurocomputing*, vol. 335, pp. 352–365, 2019.

[48] H. T. Nguyen and L. T. Nguyen, "Fingerprints classification through image analysis and machine learning method," *Algorithms*, vol. 12, no. 11, p. 241, 2019.

[49] I. Radosavovic, J. Johnson, S. Xie, W.-Y. Lo, and P. Dollár, "On network design spaces for visual recognition," in *Proceedings of the IEEE/CVF international conference on computer vision*, 2019, pp. 1882–1890.

[50] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *International conference on machine learning*, PMLR, 2019, pp. 6105–6114.

[51] F. Alqahtani and R. Zagrouba, "Fingerprint spoofing detection using machine learning," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, IEEE, 2020, pp. 1–7.

[52] O. Giudice, M. Litrico, and S. Battiato, "Single architecture and multiple task deep neural network for altered fingerprint analysis," in *2020 IEEE International Conference on Image Processing (ICIP)*, 2020, pp. 813–817. DOI: 10.1109/ICIP40778.2020.9191094.

[53] S. Gupta and B. Akin, "Accelerator-aware neural network design using automl," *arXiv preprint arXiv:2003.02838*, 2020.

[54] S. Kadam and V. Vaidya, "Review and analysis of zero, one and few shot learning approaches," in *Intelligent Systems Design and Applications: 18th International Conference on Intelligent Systems Design and Applications (ISDA 2018) held in Vellore, India, December 6-8, 2018, Volume 1*, Springer, 2020, pp. 100–112.

[55] H.-A. Pho, S. Lee, V.-N. Tuyet-Doan, and Y.-H. Kim, "Radar-based face recognition: One-shot learning approach," *IEEE Sensors Journal*, vol. 21, no. 5, pp. 6335–6341, 2020.

[56] I. Radosavovic, R. P. Kosaraju, R. Girshick, K. He, and P. Dollár, "Designing network design spaces," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 10 428–10 436.

[57] K. A. Shastry and H. A. Sanjay, "Machine learning for bioinformatics," in *Statistical Modelling and Machine Learning Principles for Bioinformatics Techniques, Tools, and Applications*, K. G. Srinivasa, G. M. Siddesh, and S. R. Manisekhar, Eds. Singapore: Springer Singapore, 2020, pp. 25–39. DOI: 10.1007/978-981-15-2445-5_3. [Online]. Available: https://doi.org/10.1007/978-981-15-2445-5_3.

[58] E. E. B. Adam, "Evaluation of fingerprint liveness detection by machine learning approach-a systematic view," *Journal of ISMAC*, vol. 3, no. 01, pp. 16–30, 2021.

[59] A. H. Aloweiwi, "Fingerprint classification using transfer learning technique," 2021.

[60] G. Kataria, A. Gupta, V. S. Kaushik, G. Chaudhary, and V. Gupta, "Fingerprint alterations type detection and gender recognition using convolutional neural networks and transfer learning," in *Computational Intelligence for Information Retrieval*, CRC Press, 2021, pp. 237–255.

[61] H. Shao, D. Zhong, X. Du, S. Du, and R. N. Veldhuis, "Few-shot learning for palmprint recognition via meta-siamese network," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–12, 2021.

[62] T. Singh, S. Bhisikar, Satakshi, and M. Kumar, "Fingerprint identification using modified capsule network," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2021, pp. 1–6. DOI: 10.1109/ICCCNT51525.2021.9580009.

[63] M. Tan and Q. Le, "Efficientnetv2: Smaller models and faster training," in *International Conference on Machine Learning*, PMLR, 2021, pp. 10 096–10 106.

[64] Netscope, "Resnet-50 architecture," in *Architecture of ResNet-50*, 2022.

[65] B. K. Oleiwi, L. H. Abood, and A. K. Farhan, "Integrated different fingerprint identification and classification systems based deep learning," in *2022 International Conference on Computer Science and Software Engineering (CSASE)*, 2022, pp. 188–193. DOI: 10.1109/CSASE51777.2022.9759632.