Template Protection of Palm Veins and Prints Using Transform Based Cancelable Biometrics

By

Anum Aftab

Reg No: 00000276042

Supervisor

Dr. Haider Abbas

A thesis submitted in conformity with the requirements for the degree of *Master of Science* in Information Security

Department of Information Security

Military College of Signals (MCS)

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

February 2022

Declaration

I, *Anum Aftab* declare that this thesis titled "Template Protection of Palm Veins and Prints Using Transform Based Cancelable Biometrics" and the work presented in it are my own and has been generated by me as a result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a Master of Science degree at NUST
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at NUST or any other institution, this has been clearly stated
3. Where I have consulted the published work of others, this is always clearly attributed
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work
5. I have acknowledged all main sources of help
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself

---

Anum Aftab,

Reg No: 00000276042

Copyright Notice

This thesis is dedicated to *my beloved parents and dear husband.*

Abstract

Lately identity management has been fully digitized due to which the work on biometrics has gained significant popularity. An increase in the adoption of biometrics in identity management means that sensitive data of the individuals can be easily compromised if unauthorized access is granted to the systems. This can lead to legal issues as it leads to an infringement of privacy of the people. In this context, the use of tokens, personal identification numbers and passwords is deemed inadequate for protecting the personal data of the people. This has stimulated research in domain of template protection and use of various methods has been adopted for protecting the biometric templates of the individuals. In this thesis, we have adopted 'Cancelable Biometrics' for template protection using transform based methods. We have used Gabor filtering prior to feature extraction as it is a non-invertible transform and satisfies one of the key requirements (non-invertibility) of the templates. Gabor filtering is followed by feature extraction using the VGG19 network trained using 'imagenet' weights. The templates obtained still are not able to satisfy a key requirement (unlinkability) which is achieved by using random projection performed for every user using a 'key'. If compromised, the existing template can be revoked and a new template can be obtained using another key, leading to a unique set of features for the same user. We have performed our experiments on the Multispectral Palm Image Dataset (CASIA). Our experiments show that the proposed method outperforms the other methods that have been considered in this thesis. The method has been analyzed with respect to privacy with theoretical evidence for non-orthogonality of the templates, and empirical evidence for unlinkability using the T-test.

Keywords: *Gabor filters, Cancelable Biometrics, Random Projection*

Acknowledgments

I would like to thank God Almighty, for letting me through all the difficulties. It was not easy especially after the loss of my dear mother but day by day you have given me strength to stand up and get going. You are the one who has let me finish my degree. I have always trusted you and will keep on trusting you.

I would like to acknowledge my supervisor Dr. Haider Abbas for his continuous support of my MS study and research. It is he who made this work possible.

I would also like to thank my committee members Maj Sohaib Khan Naizi and Dr. Waseem Iqbal for their encouragement and cooperative attitude.

Last but not the least, i would like to give special thanks to my dear husband for always standing by side and supporting me. Thanks to all my family members for their continuous support. Without you none of this would indeed be possible.

Contents

List of Figures

List of Tables

List of Abbreviations and Symbols

Abbreviations

ARM	Attacks via Record Multiplicity
AWGN	Additive White Gaussian Noise
BCs	Biometric Cryptosystems
BCH	Bose Chaudhuri Hocquenghem
CASIA	Chinese Academy of Sciences Institute of Automation
CB	Cancelable Biometrics
CNN	Convolutional Neural Network
EER	Equal Error Rate
PIN	Personal Identification Number
FA	False Accept
FR	False Reject
TA	True Accept
TR	True Reject
FAR	False Accept Rate
FRR	False Reject Rate

PIN	Personal Identification Number
PCA	Principal Component Analysis
PRN	Pseudo Random Number
ReLU	Rectified Linear Unit
RP	Random Projections
SSH	Secure Shell
NIR	Near Infrared
VGG	Visual Geometry Group

Chapter 1

Introduction

Biometrics is a mature technology by this time and has been investigated since long by various researchers. Over the last decade, there has been a large number of practical applications in which biometrics have been employed. Currently, the solutions using biometrics are providing support in our daily lives. Initially the technology was used only on large scale systems such as usage by the governments for managing citizens or managing personal presence of individuals in their respective organizations etc. However over a period of time, the technology has become widespread covering a very broad base of users and providing security features on their personal devices such as smart phones. This adoption of biometrics has been made possible mainly due to the fact that the size and cost of semiconductor technology has significantly reduced creating a scope of a wider deployment of biometrics for an even wider range of applications.

Despite an exponential growth in biometrics, an obvious question is that is the technology mature enough to provide robust solutions in all scenarios? and the answer to the best of our knowledge is that, certainly not. With the passage of time, there are more issues that need to be tackled over the horizon and we are still a long way from an absolute adoption of this technology with several issues revolving around biometrics. Traditionally, a single biometric trait was used for the purposes of authentication and most of the systems that have been developed and deployed by this time make use of only a single trait in order to perform authentication of the individuals. However over a period of time, there have been several attacks carried out on the biometrics systems, leaving a lot of room for improvement as far as the security is concerned.

It is worth mentioning that the global biometrics market value which is currently valued

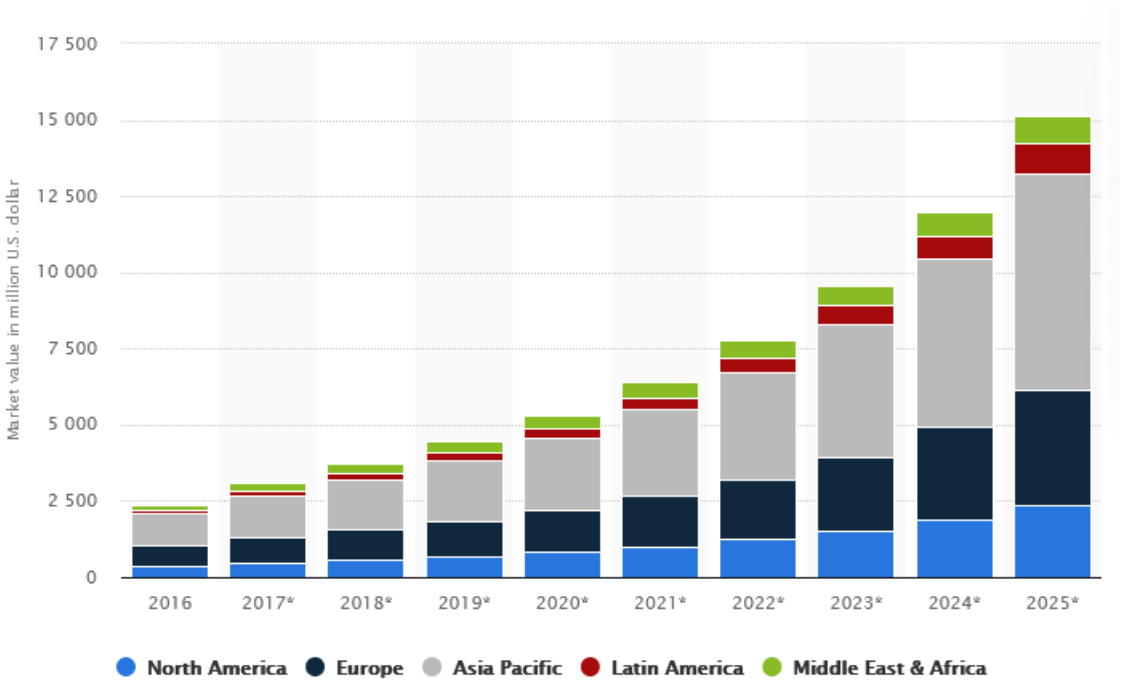

Figure 1.1: The graph shows the global biometrics market value in 2016 and a forecast from 2017 to 2025, by region. In 2025, the North American biometrics market is expected to amount to about 2.4 billion U.S. dollars in size.

at a couple of thousand million US Dollars is expected to yield a sharp raise over the next couple of years, given the widespread usage of this technology. This growing usage is expected to raise several issues for the users. These issues are mainly attributed to the fact that smart devices used by the users are randomly connected to the unknown networks, exposing the devices to several vulnerabilities. These might include stealing, forging, spoofing etc. which is a growing issue for any underlying biometric system. Given this, there is a need to devise strategies to tackle these issues to ensure safety of the user's data.

1.1 Research Goals

Personal Identification Number (PINs), tokens and passwords have become inadequate for the identity protection owing to increase in number of cyberattacks. With the increase in popularity for a biometric in providing a secure user authentication, it has become very crucial to protect the user data stored in the biometric system from the adversaries. In this thesis, the biometric data is made secure through the technique

called 'Cancelable Biometrics'.

Cancelable Biometrics (CB) refer to a wide range of techniques that integrate security of biometric template. According to [4], "Cancelable biometrics refers to a systematic and intentional repeated distortion of biometric features in order to protect sensitive user-specific data". The term 'Cancelable' depicts the ability of the template of being cancelled if lost or stolen. In that case, a new version of the original biometric is distorted to form another unique representation. It is important note that user verification is carried out in the transformed domain.

1.2 Motivation

A multibiometric system uses multiple biometric traits (e.g., fingerprint, face, and fingervein) to recognize a person [5], hence improving the reliability and accuracy of biometric systems. However, adequate attention has not been paid towards making the multibiometric templates secure. There are several ways to compromise a biometric system [4] and loss of a biometric template information to unauthorized individuals possesses security and privacy threats [6, 7] due to following reasons:

- *Intrusion attack at biometric system:* If an adversary gets an unauthorised access into a biometric system he can easily access the stored biometric template of a user. This information can be used to get an illegal entrance into the biometric system in which user is enrolled by either reverse engineering the template and disguising as this user or replaying the stolen template.
- *Database Linkage*: Once an adversary gets hold of a template it can be easily determined if the two templates from different databases belong to the same person or not. Moreover different databases hold separate parts of data regarding that person. Consequently leading to more data theft and more difficult identity-related attacks.

1.3 Scope of Work

In this thesis, we will focus on the use of hand biometric traits in order to design an authentication system. We will focus on a cancelable multibiometric system to ensure that

the templates are properly stored without the possibility of easily being able to spoof the system. The use of multiple traits ensures that the system does not rely on a single biometric trait to perform authentication as it is easy to spoof one trait. By using multiple traits, the user requires an input from at least two of his physiological/behavioral traits making it difficult to spoof two distinct traits. A second layer of protection is added in feature extraction where concatenation of features is required leading to an extended feature vector for validation. A third layer of protection is executed by ensuring that the feature extraction performed on the biometric traits is cancelable, leading to a system which is more robust to attacks carried out on the biometric systems.

1.4 Rationale of work

In this thesis, we will focus on the design of a hand based multibiometric system. The use of hand modalities exhibits numerous advantages over the use of other biometrics traits such as iris etc., which are considered one of the most accurate and distinctive biometric traits: hand based modalities are very accurate for recognition, typically use of cheap technology, are computationally less expensive for matching and less sensitive to the imaging conditions. Moreover, the hand based modalities are very robust for matching as they are insensitive to emotions and other behavioral properties of the individuals e.g. stress, tiredness etc. Given this, it is clear that with respect to some specific aspects, the employment of hand based modalities is superior in comparison to others for biometric authentication.

1.5 Main Contributions

The main contributions of the thesis are as follows:

- **Review of existing literature:** We have performed an extensive review of hand based multibiometric systems for two important aspects i.e., feature extraction and template security. The literature has been analyzed and a taxonomy has been proposed to categorize the various methods based on the methodologies employed by the authors. Appropriately, the conclusions and directions of future work have been carefully carved.

- **Feature extraction from biometric traits:** Based on the underlying trends currently being followed for feature extraction for biometric systems, we make use of convolutional neural network to perform the said task. Although, the commonly used VGG19 network is employed for feature extraction the images are subjected to pre-filtering using Gabor filters, highlighting the important features in the images before feeding them to the CNN.

- **Validate the characteristics of cancelable biometrics:** We have validated the cancelable property of the proposed method by proving that the proposed feature extraction method conforms to the two fundamental properties, which are a requisite requirement of the system i.e., irreversability and unlinkability. Promising arguments to validate these properties have been presented in the thesis.

- **Experimental validation of proposed methods:** The proposed methodology has been validated on the CASIA multispectral palm print dataset. The experiments have shown very good results of authentication while maintaining important features to ensure the cancelable nature of the proposed methods.

1.6 Thesis Organization

The thesis is organized as follows:

We discuss about the various hand based biometric traits and their literature review in chapter 2 and discuss briefly about Gabor filters and Convolutional Neural Networks in chapter 3. Later, we discuss the proposed methodology in chapter 4, present our experimental results in chapter 5 and finally conclude the thesis with the relevant findings in chapter 6.

Chapter 2

Background and Literature Review

2.1 Biometric Technology Fundamentals

Biometric authentication is used more than ever for authentication of individuals in a wide range of security applications. The reliance of systems on physiological attributes of the users has lately offered more simplicity and reliability at the same time. This has helped in avoiding many problems associated with the systems where passwords/credentials are being used, which can potentially incur some problems such as forgotten passwords, transferred or stolen credentials. The use of biometrics has led to mitigate these problems significantly given that the individual with specific biometric traits is required to validate access to the systems to avoid the above mentioned problems. Moreover, most of the existing systems are typically connected to networks, at the very least, a local area network connecting a local network with a couple of systems and more often, a wide area network eventually connecting to the world wide web. Given this, a protection mechanism is required to be in place to ensure that an unauthorized access to the system is prevented and the templates are properly protected.

There is a wide use of authentication systems in internet services and mobile devices for the protection of user content. Various tools and techniques for the management of information security have been developed. But systems based on biometrics have made significant progress to support some aspects of information security over the period of time. An in-depth and comprehensive study on biometric authentication has been

conducted in recent years by various researchers [8, 9]. With the passage of time, biometric authentication of the users is gaining more and more popularity since the systems based on biometrics are not easily compromised. This is because, the systems can be breached only if the individuals who are trying to access the systems are in possession of those physiological parameters, which are possessed by the actual users. This has led to the addition of security for the protection of the systems, and reduced their vulnerability.

2.2 Overview of a biometric system

In a biometric system, an identifier is linked to its intrinsic human characteristics. These characteristics are physiological and behavioral in nature that can be used to identify a person digitally [10, 11]. Biometric security helps in authentication which takes place by identifying human characteristics. The specific human characteristics mentioned above are defined as follows:

- Physiological: Physiological biometrics are based physical characteristics of an individual. They vary from individual to individual and are assumed to be relatively unchanging such as fingerprints, palm prints, face, iris/retina etc.
- Behavioural: Behavioral biometrics are based on a behavioral characteristics of an individual. The examples include voice, gait, signature etc.

There are four important modules in a traditional biometric system (Figure 2.1). The sensor module is responsible to acquire data from the users, the feature extraction module processes the sensor data to find a description that is feasible for matching of templates that are residing in the database. The features extraction is followed by the a matching module that generates the matching scores which are finally used to perform the decision making regarding the grant of permission to a specific user.

The several factors which are considered significant while performing the selection of a specific biometric identifier include permanence, universality, measurability, circumvention, performance etc [12]. Another important factors is the suitability of the application. Nevertheless, the choice of a single biometric identifier which meets all the requirements for every possible application is not possible since there are tradeoffs between different

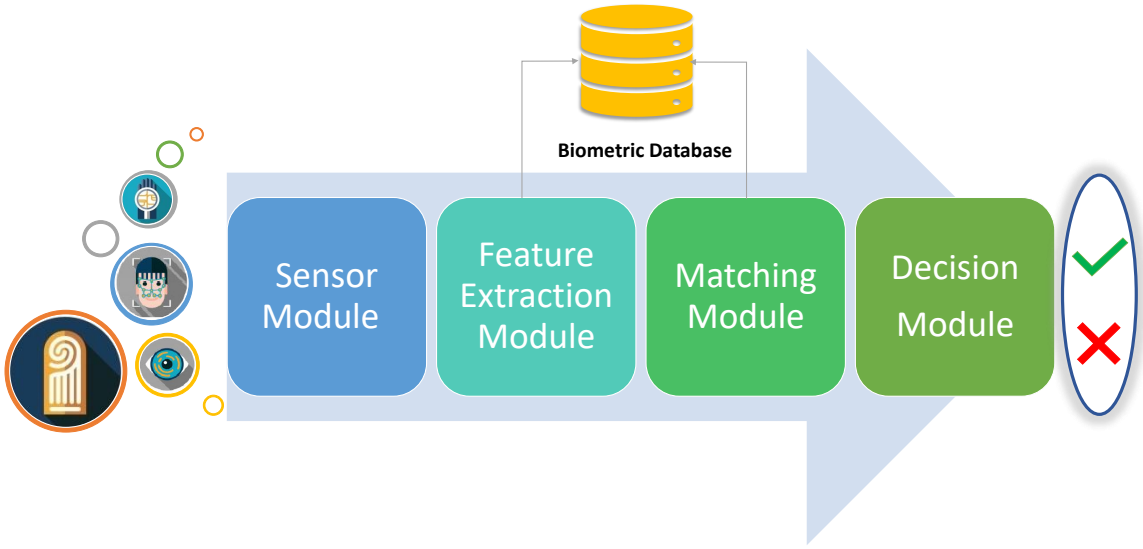

Figure 2.1: Logical blocks of a generic biometric authentication system.

performance metrics. Keeping this in view, there is a possibility to optimize a number of measures by using a combination of various biometric identifiers. Therefore, we can logically characterize a biometric system into two distinct categories: 1). Unibiometric systems, and 2). Multibiometric systems.

2.2.1 Unibiometric systems

Traditionally, biometric recognition systems are unibiometric, which employ a single biometric trait for authentication purpose. It may use one of the physical or behavioral biometric traits of the user, such as fingerprint recognition [13–15], face recognition [16–18], iris recognition [19], signature etc. In the literature, the use of unibiometric systems is widely employed with very good recognition results. However, such systems are typically constrained due to several factors including lack of accuracy due to noisy data, non-universality of biometric traits for registration, physiological limitations of biometrics and vulnerabilities in the biometric systems (Table 2.1) [20, 21].

Some biometric modalities are more vulnerable to some specific problems, e.g., spoofing a fingerprint is relatively easier as compared to a vein/palm pattern. However, the recognition accuracy of fingerprints is far more superior. These are complementary properties of two different biometric modalities which can be exploited together in a multibiometric system, hence making the system more tolerant to spoofing while maintaining a higher accuracy.

Table 2.1: Issues associated with unibiometric systems

Name	**Description**
Noise in data	The acquisition environment corrupts the data due to which the features are altered. This can result in a false registration of the user.
Lack of universality	A certain biometric trait cannot be used due to some clinical condition such as a cut in the finger, long eyelashes resulting in an iris failure etc.
Identification accuracy	For large databases, a certain biometric trait will be able to handle a maximum number of distinguishable patterns after which it will not be able to discriminate between the users.
Spoofing	Some behavioural and physical biometric traits are vulnerable to attacks e.g., signatures and even fingerprints. Successful presentation of a spoofed biometric will result in an authentication compromise.

There are several physiological modalities which can be utilized to acquire the biometric traits of the users. Appropriately, making the correct choice for making systems is a factor which requires considerations into various dimensions. The budget, ease of data acquisition, overall authentication results in terms of recognition and biometric traits which promote anti-spoofing are significant factors which determine the optimal biometric trait for biometric security research. The choice of biometric trait is done keeping a trade-off into account among several factors, that require a careful consideration based upon the applications. Retina and iris present the technologies that yield very good authentication results. Physiologically, these traits are highly discriminative for various individuals with patterns that exhibit almost no chance of repetition.

However, they are not user friendly, expensive with respect to technology and highly sensitive to the protocols used for acquisition of the data. These specific limitations have resulted in a highly restrictive use of these two modalities, specially from the perspective of the convenience of the end user. Ear is one of the most stable biometric however it is not distinctive and is also sensitive to some external factors such as wearing of cap,

jewelry etc. Face is a physiologically motivated biometric and is very useful, however, the most fundamental flaw with the face biometric is that it is a source of infringement of user's privacy. Therefore, the users are typically not comfortable with hosting of their facial data specially by the third parties.

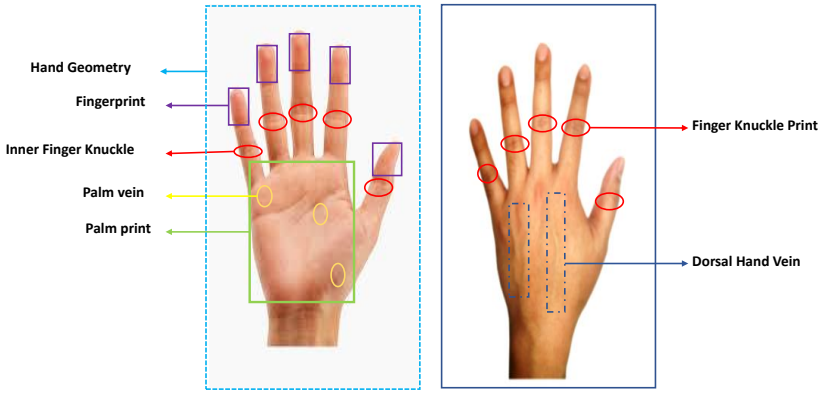

Figure 2.2: Front and back view of hands along with various biometric traits

In contrast to the above mentioned modalities, the remaining four i.e., fingerprint, palm print, hand vein and hand geometry are the modalities which are based on hands. It should be noted that all these modalities (except hand geometry) are highly accurate for recognition, make use of inexpensive technology generally, are fast for matching as they require templates of very small size and are less sensitive to acquisition conditions as compared to the other modalities that are used for biometrics (Figure 2.2).

Table 2.2: A review of pros and cons of different physiological biometric modalities

Modality	**Advantages**	**Disadvantages**
		Continued on next page

Table 2.2 – continued from previous page

Modality	Advantages	Disadvantages
Retina	• Retinal pattern cannot be forged • Highly distinctive • Provides a high security in authentication	• Not user friendly • Sensitive to medical conditions • Expensive technology • Requires controlled environment
Iris	• Highly accurate • Highly scalable • Iris pattern remains stable over a long time • Small template size, so promising speed	• Not user friendly • Expensive technology • Requires controlled environment • Occlusion due to eyelashes, lenses • Illumination should be controlled • Sensitive to medical conditions

Continued on next page

Table 2.2 – continued from previous page

Modality	Advantages	Disadvantages
Ear	• Fixed shape and appearance • Most stable	• Sensitive to earrings, hats etc. • Comparatively less distinctive
Face	• Physiologically motivated: humans identify each other based on faces • Requires a standard camera • Fast matching based on facial features	• Facial traits change over time • Dependent on lightning conditions • Causes infringement of privacy
Fingerprint	• Inexpensive technology • Secure and highly reliable • Fast matching as template size is small	• Cuts, scars etc can alter fingerprints • Easily deceived through wax finger • Some people have damaged fingerprints • Unhygienic: physical contact with the sensor

Continued on next page

Table 2.2 – continued from previous page

Modality	Advantages	Disadvantages
Palm print	• Highly distinctive • More reliable, permanent • Good results with low resolution cameras	• Sensitive to illumination variations • Large recognition area • Scanners are bulkier and expensive
Hand vein	• Contactless and hygienic • Very accurate • Difficult to forge	• Age related deformations • Relatively expensive technology • Sensitive to environment
Hand Geometry	• User friendly, contactless and hygienic • Results not effected by external factors	• Not very distinctive • Large recognition area • Large storage requirement • Can be used only for adults

Continued on next page

Table 2.2 – continued from previous page

Modality	Advantages	Disadvantages
Finger Knuckle	• Contactless and user friendly • Works with low resolution • Low cost	• Non-uniform reflections • Sensitive to environment conditions • Shortage of public databases

Fingerprint

Fingerprint is one of the most established biometric modality due to its high recognition rates and consistency, and has been existing for over a century. The ease to acquire fingerprints and their wide usage has led to many commercial applications relying on them as far as biometrics are concerned. A fingerprint is formed by coexistence of a collection of ridges and valleys, thus yielding a pattern which is distinct for different human beings. These patterns are also referred to as "minutiae" and are mainly composed of bifurcations, enclosures, ridge endings and ridge dots. Further, the minutiae are subdivided into sub minutiae such as pores, crossovers and deltas (Figure 2.3). A fingerprint biometric system has four main stages: acquisition of data, feature extraction, template creation and matching. The ease of use and a small space required for the storage of template has made it one of the best biometric technologies to employ commercially.

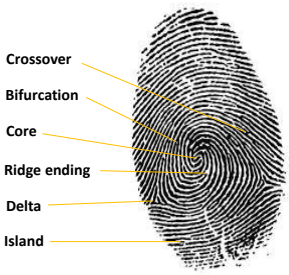

Figure 2.3: Example of a human fingerprint.

On fingerprint biometric, both quantitative and qualitative works exist. A survey of

around 160 users was done in [22, 23] in which the users gave a positive response to using this technology for smart phones. Furthermore, various technological contributions presenting quantitative results show that a fingerprints take less than 1 second for matching, achieve 0.07% equality on a database of 100 subjects, false rejection rates of upto 0.04% and false acceptance rates of upto 0%, 4.18% and 8.91% using three confidence coefficients i.e., 99.0%, 99.5% and 99.9%. These results indicate at a very high recognition performance in a very small amount of time, promoting the use of fingerprint technology for real time implementation of systems requiring biometric validation.

Palm print

Palm print as a biometric is a popular biometric modality which has attracted many researchers attention. However, it is relatively a new biometric as compared to its counterparts such as face, fingerprints etc. A palm print image consists of some rich intrinsic features such as ridges and palm lines, delta lines, principle lines, minutiae features, wrinkles etc [24, 25] that are deemed to be permanent and unique for every individual (Figure 2.4). Owing to these inherent features, palm print generates a unique biometric characteristics for every individual that are reliable for identification purposes [26, 27]. The main issue that is responsible for reducing the performance of palm print systems is the deformation of images during the image acquisition process. Attempts are being made to solve this issue by using contact devices but researchers have faced several challenges in the design of such devices including its size and limited usability, along with several challenges including position, stretch and rotation of the palm print. Lately, researchers are resorting to contactless devices again with low resolution imagery used for commercial application and high resolution imagery for applications such as criminal investigation.

Some of the most recent contributions on palm print biometric [28, 29] shows that the recognition rates of upto 98.78% and 97.2% respectively have been achieved within processing times in the order of milliseconds on databases of fairly large size (about 12000 instances). The most relevant contribution in this regard with the best accuracies are presented by Luo et al . [30] in which the authors have reported accuracy of 100% on a dataset having 4600 instances of palm prints. This is in contrast to a general perception that palm prints are not as accurate as fingerprints. However, it should be

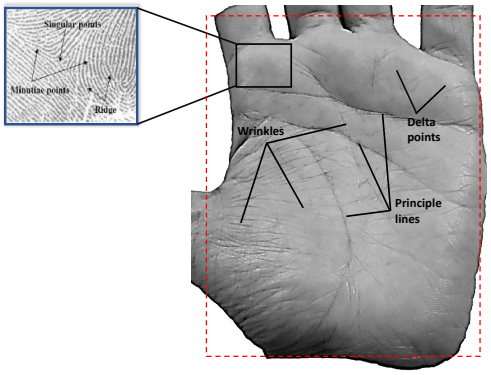

Figure 2.4: Example of human palm print

noted that the possibility to obtain a relatively large dataset to validate the findings on fingerprints having a statistically higher significance is much more likely in contrast to palm prints for which the availability of dataset is relatively limited.

Veins

Vein biometrics, also known as vascular biometrics, refers to a biometric systems that measures parts of an individual's circulatory system for identification. Vein pattern recognition technology has gained a significant attention due its unique attributes along with liveness property yielding very high recognition rates. Vein patterns are segmented into different sub-modalities amongst them most commonly used come from the palm [31], palm dorsal [32], wrist [33], or finger [34]. The sub-dermal nature of veins makes these types of biometrics a highly secure modality [35]. In a vein biometric system image acquisition is carried out by using near-infrared (NIR) imaging device. The near NIR light maps the vein locations, because the hemoglobin in veins absorbs NIR light generating a high contrast image by creating the visualization of vein pattern as shadows appearing over a white background. This generates high contrast images with vein patterns which are used for recognition using various texture feature extraction techniques.

A quick review of the literature elucidates on the facts that very high recognition rates are obtained on this biometric trait. Researchers have reported an accuracy of upto 99.4% reinforcing the theoretical claims of high uniqueness of vein patters [36]. However, the requirement of using sophisticated acquisition devices for obtaining the biometric data makes this modality relatively less popular [37]. Moreover using vein patterns can

be a challenge in some cases due to the physiological changes taking place due to ageing and various medical conditions [21].

Hand Geometry

Hand geometry/shape is a very simple biometric technology that uses the measurements of human hand to verify the identity of the individuals. The measurements include the length, shape and width of fingers and size of palm (Figure 2.5). The biometric systems employing hand geometry are widely used as they have a high public acceptance [38–40]. However, it should be noted that the systems based on this technology are not scalable as the hand geometry is not highly unique [21]. Nevertheless, it is widely used at places providing access control, where the main objective is to find out if someone is illegally trying to gain access to someone's personal identification. A hand reader guarantees that a worker is actually available at a place where he is meant to be. It is also used for implementing time attendance of the employees and helps in stopping the employees from buddy punching (which takes place commonly with fingerprint technology). Hence, the payroll accuracy of a company is guaranteed with a higher probability when hand geometry is used [38].

Due to the lack of the ability to differentiate between the people effectively, the usage of hand geometry is somewhat limited and typically it is used in conjunction with other biometric modalities for improved recognition rates. Some recent contributions on hand geometry show that an EER of upto 0.31% has been achieved by Sharma et al. [40] with upto 50 distinct users. A novel contactless sensing systems [41] based on multi sampling has been proposed which has been used to authenticate a database of 100 people representing upto 200 hands with about 50% improvement in the recognition rates [21]. Nevertheless, the technology is not as accurate as its counterparts and thus is not very useful in a standalone setting for large scale deployment for commercial purposes.

Finger knuckle print / Inner Knuckle print

Finger knuckle print is one of the emerging hand based modality used for biometric verification of the individuals [42]. The finger knuckle patterns can be easily acquired using contactless devices. In contrast to the more established modalities such as fin-

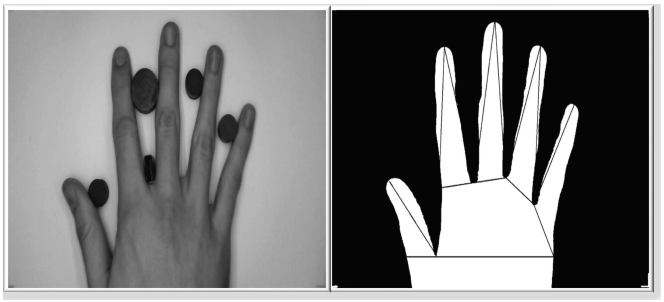

Figure 2.5: A human hand used for the extraction of hand geometry features.

gerprints requiring high resolution imagery, the knuckle patterns can be easily captured using low-resolution samples [43]. Additionally, the patterns on the outer surface of the knuckle appear at an early stage and survive for a longer periods of time and are specifically useful for the workers, labourers, cultivators etc, whose fingerprints are more susceptible to damage due to the nature of work [44]. In a biometric system based on finger knuckle, the physiology which differentiates two different people is due to the lines, creases and texture of the knuckle print which lie at the three knuckle joints of the fingers [45] (Figure 2.6). These lines appear before birth and rarely change over an individual's lifetime.

The knuckle print of a user can be obtained without any physical contact with the biometric sensor. Therefore, the chances of spoofing gets notably minimized. Since knuckle prints rarely change over time so they are considered to be highly stable for individuals from various age groups however, there usage of 8this modality is somewhat limited. Study of the literature depicts that researchers knuckle prints is a very promising modality giving very high accuracy on the identification of persons of upto 98% in real time on a dataset of size 7900, FRR of 0% and FAR of 0.062%. Since the data for finger knuckle print can be obtained contactlessly, invariance to the behavioural patterns, ease in collection process and a wide acceptability socially, the potential in using this technology on a large scale undoubtedly very huge. However, before a widespread deployment thorough research is needed on improving the identification results.

Figure 2.6: Finger dorsal knuckle print around the joints

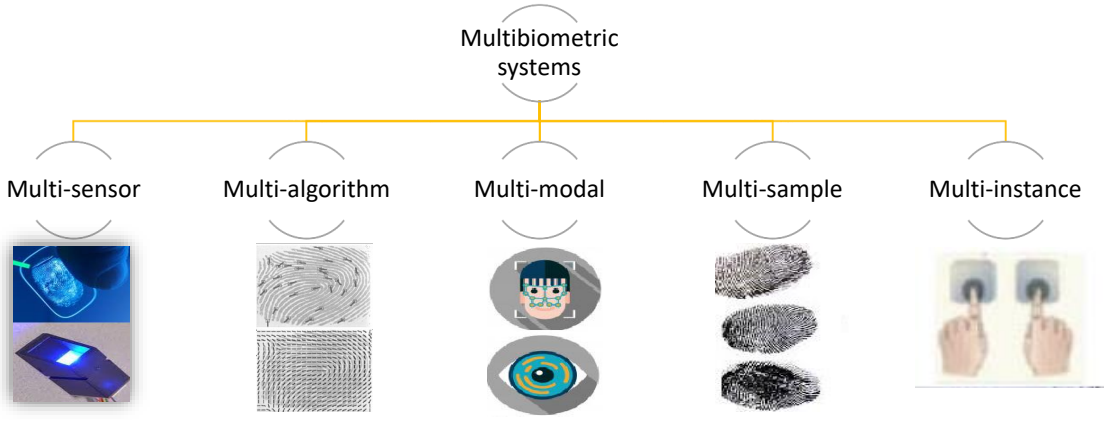

Figure 2.7: Types of multibiometric system.

2.3 Multibiometric systems

When using the unibiometric systems, we may may encounter problems due to several issues including but not limited to missing data [46] (e.g., occlusion in face image), poor sampling [47], biometric duplication [48], low discrimination among samples (e.g., hand shape/ geometry) between distinct users, vulnerability to attacks and spoofing etc [49]. In situations like these it may be necessary to make use of multiple biometric cues to boost the accuracy of a recognition system. Multibiometric systems offer so many features, making them more convenient and feasible as compared to the unibiometrc systems. There can be different sources of biometric information in a multibiometric system due to which such systems can be classified into five major categories (Figure 2.7):

2.3.1 Multi-sensor systems

The multi-sensor systems use multiple sensors in order to capture the same biometric trait of an individual [50, 51]. Such systems are desirable due to the fact that they can enhance the recognition capabilities of the systems [52]. This happens because the data acquired from various sensors may be of different quality and multi-sensor system can partially solve the problems related to poor data quality [53]. The different biometric traits, when used for recognition have the ability to complement one another, creating the possibility for a better recognition of the individuals.

2.3.2 Multi-algorithm systems

In the multi-algorithm systems, more than one algorithm is utilized to improve the recognition rates of a biometric system [54, 55]. It is cost effective to work on such systems as they do not make use of multiple biometric traits and thus do not require multiple sensors [56]. However, such systems require a lot of computational resources as multiple algorithms have to be run in order to calculate the relevant features for a single instance [57, 58]. Keeping this in view, special consideration should be given to the fact that real time performance is a requisite requirement of biometric systems and thus the feasibility of such systems might be compromised even when they have the ability to achieve very high recognition rates.

2.3.3 Multi-sample systems

In multi-sample systems, multiple samples from the same sensor are acquired from the biometric devices [20, 59]. The rudimentary concern with a single sample biometric system is in the fact that a bometric samples does undergo missing data problems due to which, effective recognition cannot be achieved [60]. The problem is mitigated in multi-sample systems by acquiring multiple samples from the devices and using multiple or the most relevant ones for recognition. The same algorithm is used to process all samples and recognition results from each sample are calculated and eventually fused to yield a final result of recognition [61]. This recognition may be based on some technical considerations e.g., a confidence score with which a specific recognition result is obtained.

2.3.4 Multi-instance systems

In multi-instance systems, the biometric data is typically extracted from multiple instances of the same body traits [62]. For example, finger biometric properties can be extracted from two fingers [63], the palm prints can be acquired from two palms [64], the iris of the individuals [65] can be used for measuring different biometric traits of the systems. The addition of multiple instances for performing recognition in a biometric system increases the discrimination capability of the system because the distinctive capability for a single individual is extended by adding more features to the pool, potentially leading to an improvement in the recognition rates for a particular system [64].

2.3.5 Multi-modal systems

In the multi-modal systems, the biometric traits from different modalities can be combined together for the purpose of identification of an individual [61]. Such systems are used to complement the weaknesses of a single biometric and usually try to make the best of different biometric traits in order to perform recognition of an individual [66]. An additional advantage of using multi-modal biometric systems is that they are more secure as compared to the uni-modal systems as more than one biometric traits are used at the time of registration of a user in a system [66–68]. Appropriately, stealing or forging one biometric trait does not guarantee an access to the system thus leading to an improved security feature for authentication in biometric systems.

Designing a multibiometric system has a very high significance, a valid design will be able to ensure that the pieces of evidence collected from various sources, when fused together using different fusion strategies can improve the recognition rates while ensuring some value added services provided to the users. However, when different modalities have to be combined to implement a multibiometric system, special consideration has to be given to several dimensions e.g., what kind of additional sensors will be required, what are the costs, is there a possibility to embed different sensors in the device and, what is the overhead of such a systems in terms of computational complexity.

2.4 Performance metrics for evaluation

Multiple metrics can be employed to assess the performance of a biometric authentication system. Choosing a particular metric/metric(s) depends upon the nature of evaluation. Following are the basic raw metrics and their descriptions:

- **True Accept (TA)** : A genuine user is correctly verified to its corresponding template stored within the biometric system.
- **True Reject (TR**) : An imposter is correctly rejected as its data does not match to any template stored within the biometric system.
- **False Accept (FA)** : An imposter is incorrectly verified as a genuine user as his data matched to the template stored with in the biometric system.

- **False Reject (FR) :** A genuine user is incorrectly rejected as his data does match to any template stored with in the biometric system.

The standard metrics that have been used to evaluate the performance of the authentication system in the literature are as follows:

- **False Accept Rate (FAR)** : Describes the percentage of an impostors that were incorrectly verified as a genuine users. It is calculated on the basis of following formula:

$$FAR = \frac{FA}{FA + TR} \tag{2.4.1}$$

- **False Reject Rate (FRR)** : Describes the percentage of genuine users that were mistakenly rejected from a biometric system. It is calculated on the basis of following formula:

$$FRR = \frac{FR}{TA + FR} \tag{2.4.2}$$

- **Correct recognition rate (CRR)** : It gives the probability that the system will correctly identify the input template from the templates in the database. It is given by the formula:

$$CRR = \frac{TA}{TA + TR} \tag{2.4.3}$$

- **Genuine Acceptance Rate (GAR)** : Describes the percentage of genuine users accepted by the biometric system. It is given by the formula:

$$GAR = 100 - FRR \tag{2.4.4}$$

- **Accuracy:** It is ratio between verified cases (both True Accept and False Accept) to all possible cases. It is given by formula:

$$Accuracy = \frac{TA + FA}{TA + FA + TR + FR} \tag{2.4.5}$$

- **Equal Error Rate (EER)** : Describes the point at which FAR and FRR are equal. Smaller values of EER refers to improved performance of a biometric system.

2.5 Fusion Methods

Fusion plays a very considerable role in the implementation of multibiometric systems. There is an inherent requirement to fuse the information collected from different modalities before using it for the purpose of recognition. Fusion can be applied in multibiometric systems in two major settings: before matching and after matching. Consequently, there are four distinct levels at which fusion can be applied i.e., sensor level, score level, feature level and decision level (Figure 2.8). The fusion applied at the first two levels is referred to as pre-matching fusion whereas the rest are categorised as post-matching fusion.

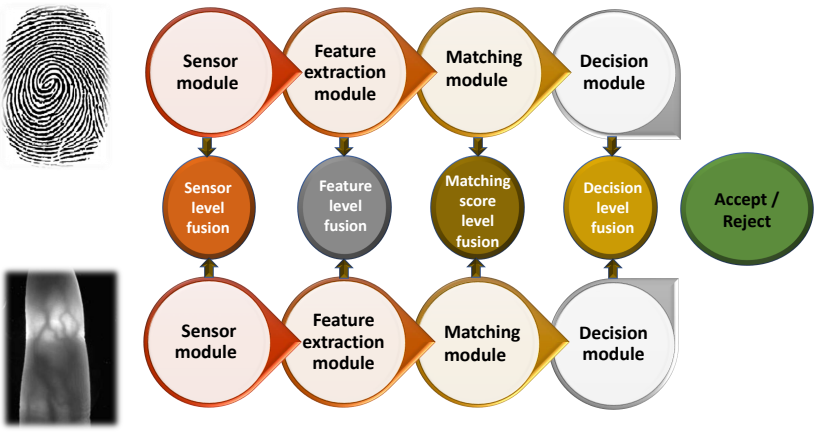

Figure 2.8: Fusion levels in a multibiometric system.

2.5.1 Sensor level fusion

In sensor level fusion the raw information is gathered from various sensors and is fused at the initial level prior to feature extraction to produce a raw fused information. Fusion of two images can take place at pixel, feature or at signal level. Fusion at sensor level can be between the multiple samples of same biometrics gathered from multiple sensors [69] or multiple instances of same biometric taken from a single sensor [70], multiple sensors etc. Relatively less research has been done on this type of fusion in biometrics.

2.5.2 Feature level fusion

In feature level fusion, the features extracted from multiple biometric sources are combined together in the form of a single feature vector. In this fusion technique, features from different sensors, samples, traits can be combined together. At this level of fusion, signals from various biometric channels are firstly pre-processed and their feature vectors are calculated independently; by using fusion algorithms, the feature vectors are fused to form a combined feature vector, which is used for recognition [71]. The incorporation of multimodal biometric traits in this type of fusion can be employed to exploit specific strengths of different biometric modalities [6, 72, 73]. Although better recognition results can be expected using this type of fusion technique, it has certain limitations including the lack of compatibility of different biometric features, curse of dimensionality, just to name a few.

2.5.3 Matching score level fusion

This type of fusion is done by joining the scores yielded by the matching module of each feature vector with the template. The features are processed independently along with the calculation of scores, followed by the calculation of composite matching scores [74–76]. This is done by the checking the confidence scores which are obtained using each feature vector. This type of fusion technique is typically easy and thus is being used by different multibiometric systems for effective execution.

2.5.4 Rank level fusion

In this type of fusion, sensor data acquired is followed by the feature extraction. The matching of this feature vector is performed against all the available templates in the database and similarity scores are obtained [77, 78]. The scores are arranged in the descending order and the entry corresponding to the lowest rank (indicating similarity of feature vector with the respective template) is taken as the most relevant to the data that is acquired from the sensor. The rank level fusion can also be employed for multibiometric traits and thus can yield a recognition score with a higher confidence. However, it should be noted that in addition to the pre-processing of sensor data, additional computational load is transferred on the matching module. Therefore, the rank level fusion

can be computationally very complex especially when more than one biometric traits are employed.

2.5.5 Decision level fusion

In this type of fusion, the information obtained from different decision modules is combined together to decide about the identity of a user [79, 80]. The recognition results of each biometric trait are individually obtained followed by a fusion of these decisions to obtain a final decision regarding recognition [81, 82]. Various methods to perform this types of fusion can be used e.g., majority voting can be employed [83]. In systems which require enhanced security and fail safe functioning, rule based decision can also be made such as the use of a logical 'AND' operation, indicating that it is necessary for all biometric traits to be yielding the same output.

2.6 Biometric system attack points and vulnerabilities

A typical biometric system can be subjected to attack at various points. Figure Figure 2.9 illustrates the various attack points in typical biometric system. As stated by Ratha et al. [4]: "There are eight possible attack points a) Biometric forgery, b) Replay attacks, c) Override feature extractor, d) Transmissions attacks, e) Database attacks, f) Override template to matcher, g) Replace matcher attacks, and h) Override decision attacks". These attack scenarios can be broadly classified for simplicity into three groups

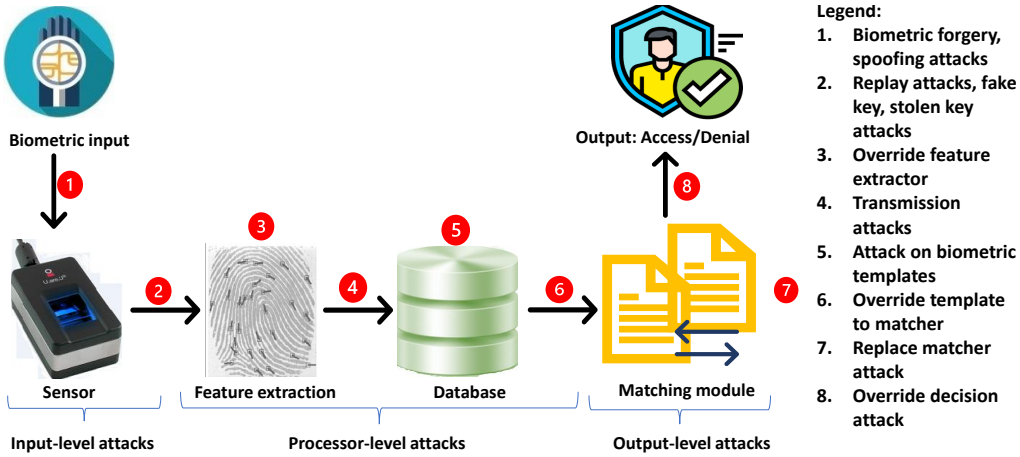

Figure 2.9: Attack points in a generic biometric system

namely: input-level, processor-level and output-level attacks [84].

2.6.1 Input-level Attacks:

Attacks like biometric presentation which include biometric forgery/fake biometric, biometric morphing attacks, and replay attacks fall into this category. In fake biometric attack, the adversary tries reconstruct a legitimate user's biometric features in order to gain access. In a recent research it was shown how simple it was to attack a smartphone using a fake fingerprint synthesized by using a silicon gum or a modelling clay [85]. In a biometric morphing attack, "biometric samples of multiple subjects are merged in the signal domain, in order to allow a successful verification of all contributing subjects against the morphed identity " [86]. Using multiple biometrics for authentication can aid in reducing forgery/spoofing attacks. A biometric system with a standalone architecture is considered more secure since the transmission of data over a communication is not present. Replay attacks occur when data is transmitted over a transmission medium. In these type of attacks, the biometric data gets intercepted and is re-transmitted by the adversary. Whenever in a system a communication channel is involved, security to the data needs to be incorporated by using techniques like cryptography, steganography, or using secure protocols like Secure Shell Protocol (SSH). However the use of multi-modal biometrics in this theses reduces the chances of spoofing.

2.6.2 Processor-level Attacks:

Attack points 3,4,5,6 of a biometric system contribute to processor-level attack. Attack by overriding the feature extractor, attacks during transmission of features to the database, database attacks, and attack by overriding the biometric template matcher are few of the processor level attacks [84]. In all of these attacks, biometric database is the most targeted area in the biometric system. Since a biometric database is a repository of biometric templates and, if somehow a template's confidentiality or integrity is jeopardized, a user may not be able to use it again since biometrics are permanent and cannot be replaced. So in order to hinder the misuse of stored biometric information i.e biometric templates, privacy protection techniques which are also known as template protection techniques have been developed. Section 2.7 discusses in detail various multibiometric template schemes. A biometric template suffers issues such as, Feature

correlation attacks, template inversion attacks, stolen-key, and fake-key attacks [87]. In Feature correlation attacks an attacker is able to extract the original biometric template from various cancelable templates of the same user acquired from independent applications [88]. Attacks via Record Multiplicity (ARM) are a type of feature correlation attacks. In this thesis, cancelable thesis has been employed for the protection against database attacks. The approach of using random projection as a cancelable technique has been found to be very effective in protecting the templates stored in the biometric database. Random projections also integrates template irreversibility, making the template resistant against inversion attacks. This techniques also makes the cancelable template unlinkable among various applications, meaning thereby they are resistant against feature correlation attacks. This technique has also shown to be resistant against stolen key and fake key attack. A detailed security analysis of the proposed cancelable biometric system is explained in Chapter 4.

2.6.3 Output-level Attacks:

Attack points 7 and 8 of FigFigure 2.9 contribute to the main types of output attacks which include replacing matcher and overriding decision module. In replacing matcher attacks, the matcher is manipulated and forced to output match scores preselected by the attacker. In overriding decision attacks, the final match decision is overridden by an attacker by corruption of comparator output. Recently in [89] Liu et al proposed qFool, a novel decision-based attack algorithm that computes adversarial examples with only a few queries hence affecting the system's decision making capacity. Output level attacks are beyond the the scope of this thesis.

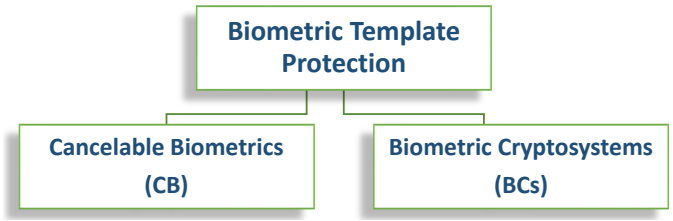

Figure 2.10: General categorization of template protections schemes

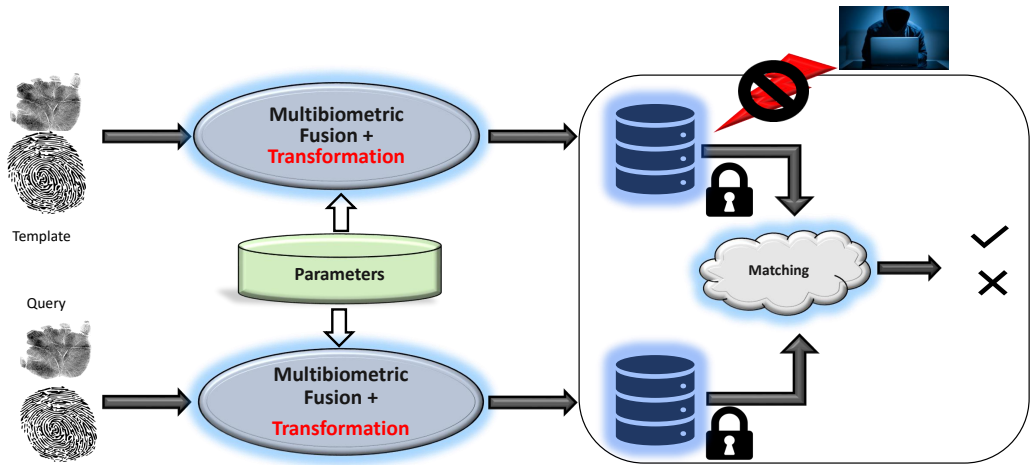

Figure 2.11: Biometric authentication system incorporating template security.

2.7 Multibiometric Template Security

With regards to the security of the biometric system, being multibiometric in nature adds itself another layer of security even though then there are multiple points of attack on an authentication system as stated in Section section 2.6. A biometric system database is an essentially crucial component that requires the highest degree of security [90]. The rationale for focusing on security of multibiometric template is that they lead to a 3-dimensional vulnerability to a biometric system in contrast to their counterparts [91]: 1. Template can be replaced by an imposter to gain unauthorized access, 2. A spoof can be created from the template to aid in unauthorized access, and 3. The stolen template can be replayed to the matcher to gain access. Therefore, it is vital to protect the templates from an adversary, unlike PINs and passwords, a biometric template if compromised cannot be revoked and reissued so considering the criticality in this context. Therefore there is a need for a secure template that must be irreversible and unlinkable [92–98] (Figure 2.11). Biometric template protection schemes can be categorized into two main classes (Figure 2.10) [99, 100]: 1. Biometric Cryptosystems (BCs), 2. Cancelable Biometrics (CB). These schemes offer various advantages over a generic biometric systems. A few most important advantages are summarized in Table 2.3.

2.7.1 Biometric Cryptosystems

Biometric cryptosystems (BCs) refers to designs that securely generate digital key from a biometric or binds a digital key to a biometric [111]. To over come the short comings

Table 2.3: Advantages of Template Protection

Advantage	**Description**
Secure template/Privacy protection	Reconstruction is hardly feasible in biometric biometric cryptosystems and cancelable biometrics as the original biometric template is concealed.
Secure key release	In biometric cryptosysytems the key release mechanisms depends on the biometrics.
Pseudonymous authentication	The encrypted identifier that is used for authentication is also a pseudonymous identifier.
Revocability of templates	Multiple instances of templates can be generated from the same biometric data.
Enhanced security	The use of cancelable biometrics and biometric cryptosystems mitigates various attacks on the biometric sysytem.
Social acceptance	The social acceptance of biometric applications is expected to increase with the use of cancelable biometrics and biometric cryptosystems.

of traditional verification methods which were based on password-based key-release, BCs brings about a considerable security benefit by offering biometric-dependant key-release since the biometrics has a strong link with the user's identity [87, 99, 112]. At the same time combining biometrics with cryptography and extracting the keys is not that straight forward due to variations present in a biometric data. Most of the BCs require helper data that contains additional information about the biometric and is used to generate or retrieve a key [91, 113]. A helper data, must not reveal significant information about original biometric templates. Table 2.4 presents a brief summary of the biometric cryptosystems.

Sutcu et al. [101] proposed the use of multibiometric features, followed by a *secure sketch* block, making it hard to extricate the original samples from the encrypted features. Karthik et al. [102] proposed a method to enable template protection using fuzzy vault framework. The authors claim to improve the recognition performance of the system along with enhanced security. Camlikaya et al. [103] proposed a technique for the fusion of fingerprint template along with behavioral biometrics (voice samples). The

algorithm enhanced the security of the biometric system by encoding the fingerprint features within the voice feature vector. The use of voice was motivated by using the property of spoken words used as password to achieve the desirable cancelable property. Multiple biometric cryptosystems were proposed by Fu et al. [104] out of which, three were used for performing biometric fusion at the cryptographic level. The authors presented no experimental results, however, a detailed theoretical analysis of algorithms, comparison and discussions were carried out. Nagar et al. [6] provided a feature-level fusion method for both fuzzy vault and fuzzy commitment schemes that simultaneously secures the multiple templates of a user using a single secure sketch. Feature level fusion using multiple characteristics of a user proves to be significant in providing high privacy as compared to the single characteristics biometric systems since only the fused feature vector is stored on the server database. Further, it requires less storage since only the combined feature vector is stored in the database server. However, it requires additional feature extraction and transformation tools for the heterogeneous features (variable formats based on distance, similarity, etc.). Another hybrid methodology to secure the biometric systems was proposed by Li et al. [105] in which a combination of computational security and information security principles was done. Decision level fusion was done in the proposed cryptosystem for performing recognition. Kumar et al. [106] proposed a multibiometric system based on cell array. Encoding and hash code computation was done using Bose Chaudhuri Hocquenghem (BCH) on the biometric modalities. The data is scattered across the two cells such that the first cell stores the hash code and the second cell stores the key. Moreover, fusion was performed at both decision and feature levels out of which the former shows better results in a multibiometric cryptosystem setting. You et al. [107] proposed a novel fuzzy vault scheme which effectively protects the multibiometric template against location attack, brute force attack and correlation attack. They have performed fusion of fingerprint and fingervein templates. Feature point fusion encoding is done through Grid projection, and fusion encodings are applied to construct the fuzzy vault. Chang et al. [108] proposed BIOFUSE in which fuzzy commitment and fuzzy vault are combined using an encryption scheme. The systems makes it difficult for an attacker to gain unauthorized access to the system without doing an impersonation of all the biometric traits at the same instant. The experiments have shown very good recognition rates with a high security. Evangelin et al. [109] used a visual shadow creation process to create multiple shadows of one image

followed by encoding and decoding using elliptic curve cryptography (ECC). Although a very secure model is obtained, the implementation time of the model was significantly expanded. Asthana et al. [110] made use of a key binding mechanism to generate a secret key using the biometric data of the user, leading to the proposition of a biocrypto system. Novel objective functions are proposed to create helper data. The local minima of objective function are taken as anchor points to retrieve the secret key and perform recognition leading to about 98% success rate in recognition even in the presence of limited noise in biometric data.

2.7.2 Cancelable Biometrics

Cancelable biometrics (CB) refers to distortion of biometric features that are intentional and systematically repeatable in nature to protect sensitive user-specific data [4]. Cancelable biometric transforms are those that are used to transform the original biometric samples such that the resulting data is computationally hard to recover. When the user registers itself in the system, his biometric sample is transformed using a one-way transformation and saved in the database. This transformation is chosen from an identification word that is specific to the user. In the verification step, the query template is used to generate a transformed template that is compared with the saved template in the database followed by the verification process. The literature on unimodal cancelable biometric systems is very rich but there are inherent problems with such systems including intraclass variability, variation in data quality and a significant similarity in interclass samples. In contrast to such systems, the multimodal biometric systems combine the feature of various biometric traits to generate the templates which are more secure and thus, resistant to various threats and attacks. The main advantage that is offered by the multibiometric systems is greater security, accuracy, noise sensitivity and resistant to spoof attacks. Table 2.5 presents a brief summary of the work done in the domain of cancelable multibiometrics.

Researchers have made several contributions on multibiometric template protection employing cancelable biometrics. Paul et al. [114] proposed a method in which two-fold random selections are made from each biometric trait, followed by a feature level fusion. Random projection of each fold is obtained followed by PCA (principal component analysis) and later K-means clustering to generate the single templates for individual

biometrics. Later, LDA (linear discriminant analysis) is applied to further improve discriminability of the features. Final authentication is carried out using a classifier. Another variant of the technique proposed in [115] makes use of Gram-Schmidt transformation instead of PCA, along with some other minor modifications in the pipeline. The authors have validated the cancelable property of the proposed method, while giving good authentication results in a multibiometric setting. Furthermore, the authors improved the results by proposing a methodology in which both Gram-Schmidt transformation and PCA were used followed by a rank level fusion for performing final authentication of the users [117]. Chin et al. [116] propose a 3-stage hybird template protection scheme. They have performed the fusion of palm print and fingerprint on the feature level, followed by the use of random tiling technique to extract unique features. Finally, the fused random features undergo 2^N discretisation to produce the template bit string. The approach addresses the criterion for template protection with an improved EER as compared to unimodal biometric sytems though it is slightly higher with refrence to multimodal system. Gomez et al. [68] made use of homomorphic probabilistic encryption to generate the biometric templates along with fusion at three different levels. A complexity analysis was also carried out to assess the feasibility of the proposed method for real time implementation. Moreover, feature level fusion is also employed yielding more secure and better cancelable biometric features. Kaur et al. [118] proposed a template transformation method named random distance method that yields privacy preserving, revocable and discriminative pseudo biometric identities, with about 50% reduced memory footprints. Yang et al. [66] proposed a multibiometric system in which the fingerprint based minutiae features and finger vein features are extracted followed by their respective binary features, and than performing feature level fusion in three different ways. The method obtained secure biometric templates with good recognition results. Gomez et al. [119] showed that the use of Bloom filter based protection schemes while elucidating that it is not a straightforward task. A statistical analysis of unprotected templates is carried out to estimate the main parameters of such schemes. Dwivedi et al. [120] proposed a method to obtain cancelable templates by using log-Gabor filters with phase quantization, followed by the generation of biometric codes. Score level fusion from multiple biometric templates are used for authentication yielding better results in comparison to unibiometric systems with better accuracy. Walia et al. [121] proposed a method to obtain cancelable features using deep neural networks

that are fused using adaptive graph based fusion method. The proposed method is used to obtain multi-modal unified templates which are empirically demonstrated to be robust to adversary attacks. Chang et al. [122] proposed an authentication approach in which bit-wise encryption scheme is used to transform a biometric template to a secure template using a secret key, that is generated from another template. The scheme fully preserves the number of bit errors in the protected and original template, ensuring that the recognition performance is the same as that in the case of unprotected templates.

Table 2.4: Related work on biometric cryptosystems

Year	Authors	Description
2007	Sutcu et al. [101]	Protection of face and fingerprint templates
2008	Karthik et al. [102]	Multibiometric template security using fuzzy vault
2008	Camlikaya et al. [103]	Encoding of fingerprint with voice features
2009	Fu et al. [104]	Multibiometric fusion at cryptographic level
2011	Nagar et al. [6]	Feature level fusion for fuzzy vault and fuzzy commitments
2015	Li et al. [105]	Biometric cryptosystem using computational security and information security, with decision level fusion
2016	Kumar et al .[106]	Multibiometric system based on cell array for storing has code and keys separately
2019	You et al. [107]	Novel fuzzy vault scheme based on the feature level fusion of the fingerprint and finger vein.
2020	Chang et al. [108]	Multibiometric cryptosystem based on Fuzzy vault and fuzzy commitment
2021	Evangelin et al. [109]	Cryptographic model based biometric template protection
2021	Asthana et al. [110]	Cryptographic key binding for template protection

Table 2.5: Related work on Cancelable Multibiometric Systems

Year	Authors	Description
2012	Paul et al. [114]	Multibiometric template protection using PCA as a transform based tool
2013	Paul et al. [115]	Multibiometric template protection using Gram-Schmidt transformation
2014	Chin et al. [116]	Hybrid template protection using feature fusion and random tiling transformation
2014	Paul et al. [117]	Multibiometric template protection using Gram-Schmidt transform, PCA and rank level fusion
2017	Gomes et al. [68]	Homomorphic probabilistic encryption for cancelable biometric template generation
2018	Yang et al. [66]	Fusion based cancelable multibiometric system
2018	Kaur et al. [118]	Random distance method for obtaining secure biometric templates
2018	Gomez et al. [119]	Bloom filter based cancelable biometric features
2019	Dwivedi et al. [120]	Cancelable features followed by score level fusion
2020	Walia et al. [121]	Cancelable deep feature, followed by adaptive graph fusion
2020	Chang et al. [122]	Novel bitwise encryption scheme to generate biometric template

Chapter 3

Feature Extraction Methods

In this chapter, we will cover the theoretical background regarding the methods that have been used in the proposed framework. The background covers two important aspects: the techniques used for feature extraction, and ways in which the extracted features are made cancelable.

3.1 Gabor Filters

In an effort to design a mathematical function which could have the ability to achieve an an optimal space-frequency representation of a signal, Gabor filters were introduced in 1946 by Dennis Gabor [123]. Their 2D counterparts were introduced by Granlund [124] after which Gabor filters have been employed for processing of the images. The Gabor filters have been found to be very appropriate for texture representation and discrimination of images and have significant practical applications.

3.1.1 Motivation

The main reasons due to which the Gabor filters are considered superior as compared to standard wavelets are as under:

- **Similarity with visual cortex:** The 2D Gabor filters exhibit a remarkable similarity with the primary visual cortex of the mammals. The relationship between various elements in the images such as receptivity, parallelism etc. are detected by the cortex of the human due to which they have the ability to find and differ-

entiate among various patterns in the images [125]. Significant research has been done on the physiology of vision and one of the most well cited contributions in this context was presented by Daugman [126] in which he presented the simple cells of cat's cortex receptive field profiles and compared them with that of Gabor filters, showing their remarkable similarity. Research suggests that a visual cortex has two main characteristics: the direction selectivity for a set of visible patterns, and ability to focus on different regions in the images based on the richness of information requiring different levels of visual attention.

Interestingly, the cells exist in pairs, a cell with an odd symmetry and another even. Appropriately, the mathematical modeling of these cells indicate their behavior as band pass filter structures which are sensitive to different scales and orientations. Although a Gabor filter might be too simplistic in terms of the richness of information which is yielded by a cell in the visual cortex, their approximate model of is presented by Gabor filters which makes their usage very inherent for the implementation of visual systems. This amazing similarity shared between Gabor filters and visual cortex makes their use fascinating for various applications.

- **Optimal space-frequency localization:** The classical Fourier analysis has a very significant limitation that its looses the notion of time / space, which might be very critical in the description of information available in a signal / image. This relationship can be precisely explained based on the following mathematical relation

$$\triangle t \times \triangle f \geq \frac{1}{2} \tag{3.1.1}$$

Which essentially means that the uncertainty between time and frequency cannot be resolved jointly beyond a certain limit. Gabor in his bid to work on the this uncertainty principle wanted to model a mathematical function which would be having the ability to yield the best possible localization both in time and frequency (not achievable using standard wavelets) i.e., to find the shape of a signal which yields a product of $\triangle t \triangle f$ with the smallest possible value, turning the above inequality into equality. Eventually, he realized that a representation which yields a minimum area of $\triangle t$ and $\triangle f$ could only be constructed by single building block: modulation of a sinusoid with a Gaussian function. This was a remarkable discov-

ery led by Gabor and has since than been used very actively in the area of signal processing. A subsequent introduction of 2D counterparts was used to effectively utilize these basis functions in the area of image processing. It should be noted that although the purpose is served by wavelets, they do not jointly resolve the space and frequency in an optimal way.

- **Multiresolution nature:** It is possible to perform multiresolution analysis of the images using Gabor filters. Specifically in applications requiring texture analysis of the images, Gabor filters are quite well suited decomposing an images into various frequencies and orientations. This decomposition is very useful in order to extract coarse and fine features from the images.

3.1.2 Gabor filter design

According to the definition, the Gabor filters are designed by modulating a sinusoidal wave with a Gaussian kernal function. Mathematical representation is as follows [127]:

$$g(x,y) = \left(\frac{1}{2\pi\sigma_x\sigma_y}\right)\exp\left(-\frac{1}{2}\left(\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\right)+2\pi jWx\right) \tag{3.1.2}$$

$$G(u,v) = \exp\left\{-\frac{1}{2}\left(\frac{(u-W)^2}{\sigma_u^2}+\frac{v^2}{\sigma_v^2}\right)\right\} \tag{3.1.3}$$

Where $\sigma_u = \frac{1}{2\pi}\sigma_x$, $\sigma_v = \frac{1}{2\pi}\sigma_y$, σ_x and σ_y are the standard deviations of the Gaussian along the x and y dimensions respectively and W is a constant that denotes the center frequency of the high frequency filter. Equation 3.1.2 is representing the multiplication of a Gaussian envelope with a complex sinusoid, forming a band-pass filter in Fourier domain, where the bandwidth of the filter is managed by the standard deviation of the Gaussian functions and center frequency is controlled by the frequency of the complex sinusoid. A bank of Gabor filters is obtained by designing a number of self similar filters by changing their parameters. If $g(x,y)$ is a mother Gabor wavelet, a set of wavelet dictionary is acquired after performing respective translations and dilations of $g(x,y)$ as follows:

$$g_{mn}(x,y) = a^{-m}g(x',y') \tag{3.1.4}$$

where

$$x' = a^{-m}(x\cos\theta + y\sin\theta) \tag{3.1.5}$$

and

$$y' = a^{-m}(-x\sin\theta + y\cos\theta) \tag{3.1.6}$$

$m = 1, 2, ..., S$ and $n = 1, 2, ..., K$. S and K are number of scales and number of orientations respectively, and $\theta = n\pi/K$. This set of Gabor functions yields a non-orthogonal set of functions facilitating in multi-orientation and multi-resolution analysis of the images. The non-orthogonality of Gabor filters implicates that the designed filters are redundant and this property will be specifically used to yield cancelable features of biometric images.

3.2 Convolutional Neural Networks

Convolutional Neural Networks (popularly known as ConvNet) are inspired by the physiological visual perception mechanism of the mammals and have the ability to obtain an effective representation of the images from their respective pixels with very little and at best no preprocessing. These are non-linear models that have the capability to learn the non-linear feature from the images [128]. A typical CNN model is primarily composed of a series of layers which are convolutional in nature and are followed by some intermediate layers (known as the convolutional base) [129]. The series of layers are interconnected such that they have the ability to extract distinctive patterns from the input images. The obtained patterns can be used to perform different classification tasks useful for a wide range of vision based applications. In order to employ CNNs, let us first understand the processing done by the fundamental constituent layers of a CNN.

3.2.1 Convolutional Base

The convolutional base is composed of three fundamental components in a CNN model, namely the convolutional layer, activation function, and pooling layer. The first compo-

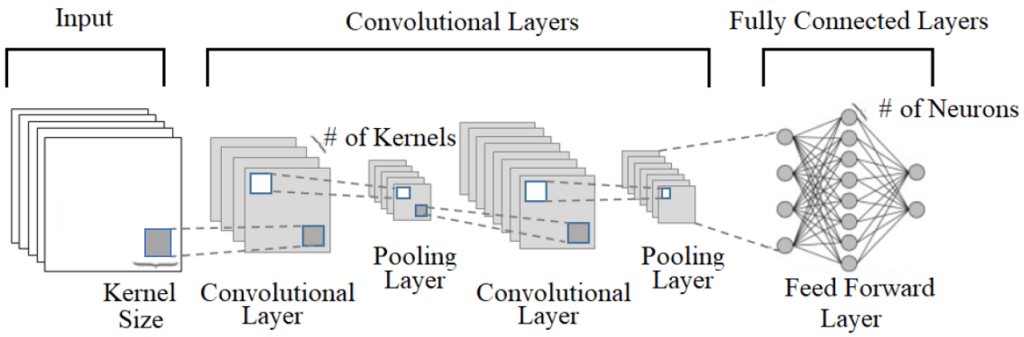

Figure 3.1: A Typical Sequential ConvNet.

nent i.e. the convolutional layer takes a tensor as an input and transform it into feature maps. this is done by applying convolution with a matrix of weights (or kernel), followed by the addition of a bias. Each convolutional layer uses a number of kernels to replicate the process of convolution in order to generate the features maps as an output.

A feature map is generated by the application of convolution of a learned kernel with the input, followed by the applying non-linear activation function on every output element. The desired non-linearity in a multilayered CNN is introduced by this layer. There are three basic activation functions which are employed, ReLU, tanh and sigmoid. ReLU layer eliminates the negative values from the feature map, assigning a zero to all of them and preserves all the positive values. There are studies showing that ReLU allows an efficient training of the CNNs as compared to their other counterparts.

There are a large number of features which are parametrized in a convolutional layer. A pooling (subsampling) layer is commonly added before the subsequent convolutional layers in a CNN. This layer applies a pooling function (average or max- pooling) on the features maps which selects a subset of numerical values from a local region in the image. By stacking different pooling and convolutional layers coarse to high level representations are possible, leading to the possibility of using the network for the classification of the images effectively. Appropriately, a combination of several convolutional, activation and pooling layers can lead to performing feature extraction from the images. The Deep ConvNets use the combined benefits of the convolutional base and layered hierarchy to learn representations for specific visual recognition tasks. After several convolutional and pooling layers one of more fully connected layers exist, similar to a multi layer perceptron. These fully connected layers help in amplifying the selective distinctive patterns in the images. The features extracted from the fully connected layer are employed

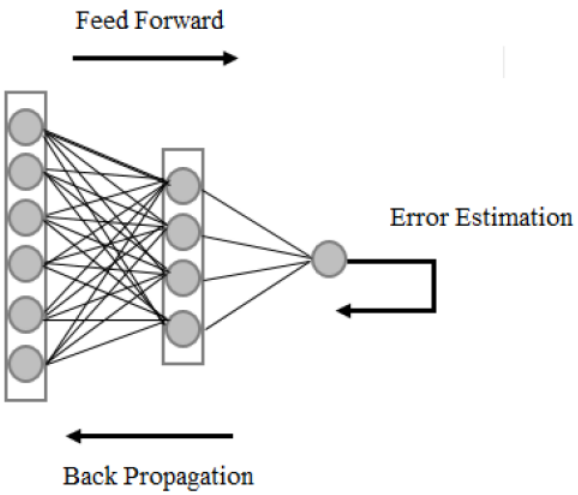

Figure 3.2: Network training in forward and backward direction.

for classification.

3.2.2 CNN Architectures

With an increase of the usage of ConvNets for various computer vision tasks, several architectures have been proposed in the literature. These include VGGNet [130], AlexNet [129], residual models like ResNet [131] and Inception models [132]. The AlexNet and VGG architectures are composed of alternating blocks of convolutional and activation layers. These models have three fully connected layers and the last layer of which is used for classification. The concept of inception blocks was introduced in inception models, in which every block is composed of the convolutional and pooling layers which are in sequence to enhance the learning. The ResNet architectures are represented by residual networks in which the layers contain the direct and additive connections also referred to as the skip connections to the subsequent layers.

3.2.3 Transfer Learning

A forward pass in a CNN model is used in order to take an input image and pass it from the CNN architecture to learn the prediction of probabilities. Nevertheless, before starting the make predictions from a CNN model it requires extensive training. This involves a forward pass (Feed Forward) and a backward pass (Back Propagation) as shown in Figure 3.2.

For a given training sample, the network produces an output. This output is used to generate the error and the loss is computed by calculating the difference between the output and the target ground truth. The objectives in the design of a network is typically to minimize the loss.

3.2.4 CNN Parameters

The main parameters which are important in the deisgn of CNNs are as follows:

- **Optimizer:** The optimizer algorithm is used to initialize the kernel weights and bias values of the nodes in a neural network. It makes adjustments based on the performance yielded by the loss function [133].
- **Loss function:** The error produced by the current state of the CNN model has to be calculated repeatedly. This require choosing an appropriate error function, termed as a loss function that calculates the performance of the model iteratively so that the weights can be appropriately adjusted.
- **Activation function:** An activation function calculates an output from an input or a set of inputs, and decides which neurons have to be activated / deactivated to get the desired output. They perform a non-linear transformation in the input to get better results from a complex network.
- **Learning rate:** The fourth important tuning parameter of a network is its learning rate. When the learning rate is small, the optimizer tends to be very slow and has the ability to get stuck at a local extrema whereas a large learning rate may result in finding a solution which is sub-optimal.

Chapter 4

Proposed Methodology

In chapter 3, the components which are utilized for the proposed cancelable multibiometric system have been presented. Mainly, these methods can be described through three important phases: pre-processing, feature extraction, cancelable template generation and user verification. Before presenting a walk-through of the proposed method, let us introduce the imaging modalities which we are using for the proposed work:

4.1 Biometric Modalities

There are several hand based modalities which have been discussed briefly in chapter 2. Primarily we will be focusing on multispectral hand palm based biometrics. The hand palm based modality refers to the usage of white light in order to illuminate palm of the hand. A human palm exhibits a large number of features which make a human

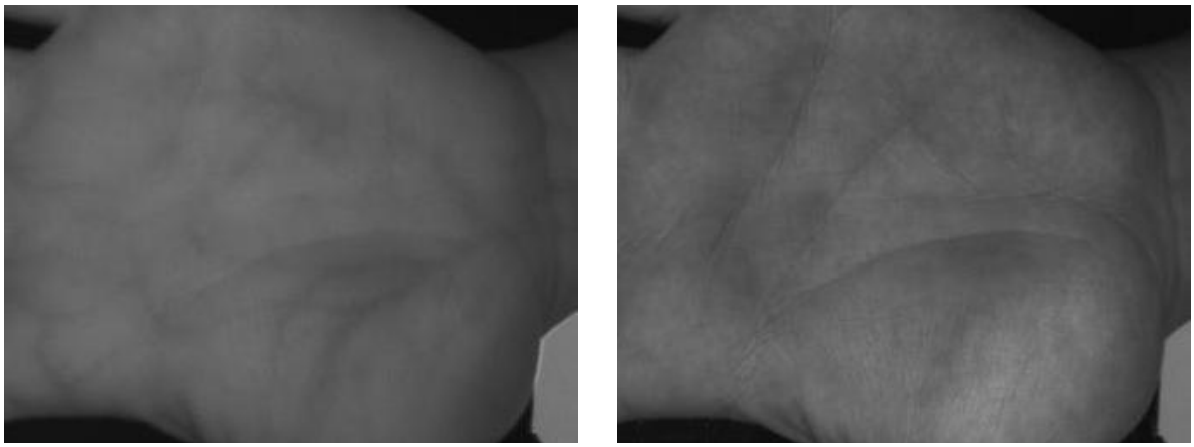

Figure 4.1: Some sample images of selected biometric modalities.

identifiable. These features mainly include the skin lines and creases which are quite unique for every individual.

Although a hand palm is quite effective as a biometric modality due to its presence on the superficial surface of the skin, it is exposed to different external factors such as cuts, bruises which may effect the ability of the systems to differentiate among the people. Keeping this in view, we are considering another modality for the proposed biometric system which is hand veins. These veins are typically not visible using the white light and thus are not detectable using standard cameras. A narrow band of light is used to illuminate the palm of the hands, which travels through the superficial skin and enhances the contrast due to high absorption of light by the veins. These enhanced veins are effectively used for executing biometric systems. The main advantages of hand veins include their robustness to superficial injury to the hands and high discriminative power for authentication of the users. We aim to propose a cancelable multibiometric system based on the above mentioned modalities.

4.2 Preprocessing

The main features which are distinctive for different users are the creases and valleys in the hand pattern for palm images and the veins for hand vein images. In order to extract these features effectively, a multiresolution technique is required which has the ability to find the fine patterns which are available in the images. It is well known from the literature that Gabor filters are special types of multiresolution wavelets which have

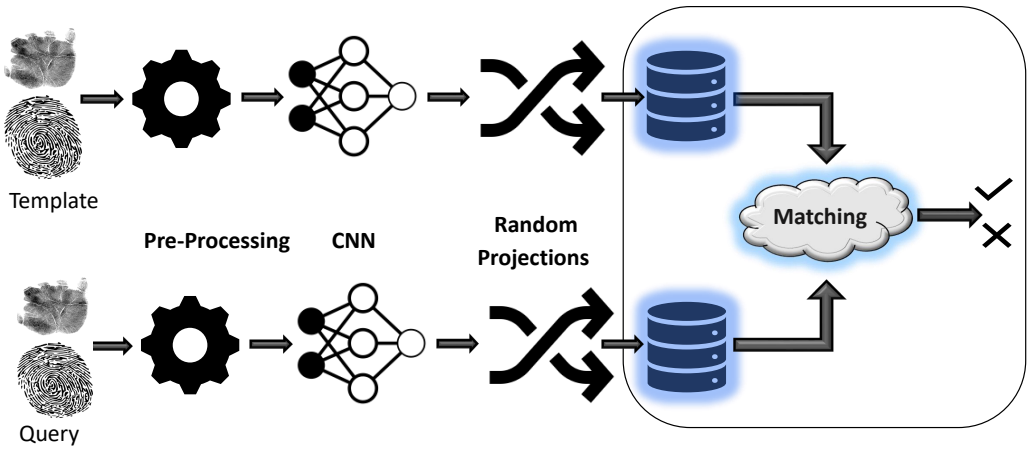

Figure 4.2: Proposed Framework

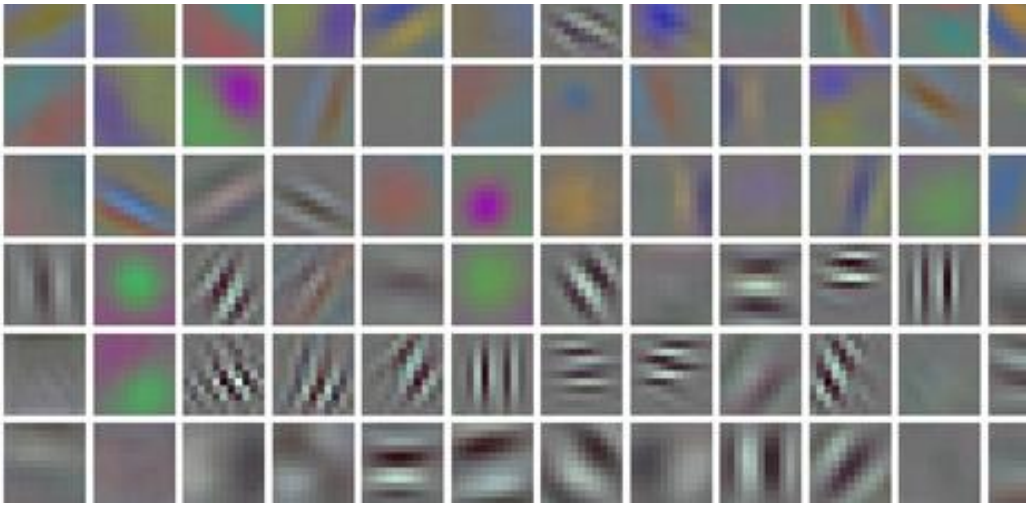

Figure 4.3: Visualization of typical trained filters of the first layer of Convolutional Networks, bearing a remarkable similarity with the Gabor filters (adapted from [1])

the ability to enhance the fine structures in the images. The use of Gabor filters offers four distinct advantages:

- **Multi-resolution features:** Gabor filters are very famous for their advantages over several texture feature extraction techniques due to their multiresolution nature. This property of Gabor filters helps in a coarse to fine analysis of the images which is compulsory for the visualization of an image texture at different levels of detail.

- **Enhancement of Texture Attributes:** Due to the direction and orientation sensitivity of Gabor filters, they have the ability to extract salient texture features in the images. This property is useful for most of the texture feature analysis techniques.

- **Non-orthogonality of Gabor Wavelets:** An important property of Gabor filters is non-orthogonality. Although this is typically taken as a disadvantage of Gabor filters as compared to standard wavelets, we will use this property to analyze the irreversibility of templates when they are subjected to Gabor filtering.

- **Similarity of Gabor responses to trained convolutional layers:** It is important to note that a standard CNN is composed of several convolutional layers and if the impulse responses of these convolutional filters (after being trained) are analysed, they show a remarkable similarity to Gabor filters. We exploit this

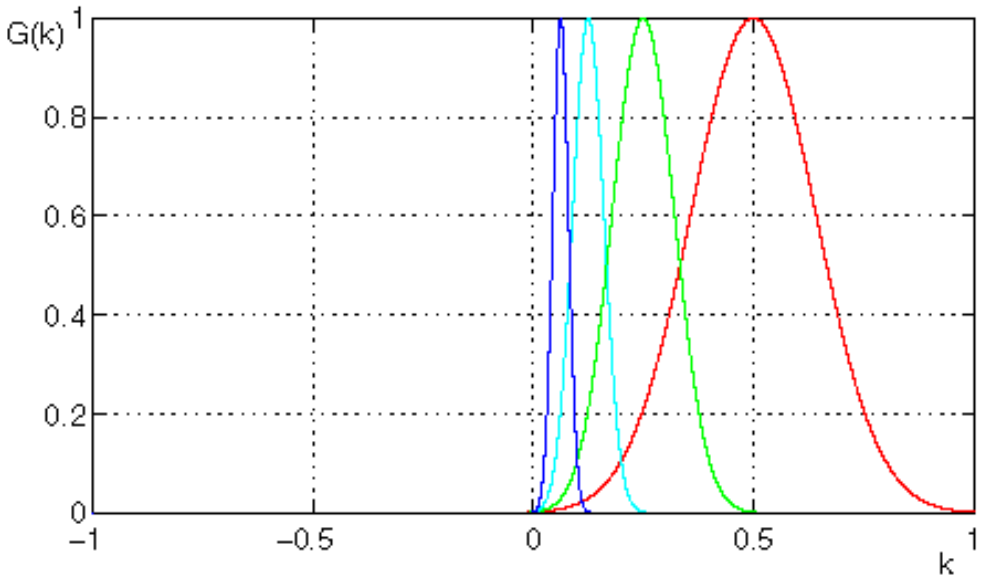

Figure 4.4: Non-Orthogonality of Gabor wavelets

behavioral similarity of Gabor filters to trained convolutional layers in order to achieve better results.

Gabor filtering is a parametric method which has the ability to generate different kernels for performing filtering of the images. The random values of these parameters based on a user specific key can be used to acquire features, which are cancelable. In our implementation, we use propose the randomization of the orientation parameter in order to achieve cancelable properties for the generated template.

4.2.1 Orientation Randomization

Let us assume that we generate K pseudo-random numbers $r_1, r_2, ..., r_S$, one for each orientation. The corresponding filter design can be achieved as a result of the modifications in equations 3.1.5 and 3.1.6 as follows:

$$x'_c = a^{-m}(x\cos\theta' + y\sin\theta')$$

$$y'_c = a^{-m}(-x\sin\theta' + y\cos\theta').$$

$m = 1, 2, ..., S$ and $n = 1, 2, ..., K$. S and K are number of scales and number of

orientations respectively, $\theta' = r_n\theta$ and r_n corresponds to the n^{th} random number. The value of θ is the same as previously defined i.e. $\theta = n\pi/K$.

4.2.2 Cancelable Properties

The randomization of orientation parameter of Gabor filters generate a chaotic matrix. When the biometric images are convolved with these chaotic matrices, cancelable templates are generated. The pseudo-randomness of the chaotic matrices guarantees the security of the template. If the template is compromised, a set of new pseudo-random numbers $r_1, r_2, ..., r_n$ are used to generate a new set of chaotic matrices thus preserving the privacy of the templates.

4.3 Feature Extraction

Due to the successful usage of CNNs in image recognition tasks, their architectural usage is wide spread and has led to a very wide range of contributions by different researchers. In this context, Simonyan et al. [130] proposed an effective and simple CNN architecture that is widely employed for various applications and is also used in the proposed feature extraction framework. The architecture was named VGG and is composed of multiple convolutional and pooling layers. Specifically, we are using the VGG-19 network which is composed of 19 layers. The advantages of the VGGnet over some other well known networks are as follows:

- Network depth: Empirical findings show that an increased depth of the network shows improved performance in different recognition tasks.
- Filter size: The predecessor ConvNet (ZfNet [134]) suggested that performing convolution with filters of smaller sizes gives better performance. Keeping this in view, the VGGNet replaced 11×11 and 5×5 filters with those of size 3×3. This reduced the number of parameters of the the network, reducing its computational complexity.

The architecture of a VGG19 network is shown in Figure 4.5. A typical VGG network has four different types of layers that are: convolution layer, max-pool layer, fully connected layer (FC), and a soft-max classification layer. The convolution layer performs the

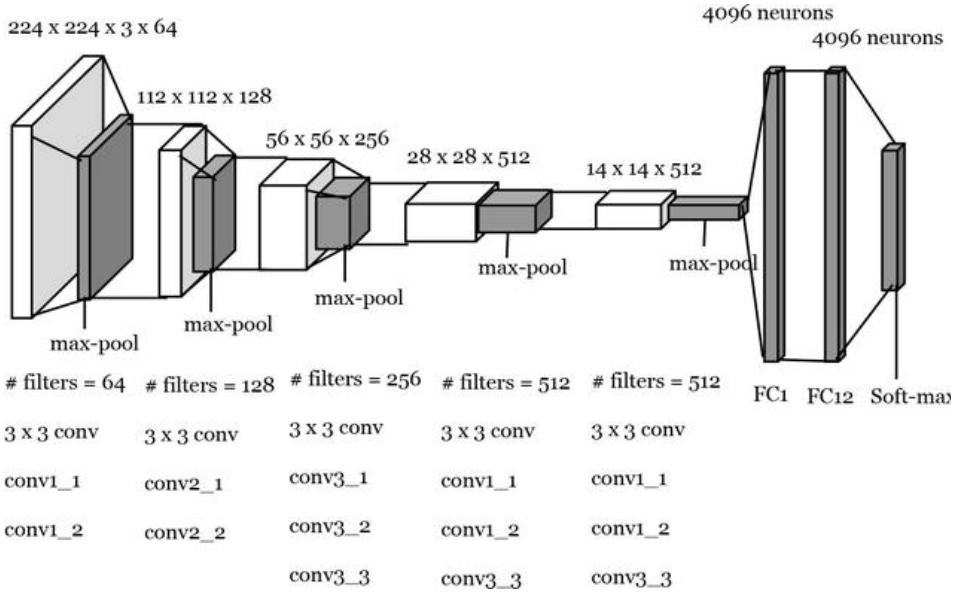

Figure 4.5: Architecture of the VGG-19 ConvNet (adapted from [2])

convolution operation of the input image with a pre-trained filter. As depicted in the figure, size of the input image is 224 × 224 × 3 and there are 64 filter of the size 3 × 3 in the first layer. As we go deep in the VGG network, the number of filters for convolution increases from 64 to 512 filters.

IN VGG19 dimensionality of input data is done by the max-pooling layer. Specifically, a sliding window of the size 2 × 2 has been used for carrying out the max value in the sliding box which reduces the input data. After the max-pooling operation, the size of the image is reduced from 224 X 224 to half of its size and becomes 112 × 112. These operations i.e convolution and max-pooling keeps on repeating till the final size f the image becomes 14 × 14. At the end a flattening operation is performed to reshape the data from 14 × 14 × 15 to be as 1-D vector of size 4096.

The image is taken as an input which is fed into a stack of convolutional layers, each layer is composed of a small receptive field of size 3×3, the convolutional stride is fixed to 1 pixel. The first two blocks are composed of two convolutional and one max pooling layer. The subsequent 3 blocks are composed of 4 convolutional layers followed by one max pooling layers. The output from these block is flattened and fed into fully connected hidden layers followed by the output layer as shown in fig **??**.

Figure 4.6: A Typical Sequential VGG19.

4.4 Random Projection

Feature extraction is followed by the generation of a cancelable template by applying a relevant transform. This transform results in the creation of a secure cancelable template, that cannot be inverted to its original form. It becomes very difficult for an attacker to obtain the original template after it has been transformed using a non-invertible technique. If any suspicious activity takes place or the template is compromised, a novel template is issues causing minimal changes / damage to the system. Another advantage is that it is possible to use various random projections to generate different templates for difference applications. According to Johnson and Lindenstrauss lemma [135],

> "if points in a vector space are of sufficiently high dimension, then they may be projected into a lower-dimensional space in a way which approximately preserves the distances between the points".

It is important to note that the Euclidean distance between feature points is maintained before and after projection, thus preserving their statistical properties. Therefore, the random projections are proven to be quite successful for obtaining cancelable biometric templates.

Let us assume that we generate features vector corresponding to the biometric data of the i^{th} user, F_i. Let G^o be an orthogonal matrix generated using a key K which is assigned to a user during the enrollment process. For N users, we generate $K_1, K_2, ..., K_N$ keys, one corresponding to every user. This generates N projection matrices $G^o_1, G^o_2, ..., G^o_N$. Once the feature vector for i^{th} user, F_i is obtained, the transformed feature set is obtained

after projection of these features on G_i. After this projection, a cancelable template for the i^{th} user is obtained which is stored in the database.

4.5 Matching

After the enrollment of a user, the cancelable templates are stored in the database. The verification process was carried out on the cancelable templates stored in the database. We are dealing with matching as a simple comparison problem. When a user wants to gain access to the system, his biometric data is acquired followed by Gabor filtering, feature extraction using VGG-19 network and performing random projection using the key used to generate the token for that respective user. Later, matching is performed using euclidean distance between the template of the respective user that is stored in the database.

Chapter 5

Experimental Results

In chapter 4 we have presented the proposed methodology that has been used in this thesis. The application of this method requires validation to be carried out on a biometric database, which is carried out in this chapter which is composed of two main sections: 1. A discussion about the performance obtained of the proposed method in terms of accuracy, and 2. A discussion about the privacy analysis of the proposed biometric template extraction method. In this thesis, we have focused on hand based modalities which is mainly motivated by the various advantages including better privacy preservation, ease of acquisition and the low cost hardware requirements for acquisition of the images.

5.1 Dataset

For carrying out our experiments we have used CASIA dataset, which is composed of multispectral palm images acquired by lights of various narrow bands to illuminate the human palms (hence called the multispectral palm images). The dataset is composed of 3000 images from 100 people. Although, different spectra are composed of different types of information using all images from the dataset will result in redundancy as some of them are visually very similar and do not convey any distinct information about a user. In specific, we have used images from two specific wavelengths: the white light, which is composed of the visible spectrum and is mainly used to the illuminate the palm patterns in the images . The other wavelength which is significant is light of a narrow band composed of 940nm, which mainly lies in the infrared range of the electromagnetic spectrum. The advantage of using the IR light is that it has a high absorption in the

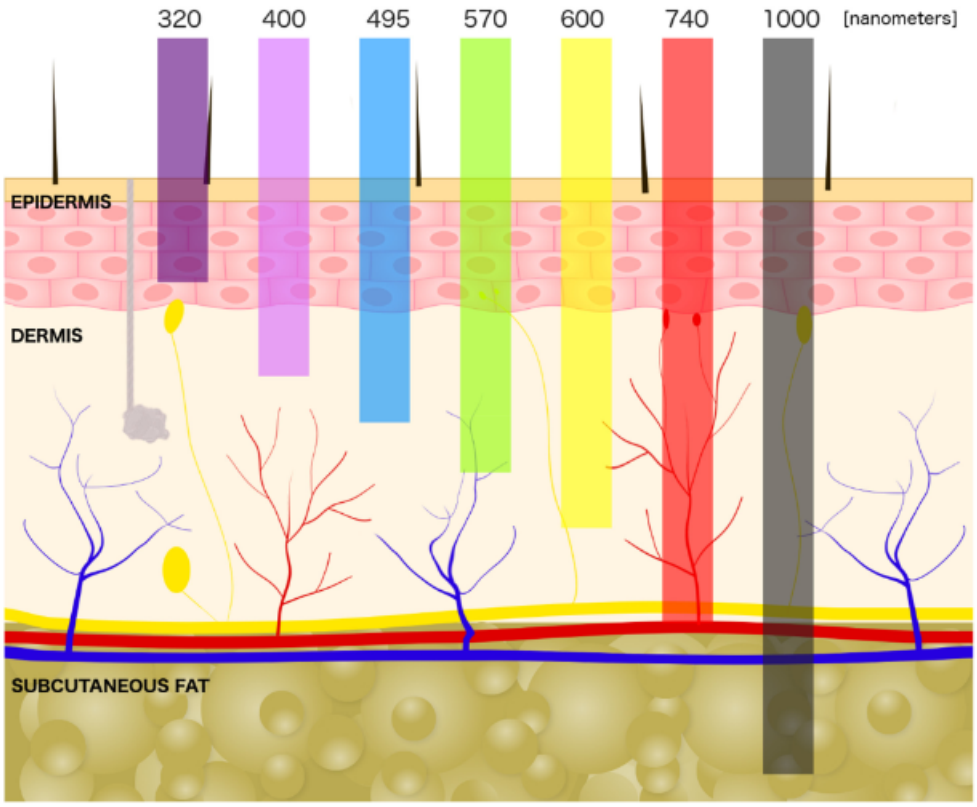

Figure 5.1: Skin cross section showing penetration of different wavelengths of light in the skin (adapted from [3]).

skin, leading to the generation of high contrast patterns in the images. Specifically, the blood vessels under the skin are enhanced using this spectrum, which enables the visualizes the subsurface structures in the images. The structures (vein patterns) are used as biometric in the palm veins and the respective images in the dataset are visible in the images which are tagged as having 940nm wavelength.

5.2 Experimental setup

There are several intricacies in the design of the test bench which has been designed to validate the proposed methodology. The proposed method is composed of Gabor filters, feature extraction (using VGG-19 network) and random projection. Their parameters are chosen as follows:

5.2.1 Gabor filter parameters

The Gabor filters have two main parameters: number of scales and number of orientations. We have performed Gabor decomposition using 4 orientations and two scales. The angular decomposition for controlling orientation parameter is kept at 45^o. For the scale parameter, the center frequency for the filter corresponding to higher frequency is kept at 0.25 whereas low frequency is kept at 0.05. It should be kept in mind that a higher number of scales and orientations can be elected but this will increase the computational complexity of the proposed method. This is because, every additional scale or orientation will generate a new filter with which the image has to be filtered. This increases the computational complexity of the method significantly. We have performed a grid search for a range of parameters and results show that the selected parameters achieve very good matching rates for the selected parameters. There is no significant improvement in the performance of the proposed method with an increase in the number of scales and orientations of the Gabor filters.

5.2.2 VGG-19 Parameters

For our experiments, we have used the pretrained VGG-19 network, that was trained on the "imagenet" dataset. The last three fully connected layers of the trained VGG-19 network are not included for our set of experiments. This is because we are using the network purely for the purpose of feature extraction. The model performs pooling using "average pooling".

5.2.3 Random Projection

The output of the VGG-19 network produces a feature vector of size 1×16896. RP has to be used in order to create cancelable templates for a particular image. In order to obtain these templates, a normally distributed, zero mean and unit variance token of size 1 is generated for a particular user. The biometric data obtained for a specific user is filtered, followed by feature extraction. Later, the learned features are projected using their respected projection vectors generated from the tokens leading to cancelable templates for every user.

5.2.4 Performance measurement

The generated templates have to be compared with those obtained for the new images. For making this comparison, we have used Euclidean Distance. The performance is measured using two parameters: Correct Recognition Rate (CRR), False Accept Rate (FAR) and False Reject Rates (FRR) which are defined as follows:

- **False Accept Rate (FAR)** : Describes the percentage of an impostors that were incorrectly verified as a genuine users. It is calculated on the basis of following formula:

$$FAR = \frac{FA}{FA + TR} \tag{5.2.1}$$

- **False Reject Rate (FRR)** : Describes the percentage of genuine users that were mistakenly rejected from a biometric system. It is calculated on the basis of following formula:

$$FRR = \frac{FR}{TA + FR} \tag{5.2.2}$$

- **Correct recognition rate (CRR)** : It gives the probability that the system will correctly identify the input template from the templates in the database. It is given by the formula:

$$CRR = \frac{TA}{TA + TR} \tag{5.2.3}$$

5.3 Results

In this section, we will discuss about the overall results that have been obtained using the proposed method. We will start with a discussion about the overall CAR and FAR measures for various methods considered for comparison purposes.

5.3.1 Overall results

In our experiments, we have performed comparison of the proposed method with several other methods. We have mainly used two different types of methods for this comparison: CNN based methods, and Statistical methods. Among the CNN based methods, we have made comparison with other networks including Inception, VGG-16, VGG-19, and

ResNet50. For the calculation of results, we have used one image from the dataset of a specific user as a training image and use the rest for the purpose of validation of the results.

Tr	InceptV3	Resnet50	VGG	Prop
1	71.78	81.25	84.68	96.95
2	85.97	89.02	93.43	96.24
3	92.24	93.09	94.71	97.51
4	94.53	94.71	95.59	98.05

Table 5.1: Correct recognition rates using different methods based on convolutional neural networks.

Our experiments show that the proposed method outperforms the other methods that have been considered in this study. Generally, the Inception shows a lower overall accuracy as compared to the other ConvNets. In the proposed method, Gabor filters are used for filtering the images followed by the used of VGG-19 network for feature extraction. As can be seen in Table 5.1, the VGG network performs well as compared to the other networks, empirically validating the choice of network for feature extraction purposes for our implementation. The performance improvement in the proposed approach is attributed to the fact that the use of Gabor filters enhances the vascular structure in

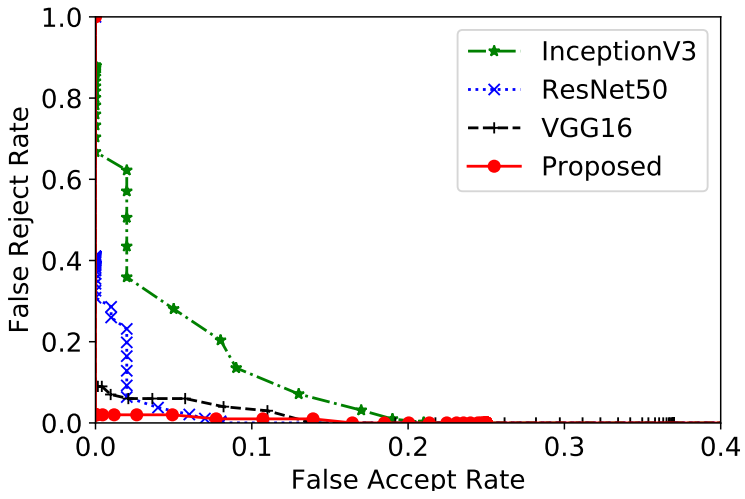

Figure 5.2: Performance of various ConvNet based methods in biometric recognition in terms of false accept and false reject rates.

the images, assisting in achieving a higher accuracy in recognition.

A visual analysis of Figure 5.2 shows that the proposed method outperforms the other methods in terms of false accept and false reject rates. Among the other methods, the InceptionV3 model shows poor performance.

Table 5.2: Confusion Matrix

	Predicted Labels	
True	98.21% (TPR)	1.79% (FNR)
Labels	1.14% (FPR)	98.86% (TNR)

The confusion matrix corresponding to the proposed method is shown in Table 5.2. As can be seen, the TPR and TNR are very high indicating the proficiency of the proposed method. It should be noted that amongst the errors yielded by the method the majority are FNR, indicating that the algorithm is conservatively sifting the samples for authentication. Moreover, the results shown are samples at an operating thresholds yielding a high TPR. If more conservative thresholds are used, the algorithm performs authentication with a TPR of ≈97% with a FNR of 0%.

5.3.2 Impact of Noise

Noise is an important factor that should be considered as far as the acquisition of biometric data is concerned. This is because, the data acquired from the sensors can have a significant level of noise which can be mainly due to the settings of the acquisition platform. Therefore, an analysis of the stability of the system is important in order to establish the robustness of the proposed system to noise. In order to do this, we add Additive White Gaussian Noise (AWGN) to our images and perform authentication on the noisy images.

Our experiments show that the proposed method outperforms the other methods in the presence of noise in the images. We attribute these good results to the fact that the Gabor filters are composed of a combination of Gaussian windows, modulated by a complex sinusoid. The frequency response of the Gaussian function is also a sinusoid. Effectively, this means that the filtering the images using Gabor filters has an inherent smoothing response of the images that helps in mitigating the noise in the images. In contrast, the techniques which use only raw image for recognition purposes do not

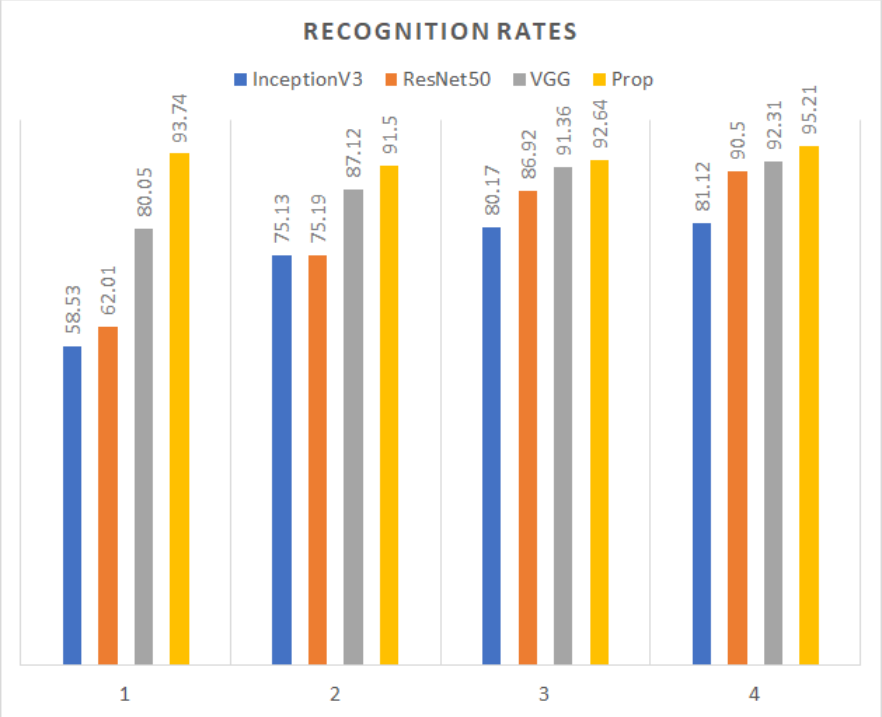

Figure 5.3: Correct recognition rates for noisy images using different methods based on convolutional neural networks.

inculcate any noise removal mechanism hence resulting in relatively lower recognition rates. In this context, we have also performed a detailed analysis of the impact of noise on the proposed method (Figure 5.3).

5.4 Privacy Analysis of Cancelable Templates

In the proposed methodology, the cancelable properties of the proposed templates are obtained using two important factors: 1. The generation of random orientations, and 2. The procedure of Random Projection. For an analysis of cancelable properties of the templates, we have considered three important factors: Diversity, Unlinkability and Non-Invertability:

5.4.1 Diversity

Each user has the capability to have his own token to generate the PRN. This enables the system to generate multiple templates from the same biometric images/sample using the randomized Gabor filters with the help of the respective PRN. Another important point

to consider is that we are using RP for template generation, which uses a key/token for a specific user and generates a random matrix on which the projection of the data is obtained to obtain the relevant template. In case a template is compromised, a new key is used to generate another template for the same biometric data, which is distinct from that obtained using another key.

5.4.2 Revocability/Reusability/Unlinkability

In the proposed method, the cancelable templates can be easily revoked or reissued by a new set of PRN when compromised. The cancelable property of the generated templates is empirically assessed for similarity when different PRNs are used to generate the templates for different users. In addition, the use of RP adds another layer of security in the templates creating more distinct templates. For quantifying unlinkability we have used T-test which, according to [136] is known to quantify the similarity/dissimilarity of the features. In most T-tests, a P-value of 0.05 or less indicates that the data is valid. For the features, lowest P-value obtained is $7.37e-90$ and upto 93% features are found to be significant with P-values of less than 0.05. In contrast, if the cancelable templates are not used, less than 1% features exhibit P-values of less than 0.05 whereas the remaining more than 99% features are found to exhibit P-values of more than 0.05, indicating the similarity of features when RP and randomized Gabor filtering is not performed. This validates the efficacy of the proposed method, generating unlinkable templates for different applications.

Method	**P-value**			
	min	max	$P < 0.05$	$P > 0.05$
With RP	$7.37e-90$	0.99	92.5%	7.5%
Without PR	0.0013	0.99	0.9%	99.1%

Table 5.3: Correct recognition rates for noisy images using different methods based on convolutional neural networks.

5.4.3 Non-Invertability

The extraction of biometric templates is carried out using various methods, ensuring the non-invertability of the templates. First and foremost, the Gabor filters which

are used for decomposition of the images are non-orthogonal. This property of non-orthogonality is inherently present due to the use of Gaussian function during filter design [137]. Effectively, the Gabor filters are non-orthogonal and therefore are non-invertible elucidating on the fact that the templates obtained using Gabor filters are inherently non-invertible. Moreover, the generation of impulse responses of Gabor filters involves the use of a PRN for generating different orientation filters. In addition, the use of RP also ensures the non-invertability of the templates if the keys used are not available for authentication.

5.5 Discussion

In this chapter, we have discussed the experimental results of the proposed method and also compared them with some other methods based on ConvNets which are available in the literature. Our experiments have shown that the proposed methods have outperformed the other methods which are available in the literature. The proposed method achieves very good authentication results. We have also performed an analysis of the proposed methods in the presence of noise in the images. The simulations have been carried out by the addition of additive white Gaussian noise (AWGN) and the proposed method consistently produces better results in comparison to its counterparts.

Finally, an analysis of the cancelable properties has also been done showing that the template protection methodology adopted in this work produces diverse templates due to the use of keys for the generation of random projection matrix. The templates are non-invertible owing to the non-invertability of Gabor filters and the requirement of keys for reversing the RP operation. The generated templates are also unlinkable which has been validated by using the t-test analysis of the features obtained using the proposed methods. Therefore, the proposed method produces templates which are secure and produce very good authentication results.

Chapter 6

Conclusions and Future Work

In this thesis, we have proposed a novel method for the extraction of cancelable biometric templates from the palm images. The prime focus has been on the use of hand based modalities for performing biometric authentication. This is attributed to the fact that the the data acquisition task for such modalities is relatively simple and unlike e.g. face recognition, the privacy of the individual is effectively preserved due to which these modalities are generally preferred. For the purpose of the study that has been carried out in this thesis we have used the CASIA dataset, which is a multispectral hand palm dataset. It is called multispectral because it uses different wavelengths of light in the visible spectrum for acquisition of the images. Some specific visible wavelengths are able to enhance the vascular structure in the images which can also be used for the purpose of biometric authentication. This generates a complementary visualization of the images with respect to the vascular structure in contrast to the palm patterns, evident using white light.

The images are subjected to the extraction of region of interest using standard segmentation methods, after which they are usable for authentication in this specific problem. There are several approaches which have been published in the literature for feature extraction which can be mainly categorized into four distinct types: statistical, model based, hand crafted and deep learning based methods. Lately, the deep learning based methods have shown significant promise in biometric authentication methods and have been widely used in the literature. Therefore, we have opted for deep learning based methods for feature extraction. However, from the literature it is clear that the detection of vessels has been widely investigated using directional filters. Since we are using

narrow band images for the detection of vessels, we believe that the use of Gabor filtered images would enhance the vascularity in the images leading to a better feature set for the proposed problem. Moreover, the directionality and scale specificity of the Gabor filters also make them a valid choice of the detection of palm prints.

We preprocessed the images using Gabor filters followed by the extraction of features using the VGG-19 network. While performing Gabor filtering, there are two important parameters which are used in the generation of impulse responses: number of scale and orientations. We have used orientation randomization in order to obtain secure templates from biometric modalities. This implies that if the templates are compromised, a new template can be generated based on a new key making the templates revocable without effecting different applications using the templates. The feature extraction using VGG-19 is followed by random projection, which generates a transformation matrix on which the biometric data is projected in order to obtain a secure template. If the template is compromised, it can be easily revoked and a new template can be generated based on a new key for a specific user. The use of keys can even be customised for different applications ensuring that if security of one application has been compromised, it does not have any impact on the other one.

Our experiments have shown that the proposed method has shown good results with a high recognition rate while keeping the false accept and false reject rates at a minimal level. This validates the functional capabilities of the proposed method. The methods has also been compared in terms of the recognition rate obtained with other methods including the most well known deep learning based methods. Although the other methods have the ability to achieve good recognition rates, their false accept and false reject rates are relatively high. In addition to quantifying the efficiency of the propose method, we have also performed a security analysis of the templates. In order to do this, we have used the T-test to compare the significance of features for the proposed method and that in which the cancelable templates are not generated. The proposed method produces highly secure templates which are significantly different when different keys are used to generate the keys. The non-invertability of the features is guaranteed with the use of Gabor filters given that these are non-orthogonal set of filters for which the reverse transformation does not yield the exact same template.

Although the proposed method shows good results, it would be interesting to use the

proposed method of a diverse dataset with a large number of samples to ensure that the method generates different templates for a large number of users. It would also be interesting to see how can different modalities be used in order to generate secure templates. There are some other research questions which can be effectively investigated including the use of more complex fusion techniques for fusing information from different biometric modalities. Moreover, it should be noted that the implementation of biometrics has to be typically carried out in real time. Since the proposed technique involves filtering using a filter bank, it can be computationally a complex task. It would be interesting to carry out a complexity analysis of the proposed technique and see how simplifications can be done in terms of computations while achieving optimal authentication results.

References

[1] Anselm Brachmann and Christoph Redies. Using convolutional neural network filters to measure left-right mirror symmetry in images. *Symmetry*, 8(12):144, 2016.

[2] Hussein Samma and Shahrel Azmin Suandi. Transfer learning of pre-trained cnn models for fingerprint liveness detection. In *Biometric Systems*. IntechOpen, 2020.

[3] Aleksandra Cios, Martyna Cieplak, Łukasz Szymański, Aneta Lewicka, Szczepan Cierniak, Wanda Stankiewicz, Mariola Mendrycka, and Sławomir Lewicki. Effect of different wavelengths of laser irradiation on the skin cells. *International Journal of Molecular Sciences*, 22(5):2437, 2021.

[4] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40 (3):614–634, 2001.

[5] Arun Ross, Karthik Nandakumar, and Anil K Jain. Introduction to multibiometrics. In *Handbook of biometrics*, pages 271–292. Springer, 2008.

[6] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Multibiometric cryptosystems based on feature-level fusion. *IEEE transactions on information forensics and security*, 7(1):255–268, 2011.

[7] Natasha Arjumand Shoaib Mirza, Haider Abbas, Farrukh Aslam Khan, and Jalal Al Muhtadi. Anticipating advanced persistent threat (apt) countermeasures using collaborative security mechanisms. In *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, pages 129–132. IEEE, 2014.

[8] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recog-

nition. *IEEE Transactions on circuits and systems for video technology*, 14(1): 4–20, 2004.

[9] Anil K Jain, Karthik Nandakumar, and Arun Ross. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern recognition letters*, 79: 80–105, 2016.

[10] Weizhi Meng, Duncan S Wong, Steven Furnell, and Jianying Zhou. Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials*, 17(3):1268–1293, 2014.

[11] Zhang Rui and Zheng Yan. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE Access*, 7:5994–6009, 2018.

[12] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov, Minkyu Choi, et al. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2(3):13–28, 2009.

[13] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[14] Lin Hong, Yifei Wan, and Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation. *IEEE transactions on pattern analysis and machine intelligence*, 20(8):777–789, 1998.

[15] Chengsheng Yuan, Xingming Sun, and Rui Lv. Fingerprint liveness detection based on multi-scale lpq and pca. *China Communications*, 13(7):60–65, 2016.

[16] Wenyi Zhao, Rama Chellappa, P Jonathon Phillips, and Azriel Rosenfeld. Face recognition: A literature survey. *ACM computing surveys (CSUR)*, 35(4):399–458, 2003.

[17] Iacopo Masi, Yue Wu, Tal Hassner, and Prem Natarajan. Deep face recognition: A survey. In *2018 31st SIBGRAPI conference on graphics, patterns and images (SIBGRAPI)*, pages 471–478. IEEE, 2018.

[18] Hao Wang, Yitong Wang, Zheng Zhou, Xing Ji, Dihong Gong, Jingchao Zhou, Zhifeng Li, and Wei Liu. Cosface: Large margin cosine loss for deep face recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 5265–5274, 2018.

[19] Kien Nguyen, Clinton Fookes, Raghavender Jillela, Sridha Sridharan, and Arun Ross. Long range iris recognition: A survey. *Pattern Recognition*, 72:123–143, 2017.

[20] Lavinia Mihaela Dinca and Gerhard Petrus Hancke. The fall of one, the rise of many: a survey on multi-biometric fusion methods. *IEEE Access*, 5:6247–6289, 2017.

[21] Muhtahir O Oloyede and Gerhard P Hancke. Unimodal and multimodal biometric sensing systems: a review. *IEEE Access*, 4:7532–7555, 2016.

[22] Juan Sebastian Arteaga-Falconi, Hussein Al Osman, and Abdulmotaleb El Saddik. Ecg authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement*, 65(3):591–600, 2015.

[23] Raffaele Cappelli, Matteo Ferrara, Annalisa Franco, and Davide Maltoni. Fingerprint verification competition 2006. *Biometric Technology Today*, 15(7-8):7–9, 2007.

[24] Fanglin Chen, Xiaolin Huang, and Jie Zhou. Hierarchical minutiae matching for fingerprint and palmprint identification. *IEEE Transactions on Image Processing*, 22(12):4964–4971, 2013.

[25] De-Shuang Huang, Wei Jia, and David Zhang. Palmprint verification based on principal lines. *Pattern Recognition*, 41(4):1316–1328, 2008.

[26] David Zhang, Wangmeng Zuo, and Feng Yue. A comparative study of palmprint recognition algorithms. *ACM computing surveys (CSUR)*, 44(1):1–37, 2012.

[27] Dexing Zhong, Xuefeng Du, and Kuncai Zhong. Decade progress of palmprint recognition: A brief survey. *Neurocomputing*, 328:16–28, 2019.

[28] Lin Zhang, Lida Li, Anqi Yang, Ying Shen, and Meng Yang. Towards contactless palmprint recognition: A novel device, a new benchmark, and a collaborative representation based identification approach. *Pattern Recognition*, 69:199–212, 2017.

[29] Mohsen Tabejamaat and Abdolmajid Mousavi. A coding-guided holistic-based palmprint recognition approach. *Multimedia Tools and Applications*, 76(6):7731–7747, 2017.

[30] Yue-Tong Luo, Lan-Ying Zhao, Bob Zhang, Wei Jia, Feng Xue, Jing-Ting Lu, Yi-Hai Zhu, and Bing-Qing Xu. Local line directional pattern for palmprint recognition. *Pattern Recognition*, 50:26–44, 2016.

[31] Yingbo Zhou and Ajay Kumar. Human identification using palm-vein images. *IEEE transactions on information forensics and security*, 6(4):1259–1274, 2011.

[32] Sandip Joardar, Amitava Chatterjee, and Anjan Rakshit. A real-time palm dorsa subcutaneous vein pattern recognition system using collaborative representation-based classification. *IEEE Transactions on Instrumentation and Measurement*, 64 (4):959–966, 2014.

[33] J Enrique Suarez Pascual, Jaime Uriarte-Antonio, Raul Sanchez-Reillo, and Michael G Lorenz. Capturing hand or wrist vein images for biometric authentication using low-cost devices. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 318–322. IEEE, 2010.

[34] Hyeon Chang Lee, Byung Jun Kang, Eui Chul Lee, and Kang Ryoung Park. Finger vein recognition using weighted local binary pattern code based on a support vector machine. *Journal of Zhejiang University SCIENCE C*, 11(7):514–524, 2010.

[35] Septimiu Crisan. A novel perspective on hand vein patterns for biometric recognition: problems, challenges, and implementations. In *Biometric Security and Privacy*, pages 21–49. Springer, 2017.

[36] Rig Das, Emanuela Piciucco, Emanuele Maiorana, and Patrizio Campisi. Convolutional neural network for finger-vein-based biometric identification. *IEEE Transactions on Information Forensics and Security*, 14(2):360–373, 2018.

[37] Venance Kilian, Nassor Ally, Josiah Nombo, Abdi T Abdalla, and Baraka Maiseli. Cost-effective and accurate palm vein recognition system based on multiframe super-resolution algorithms. *IET Biometrics*, 9(3):118–125, 2020.

[38] Aleksandra Babich. Biometric authentication. types of biometric identifiers. 2012.

[39] Anil K Jain, Sarat C Dass, and Karthik Nandakumar. Soft biometric traits for personal recognition systems. In *International conference on biometric authentication*, pages 731–738. Springer, 2004.

[40] Shefali Sharma, Shiv Ram Dubey, Satish Kumar Singh, Rajiv Saxena, and Rajat Kumar Singh. Identity verification using shape and geometry of human hands. *Expert Systems with Applications*, 42(2):821–832, 2015.

[41] Vivek Kanhangad, Ajay Kumar, and David Zhang. A unified framework for contactless hand verification. *IEEE transactions on information forensics and security*, 6(3):1014–1027, 2011.

[42] Ajay Kumar and Ch Ravikanth. Personal authentication using finger knuckle surface. *IEEE Transactions on Information Forensics and Security*, 4(1):98–110, 2009.

[43] David Zhang, Guangming Lu, and Lei Zhang. Global information for finger-knuckle-print recognition. In *Advanced Biometrics*, pages 131–149. Springer, 2018.

[44] Wenming Yang, Xiang Yu, and Qingmin Liao. Personal authentication using finger vein pattern and finger-dorsa texture fusion. In *Proceedings of the 17th ACM international conference on Multimedia*, pages 905–908, 2009.

[45] Gaurav Jaswal, Amit Kaul, and Ravinder Nath. Knuckle print biometrics and fusion schemes–overview, challenges, and solutions. *ACM Computing Surveys (CSUR)*, 49(2):1–46, 2016.

[46] Karthik Nandakumar, Anil K Jain, and Arun Ross. Fusion in multibiometric identification systems: What about the missing data? In *International Conference on Biometrics*, pages 743–752. Springer, 2009.

[47] Patrick Grother and Elham Tabassi. Performance of biometric quality measures. *IEEE transactions on pattern analysis and machine intelligence*, 29(4):531–543, 2007.

[48] Prem Sewak Sudhish, Anil K Jain, and Kai Cao. Adaptive fusion of biometric and biographic information for identity de-duplication. *Pattern Recognition Letters*, 84:199–207, 2016.

[49] Rubal Jain and Chander Kant. Attacks on biometric systems: an overview. *International Journal of Advances in Scientific Research*, 1(07):283–288, 2015.

[50] Mohamed Elhoseny, Ehab Essa, Ahmed Elkhateb, Aboul Ella Hassanien, and Ahmed Hamad. Cascade multimodal biometric system using fingerprint and iris patterns. In *International conference on advanced intelligent systems and informatics*, pages 590–599. Springer, 2017.

[51] Jaspreet Kaur and Rajdeep Singh Sohal. Multi sensor based biometric system using image processing. *Research Journal of Engineering and Technology*, 8(1): 53–62, 2017.

[52] Rick S Blum and Zheng Liu. *Multi-sensor image fusion and its applications*. CRC press, 2005.

[53] Maneet Singh, Richa Singh, and Arun Ross. A comprehensive overview of biometric fusion. *Information Fusion*, 52:187–205, 2019.

[54] Kehinde A Sotonwa and Oluwashina A Oyeniran. Feature extraction and classification technique for multi-algorithm facial recognition system. *International Journal of Latest Technology in Engineering, Management and Applied Science-IJLTEMAS*, 8(2):06–10, 2019.

[55] Ramadan Gad, Muhammad Talha, Ahmed A Abd El-Latif, M Zorkany, EL-SAYED Ayman, EL-Fishawy Nawal, and Ghulam Muhammad. Iris recognition using multi-algorithmic approaches for cognitive internet of things (ciot) framework. *Future Generation Computer Systems*, 89:178–191, 2018.

[56] Ashish Mishra. Multimodal biometrics it is: need for future systems. *International journal of computer applications*, 3(4):28–33, 2010.

[57] Qinqin Fan, Yaochu Jin, Weili Wang, and Xuefeng Yan. A performance-driven multi-algorithm selection strategy for energy consumption optimization of sea-rail intermodal transportation. *Swarm and evolutionary computation*, 44:1–17, 2019.

[58] Ulrich Scherhag, Christian Rathgeb, and Christoph Busch. Morph deterction from single face image: A multi-algorithm fusion approach. In *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications*, pages 6–12, 2018.

[59] Mohamed Elhoseny, Ahmed Elkhateb, Ahmed Sahlol, and Aboul Ella Hassanien. Multimodal biometric personal identification and verification. In *Advances in Soft*

Computing and Machine Learning in Image Processing, pages 249–276. Springer, 2018.

[60] Gaurav Goswami, Richa Singh, Mayank Vatsa, and Angshul Majumdar. Kernel group sparse representation based classifier for multimodal biometrics. In *2017 International Joint Conference on Neural Networks (IJCNN)*, pages 2894–2901. IEEE, 2017.

[61] Sandip Kumar Singh Modak and Vijay Kumar Jha. Multibiometric fusion strategy and its applications: A review. *Information Fusion*, 49:174–204, 2019.

[62] Timothy C Faltemier, Kevin W Bowyer, and Patrick J Flynn. Using multi-instance enrollment to improve performance of 3d face recognition. *Computer Vision and Image Understanding*, 112(2):114–125, 2008.

[63] Rzouga Haddada Lamia and Essoukri Ben Amara Najoua. Biometric authentication based on multi-instance fingerprint fusion in degraded context. In *2019 16th International Multi-Conference on Systems, Signals & Devices (SSD)*, pages 22–27. IEEE, 2019.

[64] Lu Leng, Ming Li, Cheonshik Kim, and Xue Bi. Dual-source discrimination power analysis for multi-instance contactless palmprint recognition. *Multimedia Tools and Applications*, 76(1):333–354, 2017.

[65] Morampudi Mahesh Kumar, Munaga VNK Prasad, and USN Raju. Bmiae: blockchain-based multi-instance iris authentication using additive elgamal homomorphic encryption. *IET Biometrics*, 9(4):165–177, 2020.

[66] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognition*, 78:242–251, 2018.

[67] Mauro Barni, Giulia Droandi, Riccardo Lazzeretti, and Tommaso Pignata. Semba: secure multi-biometric authentication. *IET Biometrics*, 8(6):411–421, 2019.

[68] Marta Gomez-Barrero, Emanuele Maiorana, Javier Galbally, Patrizio Campisi, and Julian Fierrez. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognition*, 67:149–163, 2017.

[69] Fan Yang, Michel Paindavoine, Herve Abdi, and Anthony Monopoli. Development of a fast panoramic face mosaicking and recognition system. *Optical Engineering*, 44(8):087005, 2005.

[70] Asem Othman and Arun Ross. On mixing fingerprints. *IEEE Transactions on Information Forensics and security*, 8(1):260–267, 2012.

[71] Yang Xin, Lingshuang Kong, Zhi Liu, Chunhua Wang, Hongliang Zhu, Mingcheng Gao, Chensu Zhao, and Xiaoke Xu. Multimodal feature-level fusion for biometrics identification system on iomt platform. *IEEE Access*, 6:21418–21426, 2018.

[72] D Jagadiswary and D Saraswady. Biometric authentication using fused multimodal biometric. *Procedia Computer Science*, 85:109–116, 2016.

[73] B Prasanalakshmi, A Kannammal, and R Sridevi. Multimodal biometric cryptosystem involving face, fingerprint and palm vein. *International Journal of Computer Science Issues (IJCSI)*, 8(4):604, 2011.

[74] Mingxing He, Shi-Jinn Horng, Pingzhi Fan, Ray-Shine Run, Rong-Jian Chen, Jui-Lin Lai, Muhammad Khurram Khan, and Kevin Octavius Sentosa. Performance evaluation of score level fusion in multimodal biometric systems. *Pattern Recognition*, 43(5):1789–1800, 2010.

[75] Mustafa Berkay Yılmaz and Berrin Yanıkoğlu. Score level fusion of classifiers in off-line signature verification. *Information Fusion*, 32:109–119, 2016.

[76] Waziha Kabir, M Omair Ahmad, and MNS Swamy. Normalization and weighting techniques based on genuine-impostor score fusion in multi-biometric systems. *IEEE Transactions on Information Forensics and Security*, 13(8):1989–2000, 2018.

[77] Ajay Kumar and Sumit Shekhar. Personal identification using multibiometrics rank-level fusion. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 41(5):743–752, 2010.

[78] Md Maruf Monwar and Marina L Gavrilova. Multimodal biometric system using rank-level fusion approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 39(4):867–878, 2009.

[79] Bihan Jiang, Brais Martinez, Michel F Valstar, and Maja Pantic. Decision level fusion of domain specific regions for facial action recognition. In *2014 22nd international conference on pattern recognition*, pages 1776–1781. IEEE, 2014.

[80] Gang Niu, Achmad Widodo, Jong-Duk Son, Bo-Suk Yang, Don-Ha Hwang, and Dong-Sik Kang. Decision-level fusion based on wavelet decomposition for induction motor fault diagnosis using transient current signal. *Expert Systems with Applications*, 35(3):918–928, 2008.

[81] Jing Li, Tao Qiu, Chang Wen, Kai Xie, and Fang-Qing Wen. Robust face recognition using the deep c2d-cnn model based on decision-level fusion. *Sensors*, 18 (7):2080, 2018.

[82] Aniruddha Ghosh, Richa Sharma, and PK Joshi. Random forest classification of urban landscape using landsat archive and ancillary data: Combining seasonal maps with decision level fusion. *Applied Geography*, 48:31–41, 2014.

[83] Luis O Jimenez, Anibal Morales-Morell, and Antonio Creus. Classification of hyperdimensional data based on feature and decision fusion approaches using projection pursuit, majority voting, and neural networks. *IEEE Transactions on Geoscience and Remote Sensing*, 37(3):1360–1366, 1999.

[84] Chris Roberts. Biometric attack vectors and defences. *Computers & Security*, 26 (1):14–25, 2007.

[85] R Blanco Gonzalo, Barbara Corsetti, Ines Goicoechea-Telleria, Anas Husseis, Judith Liu-Jimenez, Raul Sanchez-Reillo, Teodors Eglitis, Elakkiya Ellavarason, Richard Guest, Chiara Lunerti, et al. Attacking a smartphone biometric fingerprint system: A novice's approach. In *2018 International Carnahan Conference on Security Technology (ICCST)*, pages 1–5. IEEE, 2018.

[86] Ulrich Scherhag, Andreas Nautsch, Christian Rathgeb, Marta Gomez-Barrero, Raymond NJ Veldhuis, Luuk Spreeuwers, Maikel Schils, Davide Maltoni, Patrick Grother, Sebastien Marcel, et al. Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–7. IEEE, 2017.

[87] Anil K Jain, Arun Ross, and Umut Uludag. Biometric template security: Challenges and solutions. In *2005 13th European signal processing conference*, pages 1–4. IEEE, 2005.

[88] Xuebing Zhou, Stephen D Wolthusen, Christoph Busch, and Arjan Kuijper. Feature correlation attack on biometric privacy protection schemes. In *2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 1061–1065. IEEE, 2009.

[89] Yujia Liu, Seyed-Mohsen Moosavi-Dezfooli, and Pascal Frossard. A geometry-inspired decision-based attack. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 4890–4898, 2019.

[90] Devendra Reddy Rachapalli and Hemantha Kumar Kalluri. A survey on biometrie template protection using cancelable biometric scheme. In *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pages 1–4. IEEE, 2017.

[91] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP Journal on advances in signal processing*, 2008:1–17, 2008.

[92] George I Davida, Yair Frankel, and Brian J Matt. On enabling secure applications through off-line biometric identification. In *Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No. 98CB36186)*, pages 148–157. IEEE, 1998.

[93] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29(4):561–572, 2007.

[94] Ruud M Bolle, Jonathan H Connell, and Nalini K Ratha. Biometric perils and patches. *Pattern recognition*, 35(12):2727–2738, 2002.

[95] Ari Juels and Madhu Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006.

[96] Yagiz Sutcu, Qiming Li, and Nasir Memon. Protecting biometric templates with sketch: Theory and practice. *IEEE Transactions on Information Forensics and Security*, 2(3):503–512, 2007.

[97] Arpita Sarkar and Binod K Singh. A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, 79(37):27721–27776, 2020.

[98] RK Bharathi and SD Mohana. A review on biometric template security. In *Emerging Research in Electronics, Computer Science and Technology*, pages 589–596. Springer, 2019.

[99] Christian Rathgeb and Andreas Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1):3, 2011.

[100] Mulagala Sandhya and Munaga VNK Prasad. Biometric template protection: A systematic literature review of approaches and modalities. In *Biometric Security and Privacy*, pages 323–370. Springer, 2017.

[101] Yagiz Sutcu, Qiming Li, and Nasir Memon. Secure biometric templates from fingerprint-face features. In *2007 IEEE Conference on computer vision and pattern recognition*, pages 1–6. IEEE, 2007.

[102] Karthik Nandakumar and Anil K Jain. Multibiometric template security using fuzzy vault. In *2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems*, pages 1–6. IEEE, 2008.

[103] Eren Camlikaya, Alisher Kholmatov, and Berrin Yanikoglu. Multi-biometric templates using fingerprint and voice. In *Biometric technology for human identification V*, volume 6944, page 69440I. International Society for Optics and Photonics, 2008.

[104] Bo Fu, Simon X Yang, Jianping Li, and Dekun Hu. Multibiometric cryptosystem: Model structure and performance analysis. *IEEE Transactions on information forensics and security*, 4(4):867–882, 2009.

[105] Cai Li, Jiankun Hu, Josef Pieprzyk, and Willy Susilo. A new biocryptosystem-oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion. *IEEE transactions on Information Forensics and Security*, 10(6):1193–1206, 2015.

[106] Amioy Kumar and Ajay Kumar. A cell-array-based multibiometric cryptosystem. *IEEE access*, 4:15–25, 2015.

[107] Lin You and Ting Wang. A novel fuzzy vault scheme based on fingerprint and finger vein feature fusion. *Soft Computing*, 23(11):3843–3851, 2019.

[108] Donghoon Chang, Surabhi Garg, Mohona Ghosh, and Munawar Hasan. Biofuse: A framework for multi-biometric fusion on biocryptosystem level. *Information Sciences*, 546:481–511, 2021.

[109] L Nisha Evangelin and A Lenin Fred. Securing recognized multimodal biometric images using cryptographic model. *Multimedia Tools and Applications*, pages 1–18, 2021.

[110] Rajesh Asthana, Gurjit Singh Walia, and Anjana Gupta. A novel biometric crypto system based on cryptographic key binding with user biometrics. *Multimedia Systems*, pages 1–15, 2021.

[111] Ann Cavoukian, Alex Stoianov, et al. Biometric encryption chapter from the encyclopedia of biometrics. *Office of the Information and Privacy Commissioner*, 2009.

[112] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K Jain. Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 92(6):948–960, 2004.

[113] Aftab Ali and Farrukh Aslam Khan. A broadcast-based key agreement scheme using set reconciliation for wireless body area networks. *Journal of medical systems*, 38(5):1–12, 2014.

[114] Padma Polash Paul and Marina Gavrilova. Multimodal cancelable biometrics. In *2012 IEEE 11th international conference on cognitive informatics and cognitive computing*, pages 43–49. IEEE, 2012.

[115] Padma Polash Paul and Marina Gavrilova. Novel multimodal template generation algorithm. In *2013 IEEE 12th International Conference on Cognitive Informatics and Cognitive Computing*, pages 76–82. IEEE, 2013.

[116] Yong Jian Chin, Thian Song Ong, Andrew Beng Jin Teoh, and KOM Goh. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion*, 18:161–174, 2014.

[117] Padma Polash Paul and Marina Gavrilova. Rank level fusion of multimodal cancelable biometrics. In *2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, pages 80–87. IEEE, 2014.

[118] Harkeerat Kaur and Pritee Khanna. Random distance method for generating unimodal and multimodal cancelable biometric features. *IEEE Transactions on Information Forensics and Security*, 14(3):709–719, 2018.

[119] Marta Gomez-Barrero, Christian Rathgeb, Guoqiang Li, Raghavendra Ramachandra, Javier Galbally, and Christoph Busch. Multi-biometric template protection based on bloom filters. *Information Fusion*, 42:37–50, 2018.

[120] Rudresh Dwivedi and Somnath Dey. Score-level fusion for cancelable multibiometric verification. *Pattern Recognition Letters*, 126:58–67, 2019.

[121] Gurjit Singh Walia, Kartik Aggarwal, Kuldeep Singh, and Kunwar Singh. Design and analysis of adaptive graph based cancelable multi-biometrics approach. *IEEE Transactions on Dependable and Secure Computing*, 2020.

[122] Donghoon Chang, Surabhi Garg, Munawar Hasan, and Sweta Mishra. Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption. *IEEE Transactions on Information Forensics and Security*, 15:3152–3167, 2020.

[123] D. Gabor. Theory of communication. *IEE Journal of Radio and Communication Engineering*, 93(26), 1946.

[124] D. H. Granlund. In search of a general picture processing operator. *Computer Graphics and Image Processing*, 8, 1978.

[125] D. J. Field. Relations between the statistics of natural images and the response properties of cortical cells. *IEE Journal of Radio and Communication Engineering*, 4(12), 1987.

[126] J. G. Daugman. Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters. *Journal of Optical Society of America*, 2(7), 1985.

[127] B. S. Manjunath, P. Wu, S. Newsam, and H. D. Shin. A texture descriptor for browsing and similarity retrieval. *Elsevier, Signal Processing: Image Communication*, 16(1), 2000.

[128] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.

[129] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*, 25:1097–1105, 2012.

[130] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014.

[131] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.

[132] Christian Szegedy, Sergey Ioffe, Vincent Vanhoucke, and Alexander A Alemi. Inception-v4, inception-resnet and the impact of residual connections on learning. In *Thirty-first AAAI conference on artificial intelligence*, 2017.

[133] Dami Choi, Christopher J Shallue, Zachary Nado, Jaehoon Lee, Chris J Maddison, and George E Dahl. On empirical comparisons of optimizers for deep learning. *arXiv preprint arXiv:1910.05446*, 2019.

[134] Matthew D Zeiler and Rob Fergus. Visualizing and understanding convolutional networks. In *European conference on computer vision*, pages 818–833. Springer, 2014.

[135] William B Johnson and Joram Lindenstrauss. Extensions of lipschitz mappings into a hilbert space 26. *Contemporary mathematics*, 26, 1984.

[136] Amos Tversky. Features of similarity. *Psychological review*, 84(4):327, 1977.

[137] Sergio Schuler. *Theory and applications of the sine-Gabor wavelet frame.* University of Florida, 1997.