DEVELOPMENT OF EFFICIENT METHODS FOR BIOMETRIC CRYPTOSYSTEMS

A thesis submitted to

DELHI TECHNOLOGICAL UNIVERSITY

in partial fulfilment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

RAJESH KUMAR ASTHANA

under the supervision of

Prof. Anjana Gupta **&** **Dr. Gurjit Singh Walia**

DEPARTMENT OF APPLIED MATHEMATICS
DELHI TECHNOLOGICAL UNIVERISTY
DELHI-110042

December, 2021 **Enroll. No. : 2K16/Ph.D./AM/01**

DELHI TECHNOLOGICAL UNIVERISTY

CERTIFICATE

This is to certify that the thesis entitled "**Development of Efficient Methods for Biometric Cryptosystems**" being submitted by Rajesh Kumar Asthana (Reg. No.: 2K16/PhD/AM/01) for award of degree of Doctor of Philosophy, comprises his original research work under our supervision. The research work, to the best of our knowledge meets the requisite standard for submission of this thesis.

It is further certified that the work embodied in this thesis has neither partially nor fully submitted to any other university or institution for the award of any degree or diploma.

Prof. Anjana Gupta
Supervisor
Professor
Dept. of Applied Mathematics
Delhi Technological University

Dr. Gurjit Singh Walia
Supervisor
Scientist 'F'
Scientific Analysis Group
DRDO

Prof. S. Sivaprasad Kumar
Head of the Department
Dept. of Applied Mathematics
Delhi Technological University

Declaration of Authorship

I hereby declare that all information in the thesis entitled "**Development of Efficient Methods for Biometric Cryptosystems**" has been obtained and presented in accordance with the academic rules and ethical conducts as laid out by Delhi Technological University. I also declare that I have fully cited and referenced all materials and results that are not original to this work.

Date : **(Rajesh Kumar Asthana)**

Acknowledgements

First and foremost, thanks to the Almighty for giving me strength and inspiration to carry out this research work. I owe a deep sense of gratitude to all his comprehensive soul whose divine light has enlightened my path throughout the journey of my research.

I take this opportunity to express my heartfelt thanks to my research supervisor **Prof. Anjana Gupta** for her valuable guidance, enthusiastic encouragement and persistent support. I am truly grateful from the core of my heart for her meticulous approach, wonderful assistance of her perspective and fruitful discussions on the research topic. Her careful supervision and personal attention have given me a lot of confidence and enthusiasm, during the different stages of my doctoral investigations.

I place on record my heartfelt gratitude and sincere thanks to **Dr. Gurjit Singh Walia** who has been my supervisor, advisor and mentor. He is the one whose expertise in the field is widely acclaimed. I thank him for his valuable advice, constant support and revered guidance. I invariably fall short of words to express my sincere gratitude for his patience and motivation.

I lay my indebtedness to my current organisation where I am working, Scientific Analysis Group, Delhi, for exhibiting a faith in me and extending cooperation during the process of carrying out my research work along with my professional responsibilities in the organisation. I am thankful to the Director, SAG and all staff members of SAG, Delhi for their support during the entire period of my research.

I express my sincere gratitude to the Dean PG, Head of Applied Mathematics department, DTU faculty members, Admin staffs and others for their endless support and cooperation.

This work is dedicated to my family for their endless love, support, encouragement and blessings throughout my academics. My father, Late Shri Krishna Mohan Asthana raised and nurtured me for my education and intellectual development. My mother, Late Smt Urmila Asthana has always been a source of motivation and strength. I am indeed grateful to my wife Smt Rohita Asthana for her continuous support, care and motivation. I am also thankful to my sons, Master Arnav Asthana and Master Aarav Asthana for their immense cooperation as I could not spare sufficient time for them due to my very busy research work.

Rajesh Kumar Asthana

Dedicated to my parents

Late Shri Krishna Mohan Asthana

&

Late Smt. Urmila Asthana

Preface

Biometric systems make use of physical and behavioural characteristics of individuals for their authentication as these attributes are uniquely associated with them. For ensuring secrecy and authenticity of classified data, Cryptography is used wherein encryption and decryption of data is done using secret cryptographic keys. Thus, a major concern here is to maintain the confidentiality of secret key used for securing information. This issue can effectively be addressed by using Biometric Cryptosystems which combine biometrics and cryptography in order to utilize the best of both domains. Cryptography ensures higher level of security, whereas biometrics provides authentication and non-repudiation.

Several biometric cryptosystems based on different modalities have been proposed and developed in the past but these systems suffer from various problems. One major problem is related to unimodal biometric system in which a single biometric characteristic is used for authentication. In such systems, the noise which may creep in during data acquisition process, may lower down the performance of the system. Another issue is related to binding the secret key used in a cryptosystem to biometrics of the user. Third important challenge is protection of the biometric templates stored in the database because if these templates get compromised either through some deterministic method or brute force attack then the user would never be able to use that biometric feature in future.

In order to address these issues concerning various aspects of biometric cryptosystems, research work has been carried out and several methodologies have been developed. In order to resolve the first issue, a hybrid multimodal biometric

system which combines multimodal features using graph random walk based cross view diffusion, has been proposed. The inherent problem of biometric template protection has also been addressed by transforming each biometric feature value using some pre-defined key features.

In addition to this, a novel biometric cryptosystem has been proposed for securing the cryptographic key wherein a secret key is bound with biometric data of the user. New objective functions have been defined for creation of helper data by hiding the secret key. The helper data is subsequently used to retrieve the key.

To address the third major problem, an innovative scheme, the Random Area & Perimeter Method (RAPM)) has been proposed wherein biometric characteristics of an individual is transformed into random values that are stored as cancelable biometric templates.

Thus, by developing these innovative techniques and methods, all major issues have been addressed for an efficient biometric cryptosystem. The thesis incorporates the developed methodologies, their performance analysis and security analysis along with future directions.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the present era of technological advancement, many web-based services and their decentralization require identity management systems on a large scale. The smooth functionality of such systems in different applications viz., remote financial transactions, boarding flights/trains, granting access to nuclear facilities, sharing networked computer resources etc., rely on proper authentication of genuine users. The objective in identity management system is verification of individual's identity in order to prevent imposters from accessing protected resources [1]. Earlier, authentication of individuals was usually done by conventional knowledge-based (e.g., passwords) and token-based (e.g., ID cards) methods. There are many issues with both these methods as passwords/tokens can easily be lost, shared, manipulated or stolen thereby compromising the intended security. Biometric characteristics of an individual is unique in nature and therefore have been found effective and efficient to replace traditional methods for authentication [2]. It has become a quite favourite field of research all across the globe.

Biometric identification using a single biometric trait may be fast and easy to implement but there are so many challenges in enrolling a large population using a single biometric. Multimodal biometric system may overcome these limitations. In multimodal systems, input data are taken from single or multiple sensors by applying

them on multiple biometric characteristics. A major challenge arises here is that how to do optimal fusion of two or more biometric modalities.

The quantum of information that is being exchanged across the Internet, and sensitive nature of such data requires effective computer security. Thus, Cryptography which deals with various aspects of information security, has become a hot topic of research and development. The security provided by cipher systems mainly depends on the secrecy of the secret key. As the secret key is of large size, it is very difficult to remember and therefore, such keys are encrypted using a small password and stored on a computer's hard drive. Biometrics are used for binding with a secret key or to generate a secret key. This technique addresses all above mentioned issues. Majority of Biometric Cryptosystems (BCS) requires storage of biometric dependent public information referred to as helper data, to retrieve or generate keys [3]. Based on the way helper data is derived and used, Biometric Cryptosystems are classified as key-binding or key-generation systems.

A major concern in using a biometric system is how secure the biometric template of a user is as this insecurity among the users inhibits wide spread usage of the system. Therefore, mechanism for protection of biometric template must be developed in order to make a robust and efficient biometric authentication system.

1.1 Research Gaps in Biometric Cryptosystems

Biometric cryptosystems have to confront many challenges with regard to biometric data acquisition, user's interaction with the sensors and variation in the biometrics

[4]. During data acquisition process, lot of noise may creep in and corrupt the biometric data. Most of the methods developed so far, do not consider fusion of complementary information from multiple modalities along with protection of biometric templates. Apart from performance, security of biometric data is also a great concern. In addition, optimal fusion schemes are required to cater the effects of context sensitive environment. There is lot of scope to use multiple number of biometrics in developing a biometric cryptosystem as only few biometric characteristics have been used so far. Feature vectors from these multiple biometrics can be fused to enhance the security provided by the biometric cryptosystem.

Biometric cryptosystems generating cryptographic keys directly from biometric characteristics of the user face a serious problem as the Encryption and decryption operations are very sensitive and cannot tolerate even a single bit change in the cryptographic key which is practically very difficult to achieve. A major concern here is that if these features do not have enough entropy, then it will affect discriminating capability of the system and it may have higher false acceptance rate. One more point of concern is information leakage of stored helper data.

Another major challenge is to design biometric systems that generate non-linkable templates and provide a good trade-off between accuracy & security. In many applications, secret keys which are used in a cryptosystem are also encrypted and stored using a poorly selected user passwords that can either be guessed or obtained through brute force attacks. Apparently, this may lead to compromise of the sensitive data that is intended to be protected. Besides, so many attacks on Biometric Cryptosystems have also been proposed. Security of biometric template protection is a major issue in the sense that transformation functions and alignment of biometric

templates should be optimized in such a manner that it does not affect the accuracy of the system. Further investigations are required to be done on Cancelable Biometrics.

1.2 Research Problem

Biometric Cryptosystems and Cancelable Biometrics increases security and privacy offered by the systems while achieving high recognition rates. The domain of research problems for biometric based security has been shown in Figure 1.1. Various aspects of biometric based security that needed attention are : (i) robustness of biometric systems through consideration of multimodal authentication (ii) combining cryptography with biometrics for key binding and (iii) protection of biometric templates. The aim of the research study was to devise innovative solutions for these problems.

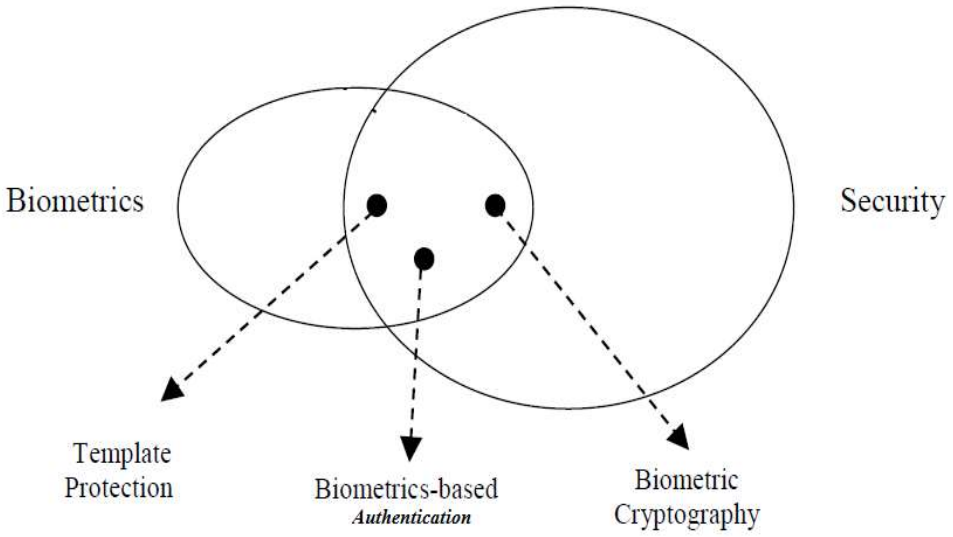


Figure 1.1: Domain of the research work

The research work was focused on the development of robust, reliable and biometric based security system. The questions, which were attempted to answer in this work, are as follow:

a) Which are the potential biometric characteristics that can be optimally fused to make a robust multimodal biometric authentication system ?

b) How score level fusion can be applied to develop an optimal multimodal biometric cryptosystems ?

c) How cryptography can be embedded into biometric framework for binding secret keys ?

d) How biometric template can be protected against various attacks ?

The proposed work was focused around these questions whose answers were explored during this research work. The details of various objectives of research are listed in the next section.

1.3 Research Motivation

Addressing the issue of identifying and authenticating people have always been difficult to achieve. Developing a system for this task requires enormous efforts and people generally fail to realize that unlike human's recognition mechanism which can easily verify individuals, the biometric systems are quite complex and many factors play their crucial roles. All over the world, biometric cryptosystems are being given

prominence for many important activities like securing classified data, banking, passport etc. But, so far biometric systems have not been used to its full potential due to apprehensions of the people that their biometric data may be compromised forever if the database which store their biometric templates somehow fall into the hands of inappropriate people. This trust deficit has severely hampered the widespread usage of the biometric systems. Other critical parameters that include robustness, consistency, universality, acceptability and efficiency in terms of false acceptance rate, false rejection rate etc., inhibit applications of biometric systems on a large scale.

Biometric systems are the need of the hour and people are hoping that science and technology would be able to remove those bottlenecks and apprehensions in the coming time. Therefore, researchers and scientists all over the world are putting their best efforts for overcoming the technical challenges and meeting expectations of the people. There are many research opportunities in the area of multimodal biometric cancelable biometrics and biometric cryptosystems.

1.4 Objectives

The objectives of this research work were to develop techniques and methods to address key questions in the study of biometric based Security. These specific objectives are summarized as follows:

Objective 1 :

To study various state of the art biometric techniques, datasets and performance metrics for biometric cryptosystems.

Objective 2 :

To design and develop an optimal multi-modal biometric authentication system with score level fusion and to make a comparative analysis with the existing systems.

Objective 3 :

To design and develop an efficient key binding scheme for biometric cryptosystems and to perform its randomness analysis using statistical tests.

Objective 4 :

To design and develop a robust biometric template protection scheme for biometric cryptosystems and to compare its performance with prominent schemes.

1.5 Thesis Outline

The aim of this research is to propose robust, reliable and efficient methods for biometric crypto systems. For accomplishing the research objectives, the methodology adopted for each objective and its implementation details have been organized into five chapters.

Chapter 1 gives a broad overview of the biometric based cryptosystems. In this chapter, research gaps and specific objectives of the research work have been described.

In Chapter 2 details of various components of biometric cryptosystems viz., biometric techniques, performance metrics and fusion methods for multi-modal biometrics have been given. Design parameters of a biometric system have also been dealt with in this chapter.

In Chapter 3, a novel Multimodal Biometric Authentication System has been proposed which combines multiple modalities and optimal score level fusion. Performance analysis has been carried out which demonstrates effectiveness of this scheme over many state-of-the-art multimodal fusion schemes.

In Chapter 4, Key binding approach has been discussed for the development of Biometric Cryptosystem. In this technique, binding of secret keys with the biometric data of the user is done in order to protect from an adversary. For this, helper data is created which helps in retrieving the secret key whenever required. Exhaustive experimentation has been carried out which shows that this biometric cryptosystem is quite efficient and only genuine user can get the secret key.

Chapter 5 brings out an innovative idea for biometric template protection. In this novel scheme for generating cancelable biometrics, area and perimeter of the curve obtained using biometric data and user-specific key data. These areas and perimeters are random values which cannot be exploited to get the original biometric data of the user. Performace and security analysis of the proposed method shows that this mechanism is quite effective in protecting biometric templates.

Apart from these, the conclusions of the research work and directions to future work have also been discussed in the Chapter 6.

1.6 Significant Contributions

A multimodal biometric system based on the combination of multiple modalities and optimal score level fusion has been developed. Experimental results demonstrate that optimal score fusion applied on cross-diffused features produce better results than existing state-of-the-art multimodal fusion schemes. EER and accuracy achieved using proposed method on four benchmarked datasets are 2.32 and 98.316 %. Techniques for data level fusion, score level fusion and decision level fusion, have been proposed for an efficient biometric system. A novel scheme for score level fusion is proposed in which multi modalities have been considered for an optimal biometric authentication system. The scheme using score level fusion out performs several state-of-the-art techniques.

A new biometric crypto system involving key binding mechanism has been proposed in which new objective functions have been introduced to create helper data by binding the secret key. Performance evaluation shows that the proposed method achieves more than 98% success rate even in presence of limited noise in the biometric data. The performance of the system does not get affected with change of length of secret key and upto a certain amount of noise induction in the user biometric data. The proposed method consistently achieves good success rate even with some changes in the neighborhood threshold values and some amount of randomization in the input values to the objective function. Proposed key binding method ensures that the secret key can be retrieved successfully by the genuine user

whereas the imposter is unable to get the secret key which was bound with the biometrics of the authorized user.

A novel scheme, the Random Area & Perimeter Method (RAPM), has been designed in which a biometric characteristic of an individual is transformed into random values which are stored as cancelable biometric templates. The proposed scheme computes area and perimeter of the Bezier curve which are obtained through interpolation of feature points of original biometrics and a random point chosen by the user. The scheme has been evaluated using various performance evaluation metrics like EER, DI, RI, ROC curve and CMC curve on the benchmark data sets. The average values obtained for EER, DI and RI are 0.0045, 6.28 and 99.64 respectively. Moreover, a dimensionality reduction to the tune of more than 95% has been obtained without compromising the matching performance.

Chapter 2

Review of Biometric Systems

Biometrics is one of the fastest growing cutting-edge technology for personal authentication as it offers enhanced security by addressing some weak spots in the present digital world. According to Juniper Research, biometrics will be used for over 20 billion transactions by 2025, a number that is exploding largely due to the increased security provided by biometric authentication technologies. Enabled with biometric authentication mechanism, people have more trust that their information is secure and organization can better protect their ecosystems from cybercriminals, malware, and bots. Establishing trust and improving user experience, all while focusing on optimal security, is essential for any organization today, and the latest biometric authentication technologies provide those benefits.

Personal authentication can be done on the basis of :

- What the user has, for example a key
- What the user knows, for example a password
- Where the user is, for example IP-address
- What the user is: biometrics methods

In various security applications above, private information is required for authentication of the genuine user. In the present technologically advanced world,

this private information is captured from physical or behavioural characteristics of the user. Biometric based authentication has many advantages over password-based or token-based authentication.

Cryptography plays a significant role in ensuring data security and confidentiality. The security provided by a crypto system mainly depends on the secrecy of the cryptographic key. If the secret key gets compromised, then it may lead to compromise of the protected data. Biometric cryptosystem provides a solution for securing the cryptographic key by binding the secret key with user biometric data. Protection of data has been recently investigated extensively due to proliferation of digital communication. Key binding based crypto systems have emerged as promising solution due to ease of usage and its adaptability. The scientific community all over the world have proposed various key binding mechanisms to secure the key from unauthorized persons by using user biometrics.

In this chapter, an overview of different aspects of biometric cryptosystems viz., various biometric techniques, standard datasets, performance metrics and fusion methods for different modalities have been discussed.

2.1 Biometric Systems : Design Aspects

Biometric system is a system that rely on measurable physiological or behavioral characteristics for verification and identification of an individual. Architecture of a biometric system is shown in Figure 2.1.

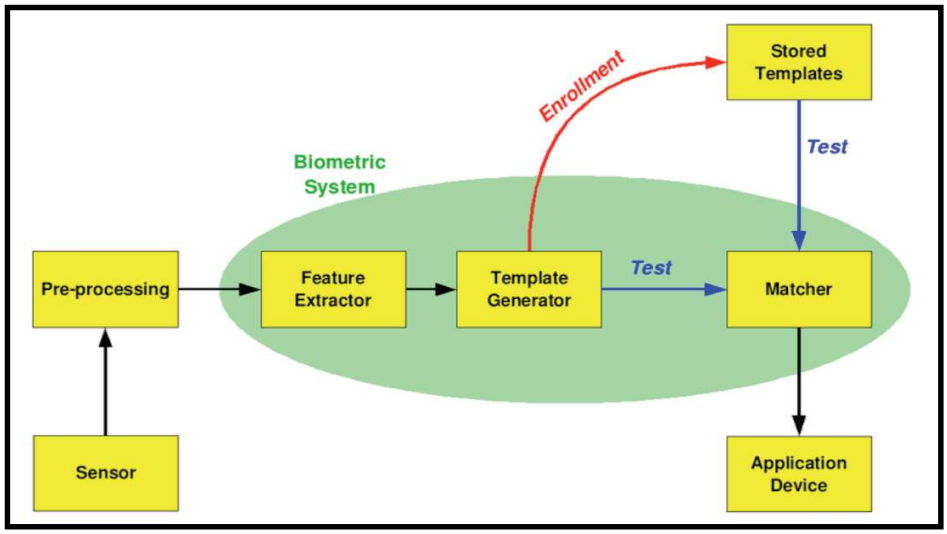


Figure 2.1 : Architecture of Biometric System

[Source : Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2]

A biometric system has following basic components [5]:

- **Biometric Sensor**: It performs analog to digital conversion during data acquisition process and provides raw biometric data.

- **Feature Extraction**: The raw biometric data is then processed and features are extracted. The extracted features should have good discriminability characteristics for every user.

- **Database**: At the time of enrolment, biometric templates are stored and a database is created. These templates are used to compare the input sample of an individual during authentication.

- **Matcher**: A matcher is an algorithm or method to compare the input data with the biometric templates stored in the database.

Biometric authentication module uses the biometric trait in two stages enrollment and authentication. During enrollment, the biometric data is captured and processed to generate biometric templates which are stored in the database. In contrast, the authentication process involves identification or verification of the query against the enrolled templates.

A biometric system operates in two modes, namely "verification" and "identification". While verification calls for one to one matching, Identification process essentially matches input queries against all the enrolled templates viz one to many matchings [6]. Each biometric technology has its strengths as well as limitations.

2.2 Issues and Challenges in Designing a Biometric System

There are several issues and challenges in designing a biometric system which is accurate, secure and convenient to use. Some of the prominent issues are as follow [7]:

- **Effect of Biometrics on System Performance**: Biometric characteristics in many cases affect the performance of a biometric system. For example, samples from identical twins may deceive a biometric recognition system. Similarly, people often make simple signatures which can be forged and it becomes very difficult for a signature-based biometrics system to verify a user correctly.

- **Non-privacy of Biometrics**: Another issue is that unlike knowledge-based and possession-based mechanisms which are replaceable, Biometrics are non-

replaceable and are absolutely private. So, its privacy must be preserved in the backdrop of invention of so many gadgets and software tools, which can be misused for recording and copying without the knowledge of the user.

- **Robustness of a Biometric System**: Most of the biometric systems are tested in the controlled environments of the laboratory and fail to give best performance in actual operating environments.

- **Need for 'Liveness' Detection in Capturing Devices**: Biometric system has to deal with the spoofing attack and forgery and it should have provisions for testing and reporting of skilled forgery detection.

- **Biometrics can be hacked**: Hackers have been able to infringe the security provided by a biometric system and have been able to access the biometric data of the user either at the time of registration or authentication. These stolen data subsequently may be misused.

2.3 Biometric Techniques

There are several biometric techniques based on different human attributes. Different biometric data are acquired using different apparatuses or sensors [8]. It should be noted that choice of a biometric input affects various aspects including performance of the biometric system. Biometric characteristics can be classified as follows:

I. **Physiological Characteristics** : The characteristics which are dependent on physical construction of human body such as fingerprints, face, hand geometry or the iris are categorised as Physiological characteristics. In general, a person can hardly influence his physical characteristics and therefore, these characteristics do not change over time.

II. **Behavioural Characteristics** : The characteristics which are related to the behaviour of a person such as signature, voice or keystroke dynamics are known as Behavioural characteristics.

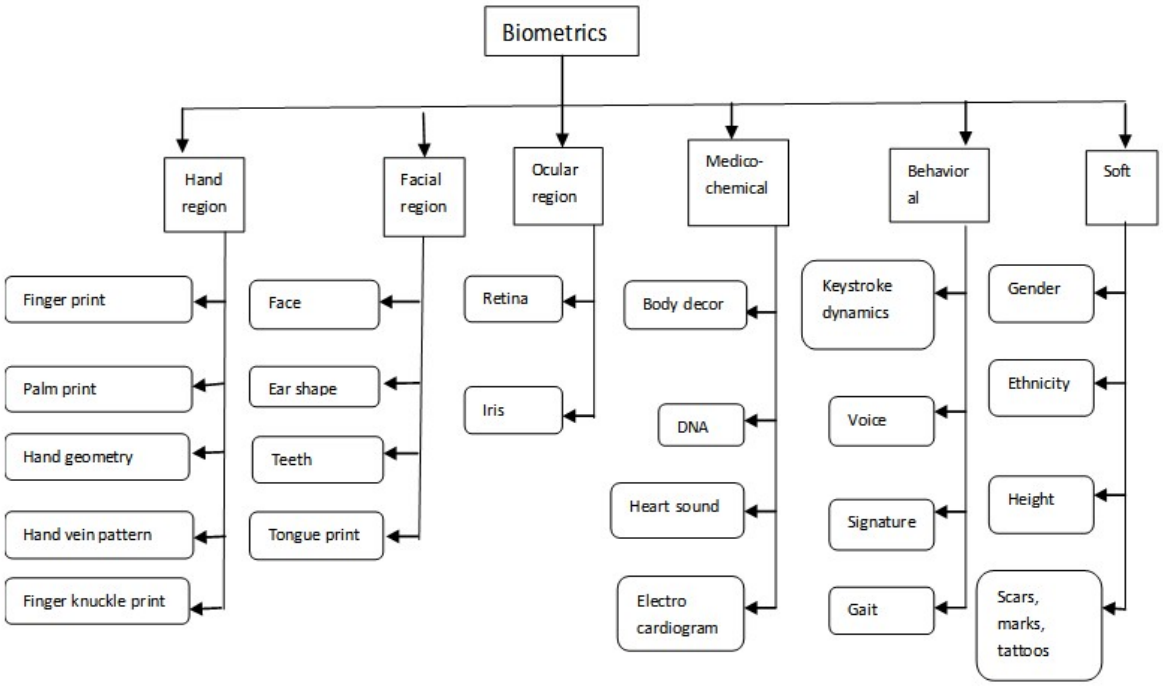


Figure 2.2 : Types of Biometrics

Some physiological and behavioural characteristics are outlined in the following subsections:

2.3.1 Fingerprint Identification

Fingerprints are unique patterns, made by friction ridges (raised) and furrows (recessed), which appear on the fingers and thumbs. Fingerprints remain unchanged during an individual's lifetime and no two finger prints in the entire world have ever been found to be identical [9]. Friction ridge patterns are grouped into three distinct types—loops, whorls and arches.

Loops – A loop is a pattern in which one or more ridges enter upon either side, recurve, touch or pass an imaginary line between delta and core and pass out or tend to pass out upon the same side the ridge entered.

Whorls – These are circular or spiral patterns, like tiny whirlpools. There could be four types of whorls: plain (concentric circles), central pocket loop (a loop with a whorl at the end), double loop (two loops that create an S-like pattern) and accidental loop (irregular shaped).

Arches – These are wave-like pattern and include plain arches and tented arches. Tented arches rise to a sharper point than plain arches.

(a) (b) (c)

Figure 2.3 : Fingerprint Patterns (a) Loops, (b) Whorls, (c)Arches

[Source : www.shutterstock.com/search/fingerprint]

Fingerprint matching techniques are of two types: minutiae-based and correlation based. Minutiae points also known as Galton points are unique features within the fingerprint pattern. They include dots, bifurcations, ending ridges, short ridges, enclosures, islands and abutting ridges.

2.3.2 Iris Recognition

Iris Recognition is based on physical features of the iris of an individual's eyes. Since iris is unique feature of an individual, it is considered to be ideal for authentication [10]. This technique is quite reliable method for identifying people accurately because iris is a very strong biometric and highly resistant to false matches.

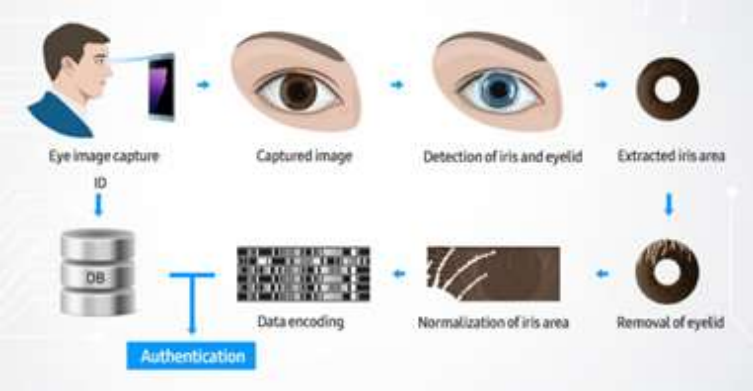


Figure 2.4 : Iris Recognition Process

[Source : https/news.samsung.com/galaxy-note7]

Some of the main advantages of this techniques are :

- **Accuracy** – It is one of the most accurate among all the biometric techniques for authentication.

- **Contactless** – As this technique is contactless, it is hygienic and less intrusive.

- **Flexible and Scalable** – This technique is quite flexible from the application point of view and it can be used at night or in the dark due to availability of infrared cameras.

- **Liveness Detection** – It is able to detect movement of the iris which identifies the liveness of the individual.

- **Fast Matching** – Iris Recognition technique has been found to be the fastest among all biometric techniques as far as matching with the enrolled database is considered.

Whilst there are numerous benefits of Iris Recognition, many issues, as listed below, still need to be addressed.

- **Distance** – Though this technique is contactless, there is limit to the maximum distance upto which iris scanner work efficiently. This limitation itself could be quite challenging in certain environments.

- **Movement** – If there is relative movement between the subject and the scanner, capturing of proper iris image could become difficult.

- **Reflection** – If the subject wears contact lenses and eyeglasses, the issue of reflection of light might crop up.

- **Cost** – In order to achieve higher accuracy, acquisition of high-quality biometric images is a major pre-requisite. For this, high end iris scanners, which are quite expensive, are required.

2.3.3 Retina Recognition

Retina Recognition technique targets the unique and complex patterns of blood vessels that exist in the retina. Patterns of blood vessels are easily identified in presence of appropriate light as it absorbs light more than the surrounding tissue. After capturing of such patterns, features are extracted using specialized methods and biometric templates are formed. The pattern of blood vessels does not change throughout the life of a person.

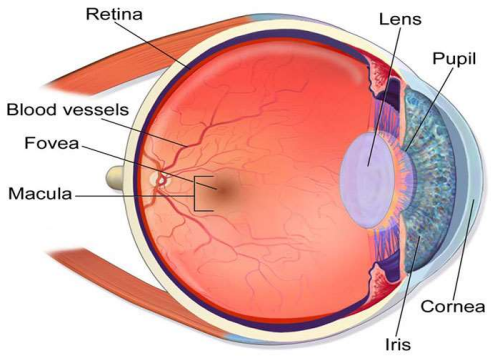


Figure 2.5 : Network of blood vessels in Retina

[Source : https://www.bayometric.com/retina-vs-face-biometric-modalities/]

Just like fingerprints and iris patterns, the network of blood vessels also does not get affected by genetic factors and hence is able to identify even identical twins. As the retina is an internal organ, it is less susceptible to intentional or unintentional modifications. High accuracy and difficulty in spoofing, makes this technique highly dependable for authentication. Due to its robust matching capabilities, this technique has been found to be way ahead for one-to-many identifications [11]. However, there are some issues like difficulty in image acquisition and limited user applications as a user may be falsely rejected because of incorrect data acquisition.

2.3.4 Face Recognition

Face recognition uses facial biometric pattern to verify the identity of a person. The facial attributes are easily captured using a photographic device. Artificial Intelligence (AI) and machine learning technologies have enabled face recognition systems to operate while maintaining high safety and reliability standards. Moreover, the identification and verification can be carried out in real time by integrating these methodologies and computing techniques [12]. This technique is also contactless as compared to some other techniques like Fingerprint matching. A major issue with this technique is that quality of captured images gets affected due to environmental conditions. There are several challenges to face recognition system viz., different illumination condition, different poses and orientations of images, other variational conditions, limited datasets for training etc.

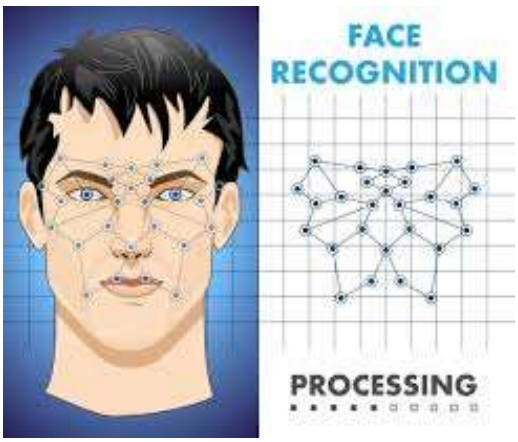


Figure 2.6 : Face Recognition

[Source : https://www.itperfection.com/network-security/biometric-authentication-methods-2fa-mfa-retina-iris-fingerprint-face-recognition-network-security-cybersecurity-authentication/]

2.3.5 Hand Geometry Recognition

Hand geometry biometrics is based on the structure of palm and fingers, including width of the fingers in different places, length of the fingers, thickness of the palm area, etc. Though these attributes do not have very strong discriminability features, still they can be used for identification and personal authentication in not so sensitive applications or situations where two factor authentication is done. Some non-descriptive characteristics can be combined to get better performance. The main advantages of this technique lie in its wide acceptability among people and requirement of a simple data processing. Though this technique is less intrusive than some other biometric techniques, but at the same time it is also less accurate since geometrical shape of the hand is not unique [13]. Generally, this technique has higher false acceptance & rejection rates due to which this method is not suitable as an identification method, but can be used as a verification method with an additional level of security. In 2002, thirty global features of hand geometry were defined which are shown in the following figure

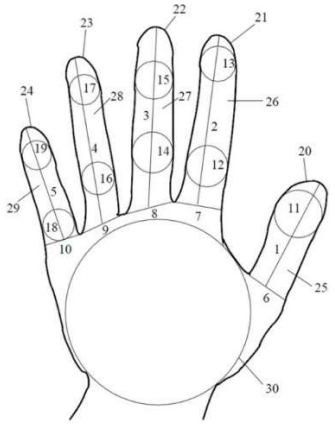


Figure 2.7 : Hand Geometry Features

[Source : https://www.intechopen.com/chapters/40073]

2.3.6 Palm Print Recognition

Palm prints are smooth patterns on the palm surface created by creases and troughs. There are three types of line patterns: principal lines, wrinkles, and ridges [14]. Principal lines are the longest, strongest and widest lines on the palm. Generally, three principal lines are found on the palm known as heart line, head line, and life line (Fig. 2.8). Wrinkles, the second type of line patterns, are comparatively thinner and more irregular. The pronounced wrinkles which are around the principal lines, can also play its role in distinguishing different palm prints. Ridges, the third type of line patterns are randomly distributed throughout the palm. This feature is very fine and hence are less useful for identification since it is very difficult to notice them under poor imaging source.

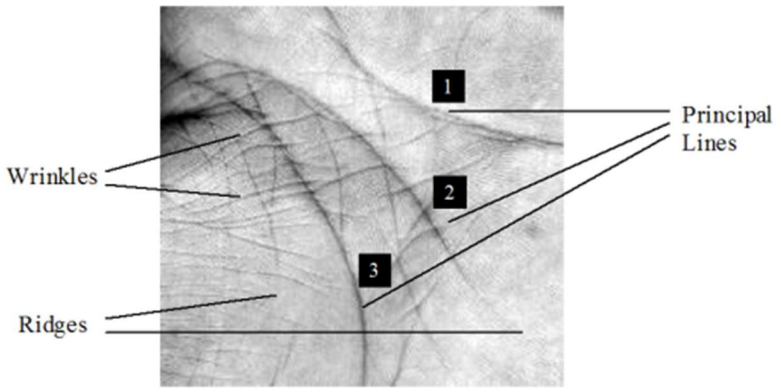


Figure 2.8 : Palm Print Features

[Source : https://www.intechopen.com/chapters/17745]

There are various approaches for extraction of palmprint features which can be categorised into: line-based, appearance-based, and texture-based approaches. On the basis of extracted features, different matching methodologies which are generally of two types namely, geometry-based matching, and feature-based matching are

used. In geometry-based matching, geometric features like points and line features are considered for comparison. In case of point features, distance metrics like Hausdorff distance give better result in comparing similarity while in case of line features, Euclidean distance performs better. In palm print, line features gives more information as compared to point features.

2.3.7 Hand Vein Recognition

The vascular patterns or blood vein patterns that exist underneath the human skin are known as Hand vein. These patterns are unique for every individual and does not change significantly especially after the age of 10 years. Not only these patterns are different for identical twins, even the left- and right-hand vein differ for any individual. It is almost impossible to copy or duplicate the vein patterns as they lie underneath the skin. Moreover, these patterns are not affected by the external factors like wet and dry hand surfaces, dirty and greasy surfaces and wear and tear. All these advantages make this biometric technique a good choice for personal identification and verification [15]. Samples of hand vein patterns are given in the Figure 2.9.

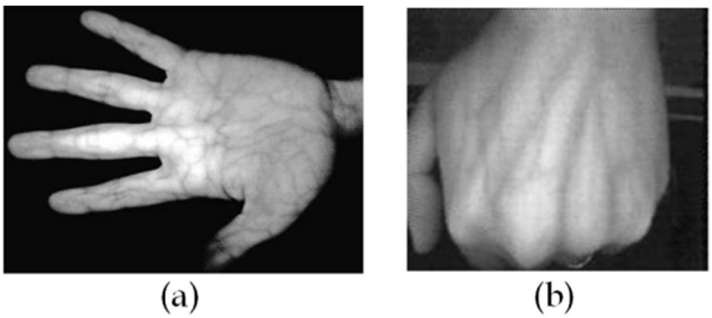


Figure 2.9 : Hand Vein Patterns

[Source : https://www.intechopen.com/chapters/17745]

These patterns are well captured using Far Infrared (FIR) imaging technology as they are not affected by poor illumination conditions. However, external factors like temperature and humidity have adverse effect on the captured biometric data.

2.3.8 DNA Matching

Deoxyribonucleic acid (DNA) of an individual is one of the most reliable biometric characteristics for personal identification as they are intrinsically digital and does not change during a person's life or even after his/her death. A major advantage of DNA is that it can be obtained from multiple biological sources like hair, nail, swab, body fluid etc. [16]. Other advantages of DNA based identity verification technology include its discriminability power, higher accuracy and internationally accepted standards for analysis. A major issue with DNA analysis is that it takes a lot of time for authentication as compared to other techniques.

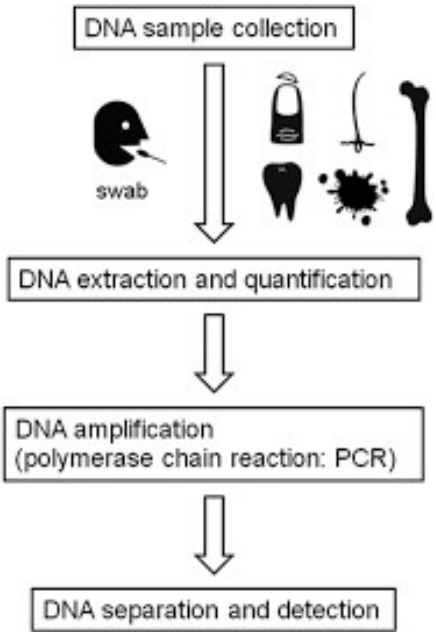


Figure 2.10 : DNA Identification

[Source : https://www.intechopen.com/chapters/16506]

2.3.9 Signature Dynamics

Signature dynamics technique focusses on how a signature is made i.e., its dynamics rather than simply comparing with the previously registered signatures. An imposter cannot get vital information about how the signature was actually made at the time of registration, by just looking at some previously written signatures [17]. Signature Dynamics technique include the following basic features :

- Size and shape of the signature
- Length and angle of lines, arcs and curves
- Period between strokes and duration of the signature
- Speed of individual stokes, acceleration and deceleration
- Number of loops in the signature

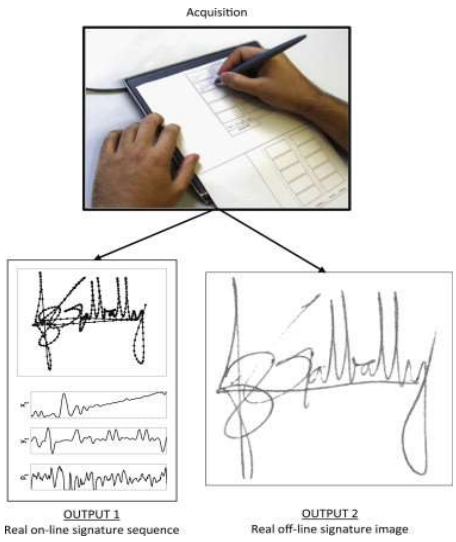


Figure 2.11 : Signature Dynamics

[Source : https/www.sciencedirect.com/science/article/S003132031500120X]

2.3.10 Speaker Verification

In speaker verification, identification/verification of a user is done by analyzing his voice characteristics. There is difference between Speaker verification and speech recognition as speech recognition focuses on what has actually been spoken while speaker verification aims to find who has spoken that [18]. Performance of this technique suffers from the background and network noise and also by the emotional state of the user.

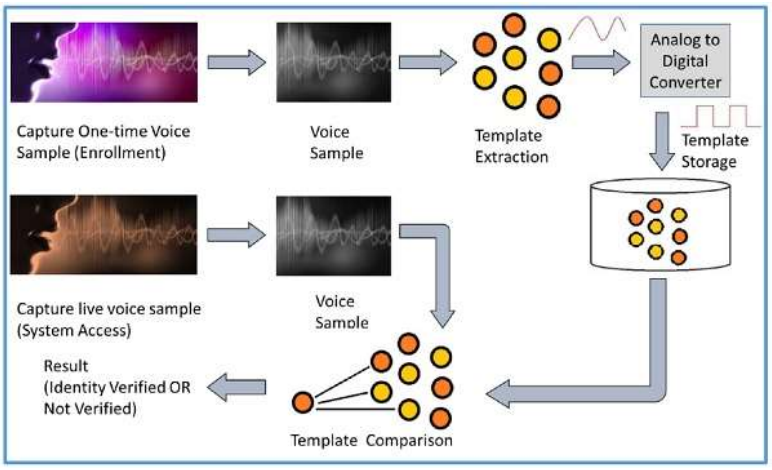


Figure 2.12 : Speaker Verification

[Source : https://www.tutorialspoint.com/biometrics/biometrics_quick_guide.htm]

2.3.11 Keystroke Dynamics

Keystrokes dynamics is quite similar in functioning to signature dynamics. In this technique, the pattern of typing on a keyboard by the user is analyzed. It measures how long a user holds a key, and how long it takes to the user to switch from one key to another. This behavioural aspect of every individual is more or less unique and so this technique offers a good authentication mechanism [19].

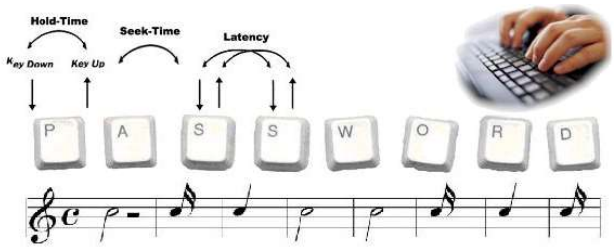


Figure 2.13 : Keystroke Dynamics

[Source : https://deepnetsecurity.com/authenticators/biometrics/typesense/]

2.4 Comparative Analysis of Biometric Techniques

Biometric systems are successfully being used in several real-life applications, but they are error prone as well. A system is required that authenticates persons accurately, reliably, rapidly, cost-effectively and user friendly. The biometric solutions mentioned in the previous section may be categorised and compared by several factors and indicators. Such a comparison as shown in Table 2.1 would provide directions when planning the deployment of a new system.

Table 2.1 : : Comparison between Biometric Techniques

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

H→High, M→Medium, L→Low

Despite rapid growth in biometric systems in the past few decades, a number of issues related to biometric traits, are yet to be resolved. Some of the issues are :

2.4.1 Hand Region Biometrics : Issues and Challenges

Hand region contains biometrics like finger print, palm print, hand geometry, hand vein pattern etc.. Main challenges in hand region biometrics are [20]:

- Images may be of poor quality, making it difficult for their usage in highly data-sensitive biometric system. Any inaccuracy or deficiency in the acquired data may lead to a lower performance of the biometric system.
- Some skin diseases like Psoriasis cause problems in fingerprint identification.
- There are examples of people having no fingerprint.
- Livelihood or enforcement has to be checked.
- Variations due to improper interaction with sensors.
- Palm print identification process is relatively slower.
- There are chances of exposer to infra-red radiations in case of hand vein pattern recognition.

2.4.2 Face Region Biometrics : Issues and Challenges

This region contains modalities such as Face, Facial Thermograph, Ear Shape and Tongue print etc.. Face region biometrics have major issues with regard to illumination, pose variation, facial expression, age effect, occlusion, makeup etc. [21].

Figure 2.14 : Illumination Problem in face region biometrics

[Source : https/what-when-how.com/face-recognition]

Figure 2.15 : Pose variation, Facial expressions and Age Effect

[Source : https://www.semanticscholar.org/paper/Face-Recognition-System-%E2%80%93-A-Survey-Richa-Josan/399f973a59493280db9686ebd9e7e218ce74a5bd/figure/1]

Figure 2.16 : Occlusion issue in face region biometrics

[Source : https://www.mdpi.com/2079-9292/9/8/1188/htm]

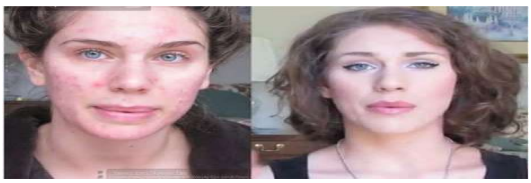


Figure 2.17 : Makeup factor in face region biometrics

[Source : https://spie.org/news/4795-makeup-challenges-automated-face-recognition-systems]

2.4.3 Ocular Region Biometrics : Issues and Challenges

The Ocular region contains modalities like Iris, Retina, Sclera and Vasculature. There are several issues with the ocular region biometrics as mentioned below [22]:

- It is difficult to scan from a larger distance.
- Infrared light may cause exposure to radiations.
- Effect of poor quality of lens on the retinal scanning device.
- Interference from external sources.
- Measurement accuracy may be affected by disease.
- Some eye disease may affect iris identification.

2.4.4 Medico-Chemical Region Biometrics : Issues and Challenges

This region contains modalities like body odour, DNA, heart sound and Electrocardiogram (ECG). Some of the issues related to these biometrics are as follows [23]:

- Intrusive data acquisition procedure
- Dependence over medical conditions
- Privacy issues
- Physical contact with sensors

2.4.5 Behavioral Biometrics : Issues and Challenges

Behavioural biometrics contain modalities like signature dynamics, keystroke dynamics, vocal characteristics and gait. The issues related to these biometrics are as under:

- They do not provide sufficient discriminatory information.
- Accuracy is severely affected by the background noise and health conditions of the subjects.
- Gait recognition suffers with high false rates due to walking conditions.

2.5 Criteria for Selection of Biometrics

Any physiological or behavioral feature is considered as biometric trait if it contains the following qualities.

- **Distinctness:** The biometric feature should be able to discriminate amongst the population.
- **Universality:** The biometric feature should be possessed by all humans.
- **Collectability:** Biometric features should be easy to acquire, pre-process and extract meaningful features.
- **Invariance:** Biometric characteristic should be invariant against time.
- **Acceptability:** People should be willing to submit their biometric data to the biometric system.
- **Difficulty to imitate:** Imitation should be difficult to avoid frauds.

2.6 Fusion of Biometric Modalities

Performance of single biometric modality based biometric system is adversely affected by noisy sensor data, unacceptable error rates and non-universality of the biometric. Generally, there is not much scope in improving the performance of the individual sensing device due to their inherent weaknesses. Multimodal biometric authentication resolves all these issues present in unimodal biometrics. Fusion of different modalities can be done at data level, feature level, decision level or score level.

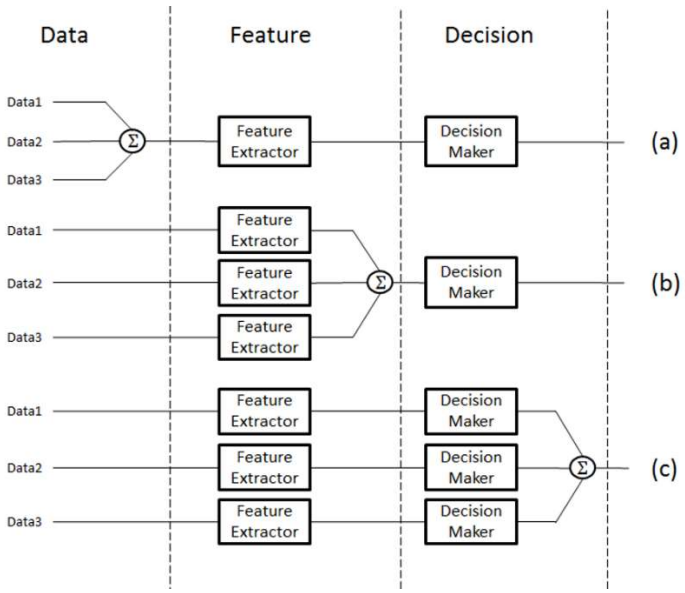


Figure 2.18 : Fusion Levels

2.6.1 Data Level Fusion

In this type of fusion, data acquired using multiple sensors from the same biometric characteristic are combined. These raw data are fused to generate new biometric data.

2.6.2 Feature Level Fusion

In Feature level fusion, feature sets from different biometrics are combined together to form a new feature set. Such concatenation of features may lead to a feature vector with a very high dimensionality which increases computational overhead.

2.6.3 Decision Level Fusion

In Decision level fusion, multiple matchers match the feature vectors with the templates and their decisions are fused together to reach the final decision by employing different techniques such as majority voting, decision table, Bayesian decision and Dempster- Shafer theory of evidence.

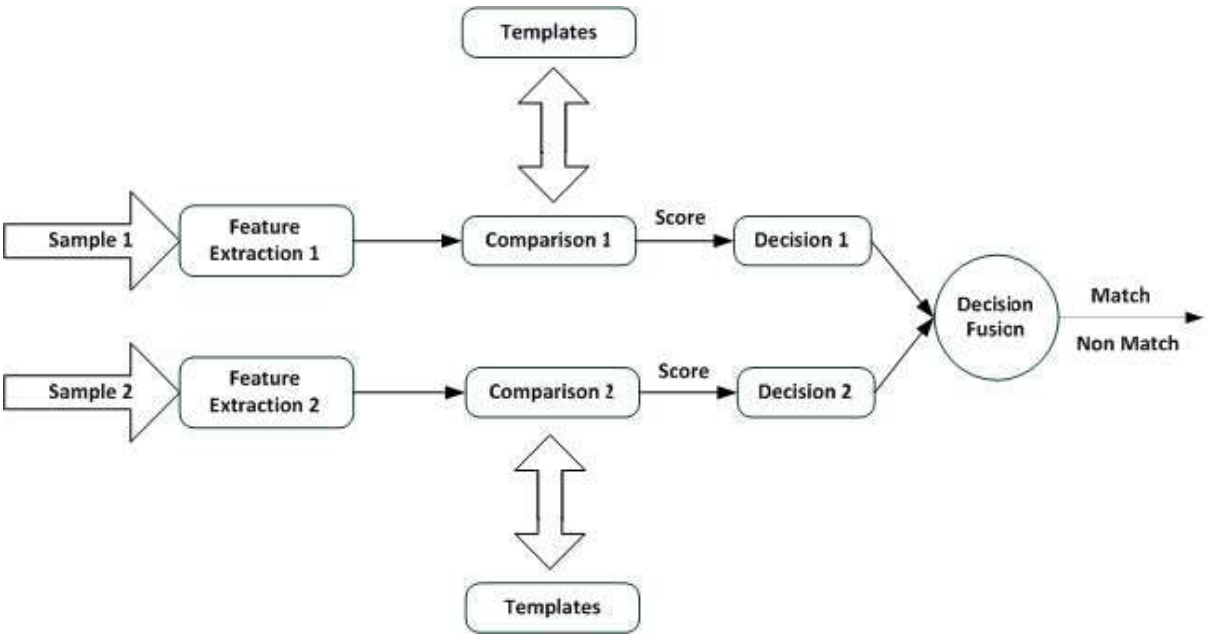


Figure 2.19 : Decision Level Fusion

2.6.4 Score Level Fusion

In this type of fusion, biometric features from different modalities are processed independently and matched with templates using different classifiers. The scores obtained from these classifiers are fused together and the decision module accepts or rejects the claimed identity based on the composite match score. The scores must be adjusted first i.e., normalization of score values must be done before arriving at a decision. Also, the similarity measures must be converted into distance measures. Threshold criteria for score selection needs to be decided. Score level fusion is less accurate in recognition in comparison to Feature level fusion.

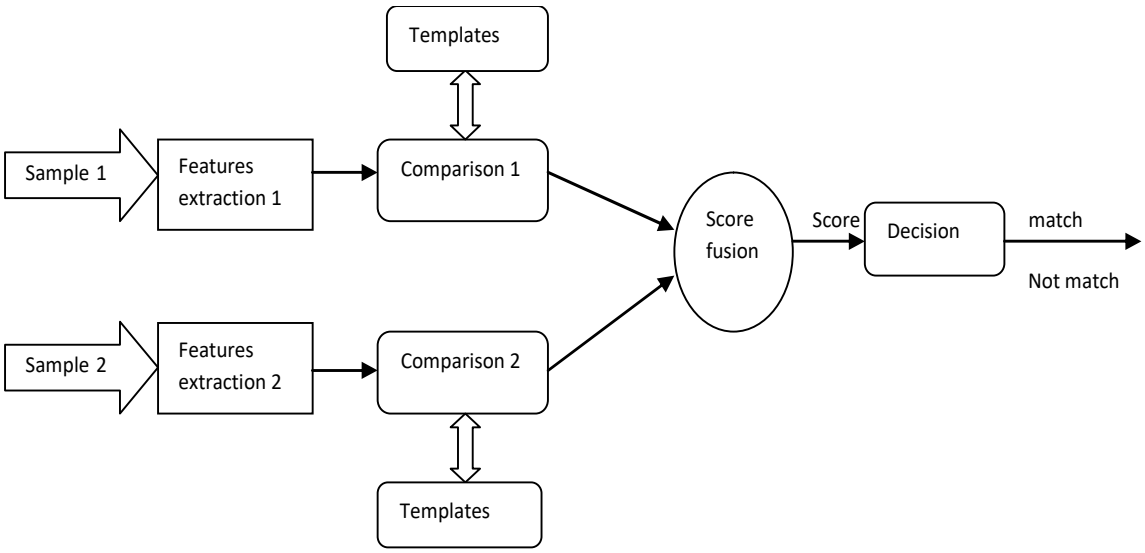


Figure 2.20 : Score Level Fusion

2.7 Performance Metrics

In order to assess performance of a biometric recognition system, following metrics are generally used while doing verification or identification [24], [25]:

2.7.1 False Acceptance Rate (FAR)

FAR is the measure of the error committed by the system when an unauthorized user is given access. If *NI* be the number of impostor patterns presented to a biometric system and *FA* be the number of cases when imposters are falsely accepted, then FAR is computed as

$$FAR = \frac{FA}{NI}$$

2.7.2 False Rejection Rate (FRR)

FRR is the measure of the error committed by the biometric system when a genuine user is denied access. If *FR* is the number of false rejects and NA is the number of authorized user patterns, then FRR is computed as

$$FRR = \frac{FR}{NA}$$

2.7.3 True Acceptance Rate (TAR)

This metric assesses the capability of the system in correctly matching the biometric data from the same individual. For any biometric systems this value should be high as far as possible. This rate is defined as

$$TAR = 1 - FRR$$

2.7.4 Weighted Error Rate (WER)

This metric is defined as the weighted sum between FNMR (FRR) and FMR (FAR).

2.7.5 Equal Error Rate (EER)

EER is the value when FAR and FRR are equal, and is represented as the point at which the plotted curves of FAR and FRR values intersect. EER is also termed as Cross-over error rate between FAR and FRR. This metric expresses the efficacy of the system in rejecting an impostor. If EER is close to zero, then performance of the system is maximum, indicating a clear separation between genuine and imposter.

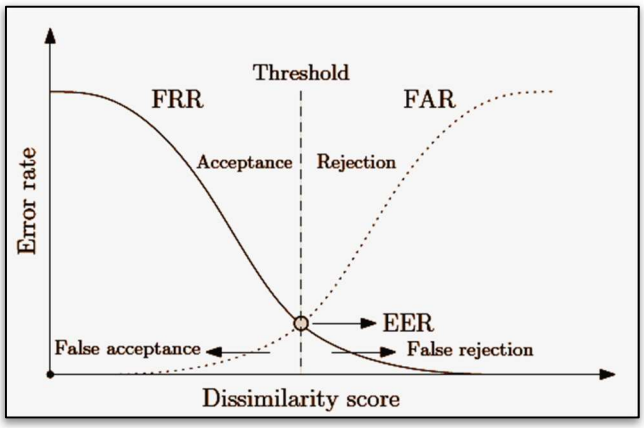


Figure 2.21 : Equal error rate (EER)

2.7.6 Receiver Operating Characteristic (ROC)

Receiver Operating Characteristic (ROC) curve is a 2-dimensional plot between False Positive Rate (FPR or FAR) and True Positive Rate (TPR). In other words, it may be defined as a plot between false match rate against the verification rate. ROC curves are also used to compare the performance of different biometric systems for different threshold values.

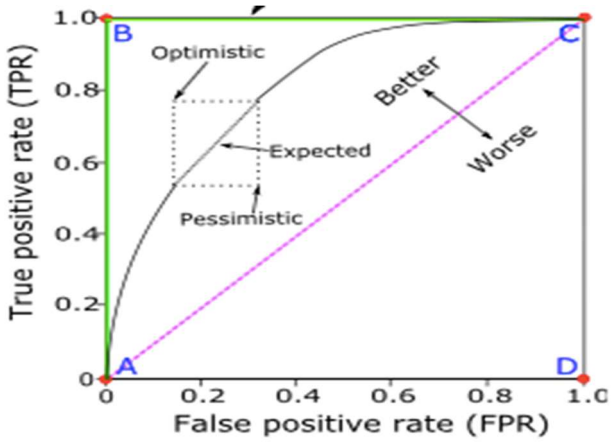


Figure 2.22 : ROC curve

2.7.7 Recognition Rate or Rank –1 Identification (RI)

Recognition Rate or Rank-1 identification is capability of the biometric system in obtaining best matching score with the correct enrolled template in comparison to other templates in the data base. A brief process for computation of RI is as follows:

- Given a biometric $B_q \in$ Query and a biometric $B_e \in$ enrolled, where q=1, ..., n and e = 1, .., m
- The output of a biometric matcher is a similarity score $s(B_q,B_e)$
- Each query biometric is matched to every enrolled biometric and a total of nxm similarity scores are computed
- The scores $s(B_q,B_e)$, for each query biometric B_q are ordered in descending order
- The query biometric B_q is assigned the rank k if the matching gallery biometric is at the k-th location in the sorted list
- Ideally, the system is expected to identify a query at the first rank

2.7.8 Cumulative Match Characteristic (CMC)

Cumulative Match Characteristic (CMC) curve is drawn by taking rank values on the x-axis and the probability of correct identification upto that rank, on the y-axis. A system whose CMC curve lies to the top left corner of CMC is considered to be better.

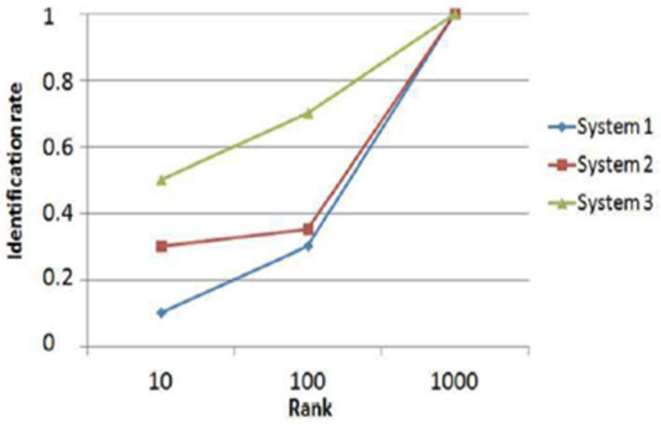


Figure 2.23 : CMC curves for various systems

2.7.9 Decidability Index (DI)

The statistic d' is essentially a reflection of how well separated the two underlying distributions (Genuine and Impostor) are. When the imposter distributions overlap significantly more than the distributions of the genuine class, it causes incorrect decisions. The decidability index measures how similar the sample is with respect to the positive class, and classifying the pattern as positive if the similarity score is above some predefined threshold. For means and standard deviations of genuine (μ_g,σ_g) and imposter (μ_i,σ_i), DI is computed as

$$d = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 - \sigma_i^2)/2}} \quad \ldots(1)$$

2.7.10 Template capacity

Template capacity represents the maximum number of enrolled templates that can be stored in the system.

2.7.11 Matching speed

Matching speed denotes the time taken by the system in verifying or authenticating an individual.

2.7.12 Failure to Enrol Rate (FTE or FER)

This metric represents the number of unsuccessful attempts while enrolling biometric templates at the time of registration.

2.7.13 Failure to Capture Rate (FTC or FCR)

FTC or FCR denotes the number of times the system fails to detect a biometric input when presented correctly.

2.8 Biometric System Evaluation

A biometric cryptosystem is evaluated on the basis of three main parameters- performance, security and privacy. These three parameters can define the acceptability of biometric based recognition system in a universal manner. To cater the need of more generalized framework for ranking and benchmarking of various

biometric recognition systems, a generalized framework is hereby proposed. The proposed evaluation framework thoroughly analyses the system based on empirical data collected from all three aspect of evaluation to defines the system acceptability, irrespective of modality and biometric matching algorithms.

In the last two decades, many biometric algorithms have been developed that now require to be ranked and benchmarked. The goal here is to identify and select those criteria that can help to categorize these algorithms on the basis of recognition accuracy, security and privacy. A secure biometric system when evaluated using these criteria and metrics, must follow a certain evaluation framework that can automate the task of generating quantitative results and perform quantitative comparison between different secure systems. Figure 2.20 shows an evaluation Framework that uses inference modelling to perform quantitative comparison.

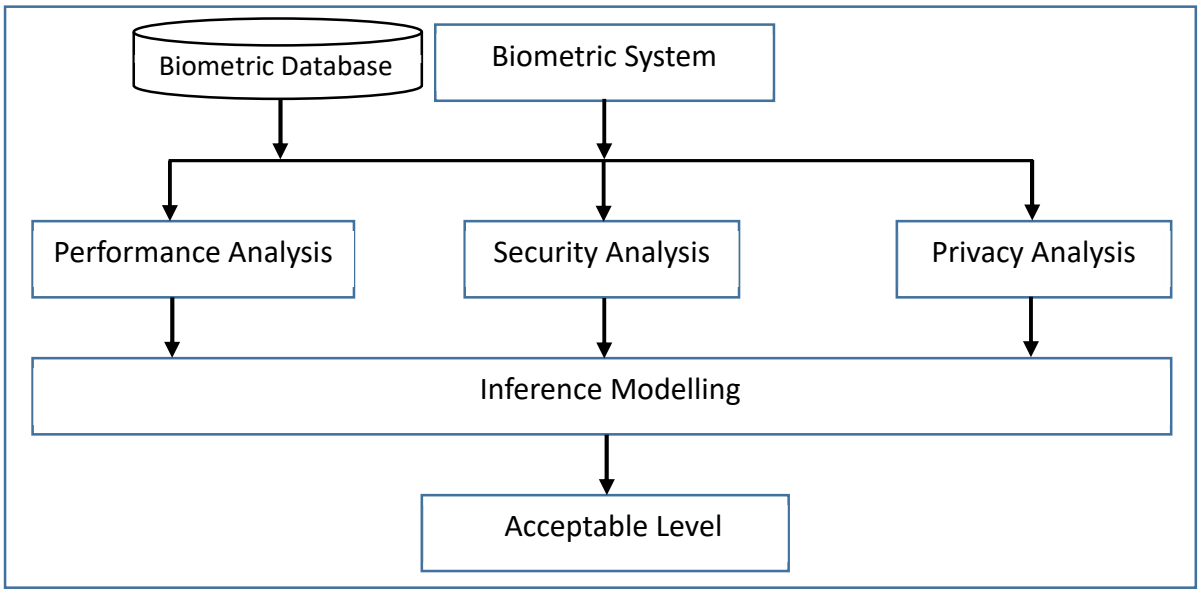


Figure 2.24 : Framework for Evaluation of Biometric based Authentication System

2.8.1 Performance Analysis

In a secure biometric system, there is a trade-off between recognition performance and protection performances (security and privacy). This trade-off certainly exists due to the unclear notion of security, that require more standardized framework for evaluation. If this lacuna can be managed, an algorithm could be developed that would simultaneously reduce both of them. ISO 19795 has standardized the performance metrics and evaluation methodologies of traditional biometric systems. Besides performance testing, this standard does provide metrics related to storage and processing of biometric information. However, ISO 24745 has defined certain criterion to evaluate the performance of biometric template protection algorithm and compare them with the traditional biometric recognition system. Some of the performance evaluation criteria are :

(i) **Accuracy**: Informally, accuracy is a statistical decision of match or non-match, made by a biometric system, illustrated through standard error rates.

(ii) **Throughput**: Intuitively, this measures the number of transactions a biometric template protection device can perform in a defined time interval.

(iii) **Storage Requirement**: This refers to the size of storage required by BTP for different implementation environments and applications/services.

(iv) **Diversity**: An important condition to apply biometric template protection algorithms on original biometric samples is to preserve the minimum intra-user variation and maximum inter-user variation.

2.8.2 Security Analysis

ISO/IEC 24745 specifies that, unlike privacy, security is performed at system level. In general, the ability of a system to maintain the confidentiality of information with provided countermeasures such as access control, integrity of biometric references, renewability and revocability, is referred to as security. To invade the security of a biometric system, an adversary may impersonate as a genuine user to get access control of various services and sensitive data. To provide standard evaluation criterion, ISO/IEC JTC1 24745 subcommittee was the first to put forward the working draft for biometric template protection schemes. This standard majorly provides guidance on various threat models, its countermeasures, requirements for privacy-compliant management, secure storage and transfer of biometric information while ensuring requirements confidentiality, integrity and revocability.

(i) **Confidentiality:** An assurance that an adversary would not be able to exploit the stolen reference templates to gain unauthorized access to sensitive data or resources.

(ii) **Integrity:** An assurance that a protected template and the associated auxiliary data cannot be modified intentionally by an adversary or accidentally altered or corrupted by an authorized entity.

(iii) **Revocability:** This refers to the ability of an administrator to remove the compromised protected template from the system and invoke a new protected template with mated or non-mated instances using system.

(iv) **Renewability:** This ensures the generation and assignment of new protected template and the associated auxiliary data, with an assurance that existing biometric based services or facilities would continue without any drop in technical performance.

There are several attacks whose applicability on a biometric system can be studied to evaluate the security provided by the biometric system. Some of the prominent attacks are as follows :

(i) **Spoofing Attack:** Spoofing attack can only be applied at the sensor level, hence is categorised into direct attack. This could inhibit full exploitation of the potential of biometric technology. Hence, system robustness against spoofing must be tested. Biometric authentication system must be tested for genuine, zero-effort impostor and spoofed trials. A score distribution of these, could likely illustrate the significant effect of spoofed dataset. The overlap of score distribution between genuine and spoofed trials is found to be greater than between genuine and imposter. The system vulnerability towards spoofed dataset can be quantitively measured using spoof false acceptance rate (SFAR). SFAR reflects the percentage of spoofed dataset classified as genuine subjects on a given decision threshold. The FAR obtained for legitimate users is compared against the SFAR to adjust the decision threshold. A plot of Receiver operating characteristic for same False rejection rate of system against SFAR and FAR could allow to optimally decide threshold which could reduce system vulnerability against spoofing. Multi-biometric system could prove to be an important solution to avoid spoofing attacks o biometric authentication system.

(ii) **Attack via Record Multiplicity:** This attack is performed when an attacker illegally accesses database. This access could lead to compromise of protected templates and secret data. When a user is registered at multiple secure biometric authentication systems with same mated instance of biometric sample, this could possibly act as an advantage for attacker. To proceed, attacker may perform correlation analysis on the protected data by linking different databases, to extract pattern of encoded template and associated secret data or may able to retrieve the original template and secret data. To evaluate this attack, unlinkability and revocability analysis is performed.

(iii) **Brute Force Attack:** A brute force attack is systematic attempt of guessing original template until the correct one is found. Here this attack can be successfully executed if same key is used among users for encoding their respective biometrics. If an attacker discovers or steals key from biometric user, it could possibly help to decode all protected template obtained from database of biometric system. Hence, key diversification must necessarily be applied. To evaluate this attack, unlinkability and irreversibility analysis is performed in a condition when same key is used among users to generate encoded biometric data. With this evaluation approach, the robustness of biometric authentication system can be proved.

Evaluation through attacks only specifies the security that biometric system can offer. However, testing of secrecy of biometric template is another level of evaluation that must be served to fully exploit the risk associated with compromise of biometric trait of a user, when the template is leaked or stolen or forged.

2.8.3 Privacy Analysis

Privacy refers to the secrecy at information level. To evaluate privacy offered by biometric protection algorithms, following are the criterion chosen by ISO/IEC 24745: Irreversibility, Unlinkability, and Confidentiality. Specifically, these criterion ensures that the original biometric wouldn't be compromised if protected template get stolen, secondly, an individual could not get tracked by collection of multiple-reference template used at different organization for different applications/services and lastly, the reference template would not be disclosed to unauthorized entity. ISO/IEC 24745 standard provides following definitions of the above-mentioned criterion.

(i) **Irreversibility:** This refers to the computational complexity offered by the renewable protected template to counter the purpose of adversary trying to determine the original biometric sample from the same. In other words, irreversibility check for the leakage of information through Protected template (PT) or the Auxiliary Data (AD).

(ii) **Unlinkability:** Informally, linkability is the ability of an adversary to classify the renewable reference templates on the basis of multiple reference templates. Hence cross matching is the common term to be used in association with unlinkability to understand and analyse its effect on privacy. Few authors have replaced this with "cross comparison". This cross comparison cannot be done through theoretical evaluation and hence must be perceived through practical evaluation approaches. Unlinkability is measured across the applications through cross comparison. If two PTs for mated instances differ considerably,

then the unlinkability condition is fulfilled. Also, when an adversary is not able to get any partial information from the protected template that could be useful to get authorized over a conventional biometric system, unlinkability is attained. To measure the unlinkability, false cross match rate and false non cross match rate are particularly used.

(iii) **Confidentiality:** Confidentiality shows implications for both security and privacy. This property confirms that the secrecy of biometric data would not be hampered. Hence ensures that PT and AD would not be disclosed or accessed in an unauthorized manner.

2.8.4 Inference Modelling

Individual metrices for the three verticals in Figure 2.20 are evaluated over the database from different benchmark. The metric classifier for each classifier is unified to obtain the belief mass about the classifier. The belief mass for the security, privacy and performance evaluation vertical is subjected to classifier fusion. For this, DSmT based approach can be incorporate din model. The inference model can be designed to boost concurrent classifier and suppress classifier. Also, conflicting mass between belief mass can be efficiently modeled and resolved. For instance, propositional conflict resolution rules (PCR) can be used to achieve final acceptance level for the biometric system. The result obtained through these inferences can help us in ranking and benchmarking the biometric algorithms. The acceptability of secure biometric system depends on the fulfillment of criteria that would be measured using these metrics.

2.9 Significant Findings

Evaluation of a biometric system can be done at two stages : Theoretical and Practical. Both stages must be benchmarked and ranked so that the system acceptability level can analysed. The protection performance includes security and privacy analysis of algorithms. In this chapter, the system evaluation strategies using different metrics and various types of attack that can be mounted on a biometric system have been discussed. While metrics such as EER, ROC, CMC, DI and RI helps to completely evaluate system performance, attacks such as brute force, ARM and spoof, helps to decide the acceptance of security criteria. The lack of standard metrics to measure the non-invertibility and revocability, somehow challenges authors to prove the acceptability of their system. Although for unlinkability, few authors have used common metrics but that too is non-standard. It has been observed that the error rate is high in unimodal biometric system as compared to multimodal biometric system. The study shows that multimodal biometric system outperforms the unimodal system in general.

The framework for evaluation of biometric systems can be further augmented by inclusion of more metric for security, privacy and performance. This not only provides more assurance but also improves universal acceptability. Evaluation over the database from various benchmark recovers the biases in database, if any. This work can be further extended in future toward inclusion and standardization of evaluation metric. Also, threshold values for various hyper parameters can be defined in concurrence with the user security and usage requirement.

Chapter 3

Multimodal Biometric Authentication Systems

The objective of this work is to develop a secure multimodal biometric system with an optimal fusion of modalities. A cancelable biometric feature generation method using transformation of each modality feature by some pre-defined key features has been proposed. Key features for individual modality are extracted and stored during the training phase of the proposed model. The exhaustive space of key features enables high brute force complexity for the generated cancelable feature.

3.1 Introduction

In the present digital world, biometric systems have made an extensive proliferation to meet the security requirements in various applications ranging from identification to verification in various domains such as forensics, banking, surveillance and law enforcement. Generally, biometric systems are based on physiological (iris, fingerprints, face) or behavioural (voice, gait, handwriting) attributes or modalities for identifying people [26]. These traits need to be universal, invariant and distinctive [27]. They should also be easy to collect and difficult to imitate. Mostly,

biometric systems can be categorized as unimodal or multimodal [28]. In unimodal systems, only a single biometric form the basis to perform recognition or verification [29]. On the other hand, multimodal systems use information extracted from multiple traits such as face and ear [30, 31], face and voice [32], face and palm print [33] and fingerprint and iris [34]. Generally, usage of multiple traits enhances performance of multimodal system over unimodal system under unreliable and noisy inputs. Multimodal systems are relatively immune to spoofing because forging multiple features simultaneously is a difficult proposition.

Multimodal systems have extensively been studied in the last two decades. Most of the multimodal systems address either optimal combination of modalities or their template protection for developing a robust and reliable solution. Feature level fusion is considered as a good option for combining multiple modalities. Generally, normalized features are combined through concatenation of individual features [33, 34]. In order to cater for incomplete or corrupted input sample, multimodal systems based upon adaptive feature fusion were proposed in [31, 32]. Adaptive fusion rules for combining multiple modalities, exploited image quality parameters for superior performance. Huang et al. proposed a new quality index 'sparse coding error ratio' to analyse input face and ear image quality. In this, quality measure was used to perform weighted feature fusion and thus, mitigate the impact of less reliable modality on the final feature vector. Similarly, in [31], weighted feature fusion was proposed to reduce the effect of extreme pixel corruption among face and ear input images. This was facilitated by a piecewise linear function for selection of weights based on quality and hence ensured collaboration and adaptiveness among multiple modalities. Hence, the matchers are adjusted dynamically based on the signal quality. Both schemes obtain non-class discriminatory information from the quality

of images to facilitate the fusion. However, none of the schemes extract the complementary non-class discriminatory information among different modalities.

Score level fusion was also explored for handling noisy input samples and features vectors with high dimensionality. This fusion methodology can be categorised into combination-based, classifier-based and density-based approach. In combination based score fusion methods multiple classifier scores are combined using statistical methods such as SUM, weighted sum and Hamacher T-Norms etc. Alternatively, classifiers such as SVM [35] can be trained to distinguish between genuine and imposter input score vectors. In addition, individual classifiers scores are processed before subjection to score based fusion model for greater performance. In [32], scores were optimized using confidence factors obtained using particle swarm optimization (PSO). Further, confidence factors were utilized as weights in calculating belief masses for each modality. Similarly, in [36], individual biometric scores are combined using an optimal score fusion model. Individual scores obtained from multi-modal matchers were optimized using confidence factors. The confidence levels were obtained using BSA algorithm. The optimized classifier beliefs were combined using PCR-6 rules to achieve adaptive combination of multiple modalities.

Most of these methods do not consider extraction of complementary information from multiple modalities along with protection of biometric templates. Apart from performance, security of biometric data is also a prime concern. Biometric template protection methods include biometric cancelable biometrics. Cancelable biometrics provide feature transformation in order to secure biometric information of subject [37]. Generally, methods for cancelable biometrics consider either irreversible transformation [38] and bio-hashing. However, irreversible transformations

decrease the discriminability of biometric features leading to low accuracy [39]. In contrast, bio-hashing or salting was proposed to generate irreversible, revocable and secure biometric templates. In this direction, Teoh et. al. [40] elaborated a biometric hash framework which integrated biometrics and external inputs like password and used a random multi-space quantization (RMQ) process to generate RMQ biometric-hash. Similar, transformation was proposed for iris by Chin et al. [41]. S-iris encoding was performed through iterated random password and inner-product of iris feature. Generated S-iris code is revocable and non-invertible. Connie et al. [42] obtained a palm-hash using pseudo-random keys. Experiments were conducted on 50 user self-created database. Savvides et al. [43] proposed an alternative method for generating cancelable feature for face by convolution of initial images with random kernels to produce different encrypted biometric filters which are revocable. However, these methods are studied for obtaining unimodal cancelable features.

Recently, usage of cancelable features in multimodal biometric systems have been suggested. In [44] fusion approaches for multi-modal cancelable biometric recognition were investigated. Naïve bayes and k-NN and MLP were used as individual classifiers. In [45] fingerprint and signature modalities were used for generation of cancellable biometric templates. GA and PSO were used for feature selection. The study shows that future direction for biometric system should focus on taking advantages of both feature and score level fusion. Further, Usage of complementary information across multiple modalities can enhance the performance. In addition, optimal fusion schemes are required to cater the effects of context sensitive environment. Apart from performance, safety of biometric template is foremost concern. Further, due to technology advancements towards availability of high computational power, brute force complexity of future biometric template

protection scheme should be high. Considering these research gaps in multimodal biometric system, a novel approach for a multimodal biometric system with highly secure method for template protection has been proposed. Details of proposed approach follow in the following section.

3.2 Proposed Multimodal Biometric Authentication System

A multimodal biometric system by combining multiple modalities and applying optimal score level fusion has been proposed. Key features have been used for each modality for generating cancelable biometric templates. Feature values obtained from individual characteristic have been combined with key features to perform feature transformation. A robust template is generated by diffusion of individual transformed matrices using graph-based random walk cross-diffusion. The detailed architecture of proposed method is shown in Figure 3.1.

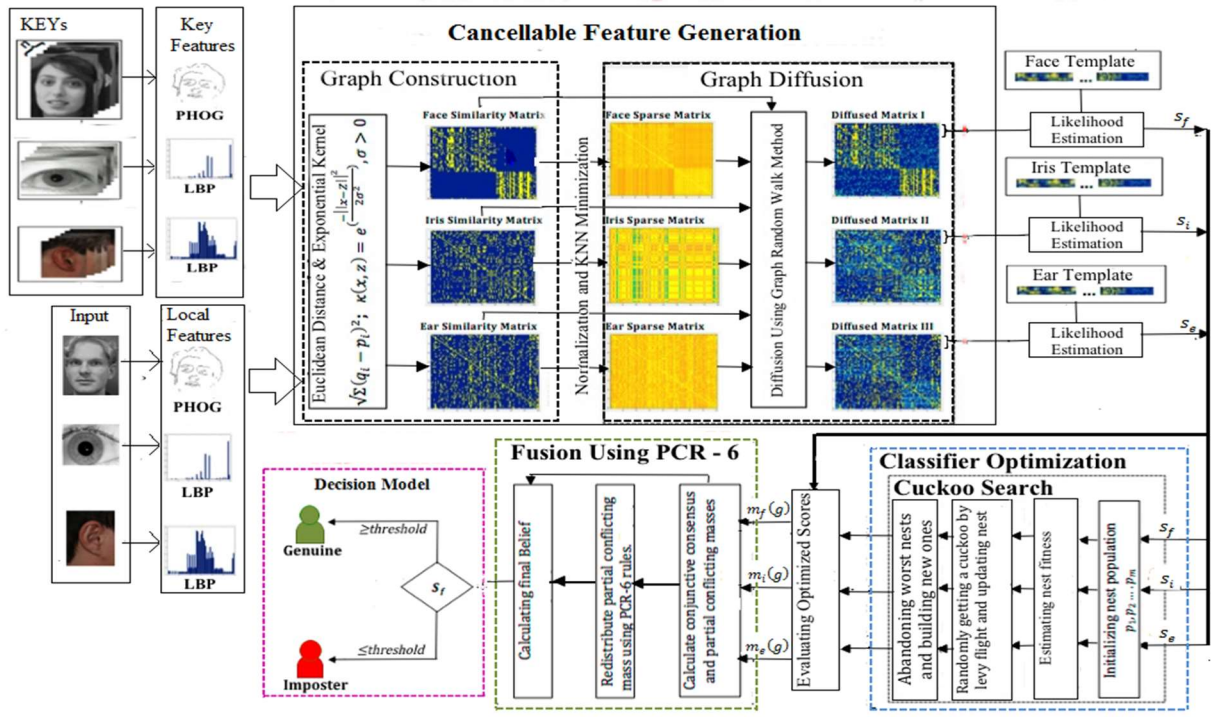


Figure 3.1 : Architecture of Proposed Secure Multimodal Biometric System

In the proposed framework, three modalities viz. Face, Iris and Ear have been considered for generation of key features and individual traits for biometric system. Euclidian distances between input local feature and the key features have been computed and then these distances are applied on an exponential kernel to get the Similarity matrices. Then Sparse matrices are formed from these similarity matrices. This transformation of features is followed by diffusion of transformed features using a multi-view cross over graph random walk [46] adapted for multimodal systems. Using this, similarity matrix for individual modality is diffused with sparse matrices of other modalities to yield a diffused graph from which individual cancelable feature are extracted. This process dynamically retains the complementary information from the input images.

Extracted cancelable features thus generated are non-invertible and used to create templates. Similarly, at the time of authentication, these cancelable features are extracted for each modality for comparison with stored templates. Matching scores for individual modality are obtained using Bhattacharya distance and subjected to a two-stage fusion model [47]. Wherein, the problem has been modelled as a Shafer model with two classes as genuine and imposter. The generated masses are subjected to cuckoo search optimization to obtain optimal confidence factors of individual classifier [48]. Individual beliefs are optimally combined using DSmT based PCR-6 rules. On the basis of this optimal score, the user is categorized as genuine or imposter. Different stages in the proposed scheme for multimodal biometric system have been discussed in the following sections.

3.2.1 Multimodal Feature Extraction

The proposed scheme is based on three biometrics of the subject viz. facial shape, iris and ear texture. Facial shape is extracted using Pyramid Histogram of Oriented Gradient (PHOG) [49]. PHOG descriptor is invariant to geometric transformations and illumination changes. Local Binary Pattern (LBP) is used for extracting iris features [50] and ear texture [51].

Face local feature vector l_f of dimensionality u_f is extracted from input face image I_f using PHOG. The PHOG vector obtained is $\left(v_1, v_2, \dots, v_{u_f}\right)$ of the dimensions u_f. The PHOG vector is further normalized to get the local feature vector l_f, which represents the spatial distribution of edges given by Eq. (1)

$$l_f = \left(v_1 v_2 \dots v_{u_f}\right) / \sum_{j=1}^{u_f} v_j \qquad \dots(1)$$

In addition, for an ear input image, information regarding texture is acquired for finding local feature vector by applying Gabor filter followed by LBP [51]. For this, the input image I_e is converted into Gabor Magnitude Picture (GMP) G_e by applying Gabor filter at every pixel using Eq. (2)

$$G_e(x, y, \beta, \omega, \lambda, \gamma, \Phi) = \cos\left(2\pi \frac{x'}{\lambda} + \psi\right) * \exp\left(-\frac{(x')^2 + \gamma^2 (y')^2}{2\beta^2}\right) \qquad \dots(2)$$

where $x' = x\cos\omega + y\sin\omega$ and $y' = -x\sin\omega + y\cos\omega$, λ represents wavelength of sinusoidal factor, φ is the phase offset, β is standard deviation of the Gaussian envelope, ω represents the orientation of the normal to the parallel strips of a Gabor function and γ is the spatial aspect ratio.

Ear description vector l_e of dimensionality u_e is calculated by constructing histogram $(H_1, H_2, \dots, H_{u_e})$ of LBP values obtained for each pixel of image G_e and normalizing it using Eq. (3)

$$l_e = \frac{(H_1, H_2, \dots, H_{u_e})}{\sum_{i=1}^{u_e} H_i} \quad \dots(3)$$

where $(H_1, H_2, \dots, H_{u_e})$ is the histogram of LBP values calculated from G_e and u_e are the number of bins.

The localized iris is converted into a rectangular image I_R of dimensions $M \times N$ using rubber sheet normalization [50]. The feature vector l_i of dimensionality u_i is obtained after finding LBP histogram of image I_R. After obtaining LBP Histogram values $(B_1, B_2, \dots, B_{u_i})$, iris local feature vector l_i is obtained using Eq. (4)

$$l_i = \frac{(B_1, B_2, \dots, B_{u_i})}{\sum_{i=1}^{u_i} B_i} \quad \dots(4)$$

where $(B_1, B_2, \dots, B_{u_i})$ is the histogram of LBP values calculated from I_R and u_i are the number of bins. After obtaining local feature vectors l_j where $j \in \{f, e, i\}$ cancelable features are generated and same is discussed as follows.

3.2.2 Cancelable Feature Generation

The cancelable features are imperative for any reliable and secure biometric system. In order to achieve this, an adapted iterative graph random walk cross-view diffusion for multimodal biometric system has been proposed. For this, local feature vectors

are transformed using key features which are generated from a set of key images $\{K_1, K_2, \dots, K_n\}$ for each modality. Key images for a modality are a set of input images of the same trait. The extraction of key features also follows the same process for each modality as discussed in the above sub section. Concatenation feature vector F is obtained to get a representation of local feature vector with respect to key features $(k_{1,j}, k_{2,j}, \dots, k_{n,j})$ for n keys of j^{th} modality using Eq. (5)

$$F_j = \left(l_j, k_{1,j}, \dots, k_{n,j}\right)' \quad \dots(5)$$

where j ∈ {f , e, i} correspond to face, ear and iris features.

To obtain a feature transformation, initially, a $(n + 1) \times (n + 1)$ similarity matrix E_j is generated from feature concatenation vector F_j for each modality using Euclidean distance d [52] between two vectors using Eq.(6)

$$E_j(a, b) \propto e^{-\frac{d\left(F_j(a), F_j(b)\right)}{2}} \quad \dots(6)$$

where both a and b vary from 1 to $(n + 1)$ and $j \in \{f , e, i\}$ correspond to face, ear and iris modalities. Further, each similarity matrix E_j is normalized to obtain normalized similarity matrix E_j^* for obtaining maximum variance and reduce redundancy using Eq. (7)

$$E_j^*(a, b) = \frac{E_j(a,b)}{\sqrt{\left[\{E_j(a,1)\}^2 + \{E_j(a,2)\}^2 + \cdots + \{E_j(a,u_j)\}^2\right]}} \quad \dots(7)$$

Sparse matrix S_j for j^{th} modality is calculated after k-NN reduction and normalization in order to obtain an efficient representation of similarity matrix [53]. Initially, E_j^* is

reduced to a data anchor matrix $\widetilde{E_J}$for each modality by applying k-NN [54] given by Eq. (8). The number of nearest neighbours k is considered to be a critical tuning parameter for optimal generation of sparse matrix. Bootstrapping process was considered for optimal selection of nearest neighbours k value [55]. The optimal value determined using this process is square root of a.

$$\widetilde{E_J}(a,b) = \begin{cases} E_j^*(a,b), & if\ b \in kNN(a) \\ 0, & else \end{cases} \quad ...(8)$$

Further, $\widetilde{E_J}$ is normalized to get the sparse matrix S_j using Eq. (9)

$$S_j(a,b) = \frac{\widetilde{E_J}(a,b)}{\sum_{b \in kNN(a)} \widetilde{E_J}(a,b)} \quad ...(9)$$

where both a and b vary from 1 to (n + 1).

Information obtained from each modality by the virtue of its Sparse and Data anchor matrix S_j and $\widetilde{E_J}$ is diffused with information from other modalities in order to obtain cancelable features. For this, graph based random walk cross view diffusion has been considered. Diffusion follows the transformation of initial local feature. The number of iterations w is determined by convergence of the cross-diffusion process. For a given Sparse and Data anchor matrices of the three modalities, the cross-diffusion process converges after the chosen number of iterations. The goal of this process is to obtain a distance metric that can successfully retain similarity data from sparse matrix. To achieve this, the optimal value of w has been determined as 20. Initial Affinity matrix V_{jo}, diagonal matrix D_{jo} and normalized affinity matrix B_{jo} for j^{th} modality are obtained using Eq.(10-12)

$$V_{j\,0} = \widetilde{E_{J\,0}} \times \widetilde{E_{J\,0}}^{\,T} \quad \ldots(10)$$

$$D_{j0}(a,b) = \sum_{b=1}^{n} V_{j\,0}(a,b) \quad \ldots(11)$$

$$B_{j\,0} = D_{j\,0}^{-\frac{1}{2}} \times V_{j\,0} \times D_{j\,0}^{-\frac{1}{2}} \quad \ldots(12)$$

where $j \in \{f, e, i\}$ and $\widetilde{E_{J\,0}}$ is the initial data anchor matrix for j^{th} modality. After obtaining initial affinity, diagonal and normalized affinity matrix, cross diffusion is carried out in order to reach consensus among multiple modalities.

First, update initial Data anchor matrix $\widetilde{E_J}$ is determined using Eq. (13)

$$\widetilde{E_J} = \alpha_j B_j * \widetilde{E_J} + \left(1 - \delta_j\right)\widetilde{E_{J\,0}} \quad \ldots(13)$$

where $j \in \{f, e, i\}$. α_i and δ_i are the free parameters used for updating Data anchor matrix during the iterative cross diffusion process. These parameters are determined through grid search during the learning phase of the proposed model. For this, the optimum value of these parameters has been searched in the range [0,1] with a step size of 0.1. The optimum values of these parameters are chosen such that their sum is equal to 1.

Further, graph random walk is applied over face, ear, iris using Eq. (14-16)

$$\widetilde{E_f} = S_f * \frac{1}{2} * \left[\widetilde{E_e}^{T} * S_f + \widetilde{E_\iota}^{T} * S_f\right] + \varepsilon A \quad \ldots(14)$$

$$\widetilde{E_e} = S_e * \frac{1}{2} * \left[\widetilde{E_\iota}^{T} * S_e + \widetilde{E_f}^{T} * S_e\right] + \varepsilon A \quad \ldots(15)$$

$$\widetilde{E_\iota} = S_i * \frac{1}{2} * \left[\widetilde{E_e}^{T} * S_i + \widetilde{E_f}^{T} * S_i\right] + \varepsilon A \quad \ldots(16)$$

where A is the unit matrix which is added to the symmetric similarity via a weight ε to increase noise immunity. This parameter is fixed to 0.8 for the experiments.

Affinity matrix $\boldsymbol{V_j}$, normalized affinity matrix $\boldsymbol{B_j}$ and diagonal matrix $\boldsymbol{D_j}$ are updated using Eq. (17-19)

$$V_j = \widetilde{E_J} * \widetilde{E_J}^T \quad \ldots(17)$$

$$B_j = D_j^{-\frac{1}{2}} \times V_j \times D_j^{-\frac{1}{2}} \quad \ldots(18)$$

$$D_j(a,b) = \sum_{b=1}^{u_j} V_j(a,b) \quad \ldots(19)$$

where $j \in \{f, e, i\}$, final data anchor matrix $\breve{E}_j$ gives diffused graph for j^{th} modality. Cancelable feature is obtained from diffused graph by selecting information significant to the input subject. From eqn. (6), it can be observed that 1st row contains most significant information with respect to input. Cancelable feature is stored as template $\mathbf{A_{j,Temp}}$ during enrollment and utilized as a cancellable feature $\mathbf{A_j}$ in likelihood calculations of j^{th} modality during authentication. These cancelable features for each modality are obtained using Eq. (20)

$$A_j = \widetilde{E_j}(1,:) \quad \ldots(20)$$

In order to calculate scores of j^{th} modality during authentication, initially, the Bhattacharya distance $\delta(\mathbf{A_j}, \mathbf{A_{j,Temp}})$ between the cancelable feature ($\mathbf{A_j}$) and template ($\mathbf{A_{j,Temp}}$) is determined using Eq. (21).

$$\delta\left(A_j, A_{j,Temp}\right) = \left(1 - \sum_{j=1}^{u_j} \sqrt{A_j(i) * A_{j,Temp}(j)}\right)^{1/2} \quad \ldots(21)$$

Likelihood $s_j(g)$ of obtained cancellable feature $\mathbf{A_j}$ of j^{th} modality is calculated using Eq. (22)

$$s_j(g) \propto exp\left(-\frac{\left(\delta(A_j, A_{j,Temp})\right)^2}{2\sigma_j^2}\right) \quad \ldots(22)$$

where $j \in \{f, e, i\}$ correspond to face, ear and iris and σ_j is the standard deviation for j^{th} modality.

The likelihood is calculated for the cancelable feature of each modality as $s_j(g)$, where $j \in \{f, e, i\}$ correspond to face, ear and iris. These estimated likelihood scores are passed to the proposed multistage optimal score fusion model.

3.2.3 Optimal Score Level Fusion Model

The individual scores are optimally fused for achieving precise decision boundary. A multistage score fusion model has been proposed for obtaining final belief for making decisions. Initially, scores are optimized using cuckoo search [56] and converted to individual belief masses. Conflict among individual belief is determined and redistributed using DSmT based PCR-6 rules [57, 58]. Detail of the proposed approach is given below:

(a) Score optimization

Optimization is done by suppressing and boosting (scaling) scores by a confidence parameter in order to improve the performance of the system. Hence, the matching scores of the input images are dynamically adjusted by the confidence factor of the

individual matchers. Shafer's model has been used to fuse data from three modalities. In this model, frame of discernment is defined with two elements viz. genuine and imposter $\Omega = \{g, im\}$. Each biometric trait provides a score about a subject which is obtained using Eq. (22). For converting the score to respective belief mass denoeux belief system [59] is used using Eq. (23-24)

$$m_j(g) = C_j \times s_j(g) \quad \ldots(23)$$

$$m_j(im) = 1 - C_j \times s_j(g) \quad \ldots(24)$$

where $j \in \{f, e, i\}$ correspond to face, ear and iris respectively and corresponding $\mathbf{C_j}$ are confidence factor for individual classifier.

In order to determine individual classifier confidence factor, cuckoo search has been applied with initial likelihoods as its input space. Fitness of each nest is observed relative to other nests and l nests with best fitness (with Minimum FAR and FRR) are retained while worst w nests are abandoned and a new population is generated. Fitness of a nest is evaluated through a Bayesian risk function [60] for face, ear and iris using Eq. (25)

$$fitness_j = cost_{fa} * FAR_j + cost_{fr} * FRR_j \quad \ldots(25)$$

where $j \in \{f, e, i\}$ correspond to face, ear and iris and $cost_{fa}$ is the cost of false acceptance whereas $cost_{fr}$ is the cost of false rejection. The fitness function quantifies the risk of unauthorized access and unrecognition due to false acceptance and false rejection respectively. Generally, the cost of false rejection and cost of false acceptance are chosen in concurrence with the security requirement. For biometric

systems with stringent security requirement, the cost of false acceptance ($cost_{fa}$) is maximized and the cost of false rejection ($cost_{fr}$) is minimized. It was also reported that the range of $cost_{fa}$ and $cost_{fa}$ should be in the range from 0 to 2 and their sum should be 2. Considering this, the values of $cost_{fa}$ and $cost_{fr}$ have been chosen as 1 in order to minimize the Global Bayesian error function and also to optimize the decision model threshold. Finally, confidence parameter C_j for j^{th} modality is value of the nest with minimum objective function value. Using Eq.(23) genuine belief masses for face ($m_f(g)$), for iris ($m_i(g)$) and for ear ($m_e(g)$). Similarly, imposter belief masses $m_f(g)$, $m_e(g)$ and $m_i(g)$ are obtained using Eq (24). These masses are further subjected to optimal multimodal fusion model as described below.

(b) Optimal Fusion

Optimized belief masses are optimally fused using $D_{sm}T$ based PCR-6 rules to achieve final belief about the subject. For this conjunctive consensus are estimated using Eq. (26-27)

$$m_{fei}(g) = \prod_{j=1}^{3} m_j(g) \quad \ldots(26)$$

$$m_{fei}(im) = \prod_{j=1}^{3} m_j(g) \quad \ldots(27)$$

where $j \in \{f, e, ir\}$.

In addition, Total conflict among modalities is obtained by adding partial conflicting masses of genuine and imposter scores of experts using Eq. (28)

$$m_{fei}(g \cap im) = m_f(g) \times m_i(im) \times m_e(im) + m_f(im) \times m_i(g) \times m_e(im) + m_f(im) \times m_i(im) \times m_e(g) + m_f(g) \times$$

$$m_i(im) \times m_e(g) + m_f(g) \times m_i(g) \times m_e(im) +$$

$$m_f(g) \times m_i(g) \times m_e(g) \quad \ldots(28)$$

Total conflict consists of 6 partial conflicts which are redistributed among the two classes of subjects using Eq. (29-34), where x_1 - x_9 are conflict redistribution mass for genuine class of the subject and y_1 - y_9 are conflict redistribution mass of imposter class.

$$\frac{x_1}{m_i(g)} = \frac{y_1}{m_f(im)} = \frac{y_2}{m_e(im)} = \frac{m_i(g) \times m_f(im) \times m_e(im)}{m_i(g) + m_f(im) + m_e(im)} \quad \ldots(29)$$

$$\frac{x_2}{m_f(g)} = \frac{y_3}{m_i(im)} = \frac{y_4}{m_e(im)} = \frac{m_i(im) \times m_f(g) \times m_e(im)}{m_i(im) + m_f(g) + m_e(im)} \quad \ldots(30)$$

$$\frac{x_3}{m_e(g)} = \frac{y_5}{m_f(im)} = \frac{y_6}{m_i(im)} = \frac{m_i(im) \times m_f(im) \times m_e(g)}{m_i(im) + m_f(im) + m_e(g)} \quad \ldots(31)$$

$$\frac{x_4}{m_f(g)} = \frac{x_5}{m_i(g)} = \frac{y_7}{m_e(im)} = \frac{m_i(g) \times m_f(g) \times m_e(im)}{m_i(g) + m_f(g) + m_e(im)} \quad \ldots(32)$$

$$\frac{x_6}{m_f(g)} = \frac{x_7}{m_e(g)} = \frac{y_8}{m_i(im)} = \frac{m_i(im) \times m_f(g) \times m_e(g)}{m_i(im) + m_f(g) + m_e(g)} \quad \ldots(33)$$

$$\frac{x_8}{m_e(g)} = \frac{x_9}{m_i(g)} = \frac{y_9}{m_f(im)} = \frac{m_i(g) \times m_f(im) \times m_e(g)}{m_i(g) + m_f(im) + m_e(g)} \quad \ldots(34)$$

The final belief about the subject is obtained by summation of estimated redistribution masses and respective conjective consensus using Eq-(35-36)

$$m_{pcr6}(g) = m_{fei}(g) + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 \quad \ldots(35)$$

$$m_{pcr6}(im) = m_{fei}(im) + y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7 + y_8 + y_9 \quad \ldots(36)$$

$m_{pcr6}(g)$ and $m_{pcr6}(im)$ represent the final belief of the subject being genuine and that being imposter respectively. If the matching score of the input with the template is above a pre-specified threshold, the person is declared genuine and imposter otherwise.

Pseudo Code of the Proposed Biometric System

Input: I_f , I_e , I_i (input images) **Genuine/Imposter Classification**

1: *Generation of local feature vectors:*
2: **function** FEATURE EXTRACTION (I_f , I_e , I_i)
3: Obtain l_f , l_e and l_i from Eq. (1), Eq. (3) and Eq.(4)
4: **return** l_f , l_e , l_i
5: *Generation of key features for transformation:*
6: **for** all n key image triplets {($K_{1,f}$, $K_{2,e}$, $K_{n,i}$)...($K_{n,f}$, $K_{n,e}$, $K_{n,i}$)} **do**
7: ($k_{n,f}$, $k_{n,e}$, $k_{n,i}$) = feature extraction($K_{n,f}$, $K_{n,e}$, $K_{n,i}$)
8: **end for**
9: *Feature Transformation:*
10: **for** $\forall\, j \in \{f, e, i\}$ **do**
11: Generate F_j using Eq. (5)
12: $v \leftarrow$ number of transformation operations
13: $v = 4$
14: **for** p : 1 to v **do**
15: **for** a : 1 to $n + 1$ **do**
16: **for** b : 1 to $n + 1$ **do**
17: **if** $p = 1$ **then**
18: Obtain E_j using Eq. (6)

end if

if $p = 2$ **then**

Obtain E_j^* using Eq. (7)

end if

if $p = 3$ **then**

Obtain $\breve{E}_j$ using Eq. (8)

end if

if $p = 4$ **then**

obtain S_j using Eq. (9)

end if

end for

end for

end for

end for

Cross diffusion:

for $\forall\, j \in \{f, e, i\}$ **do**

$w \leftarrow$ number of cross diffusion iterations

while $w > 0$ **do**

Initialize V_{jo}, D_{jo}, B_{jo} using Eq. (10-12)

Update $\widetilde{E_{j0}}$ using Eq. (13) and apply graph random walk over other j^{th} modality using (14), (15) or (16)

Update V_j ,D_j , B_j using Eq. (17-19)

$w = w - 1$

end while

Obtain A_j using Eq. (20)

43: **end for**

44: **return** (A_f ,A_e ,A_i)

45: *Optimal score fusion:*

46: Obtain scores s_f , s_e and s_i using Eq. (21)-(22)

47: Obtain optimized and genuine masses using Eq. (23)- (24)

48: Obtain conjunctive consensus among masses from Eq. (26)-(27)

49: Calculate partial conflicts from Eq. (28)-(34) and find final beliefs of the subject from Eq. (35)

50: Classify the subject into classes based on threshold

3.3 Experimental Validation

This section details different aspects of experiments performed in order to compare and contrast the proposed multimodal biometric system with the state-of-the-art systems. Qualitative and quantitative results are demonstrated and detailed security analysis is described as follows.

3.3.1 Datasets

The proposed multimodal system is based upon the face, ear and iris of a subject. For each subject, enrolment and test images are required for every trait. Features obtained from enrollment images are stored as templates. Further, matching scores are calculated from these templates and feature from test images. It is assumed that these traits are independent of each other. Based on this assumption, four virtual multimodal datasets were built from various publicly available databases of these

traits. Three images are taken randomly from a distinct subject of these unimodal databases. Further, two of the images are used for template generation and another as a test image for an experiment. Virtual Datasets have been obtained by unique combinations of benchmark Face, Iris and Ear Databases namely ORL Face database, Computer Vision Science Research Projects face Database [61], MMU iris database [62], AMI ear database [63], CASIA Iris Database v1[64], IIT Delhi Iris [65] and Ear Database [66]. ORL Face database [62] has 10 images of 40 distinct subjects taken with varying lighting conditions, facial details and expressions. Moreover, the images are of the size 92x112 pixels with 256 grey levels. Computer vision science research projects face database is an expansive database of true colour images with a total of 395 distinct subjects with 20 individual images. AMI Ear database consists of 100 different subjects with 7 images per subject each of resolution 492x702 pixels. Casia Iris Database v1 has 108 distinct subjects with 3 images for each side for every subject. Each captured image is uniformly illuminated with a total resolution of 320x280. MMU Iris database consists of total 450 images with 5 images per iris. IIT Delhi Iris Database has 224 distinct subjects with a resolution of 320 x 240 pixels. Finally, IIT Ear Database was acquired from a distinct 121 subjects with a resolution of 50 x 180 pixels in an indoor environment.

The proposed method has been evaluated on a total of four virtual datasets obtained from these benchmark databases. Dataset 1 contains 50 distinct subjects with taken from 40 distinct subjects of from ORL Face database and 10 distinct subjects of Computer vision science research projects face database. Ear and iris images are taken from AMI Ear database and MMU Iris database. For each subject, one image is retained for testing while two images are used for training. Dataset 2 is generated similarly with 80 distinct subjects each from Computer vision science research

projects face database, IIT Delhi Iris Database and IIT Delhi Ear database. Database 3 is obtained from 40 distinct subjects from Computer vision science research projects face database, CASIA Iris Database v1 and IIT Ear Database. Finally, Dataset 4 contains randomly chosen 100 subjects from datasets 1, 2 and 3. Keys are acquired for each modality from these public datasets.

3.3.2 Performance metrics

Different performance metrics such as decidability index [67], EER [68], accuracy are used to evaluate the performance of proposed biometric system. Qualitative treatment is done by observing the score distributions of genuine and imposter classes of the proposed model. EER and Accuracy are obtained from test datasets for various state of the art biometric systems and the proposed method. Various performance metrics are described as follows.

Decidability: Performance evaluation of the proposed model is carried out through decidability calculations. Decidability is calculated by the statistic d-prime (d') which measures the distance between genuine and imposter score distributions. It is calculated as the difference between the means of genuine and imposter compared to their variances given by eq. (37). D-prime, however, not the only measure of decidability. F-ratio is a similar measure which can be used to calculate decidability. Both d-prime (d') and F-ratio are independent of threshold. Further, F-ratio is directly related to the EER while d-prime can be directly obtained from Acceptance rate and FAR.

$$d' = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 + \sigma_i^2)/2}} \quad \ldots(37)$$

where μ_g, μ_i are the means of genuine and imposter distributions. σ_g, σ_i are standard deviation of genuine and imposter score distributions.

Equal Error Rate (EER): Equal Error Rate (EER) is obtained from the Receiver Operating Characteristic (ROC) curve at the point where the rate of false rejection is equal to the rate of false acceptance. Experimental EER values are obtained from ROC curves as depicted in Figure 3.3. For experimental validation, empirical EER value have been computed directly from ROC curves instead of its theoretical EER value determined through score distributions via F-ratio. This is mainly performed to avoid any error between theoretical and experimental EER value. This difference in theoretical and empirical EER values was mainly attributed to the imperfect Gaussian nature of the genuine and imposter score distributions [68].

Accuracy: Accuracy quantifies the ability of a system to successfully authenticate an enrolled subject and determined using Eq. (38)

$$accuracy = \frac{N_g}{N_i + N_g} \quad \ldots(38)$$

where N_g are the number of successful genuine attempts and N_i are the number of successful imposter attempts. A genuine attempt is registered if an enrolled subject is authenticated in the first attempt and unsuccessful on the other hand if an enrolled subject is not authenticated.

Table 3.1 : Values of Experimental Parameters

Parameter	Description	Experimental Values
k	No. of Nearest Neighbours	8
α, δ	Cross-Diffusion parameters	1

w	Cross-Diffusion Iterations	20
N	Cuckoo Search Population	30
C_{fa}	Cost of False Acceptance	1
C_{fr}	Cost of False Rejection	1

3.3.3 Experimental Details

Two experiments have been carried out in order to evaluate and contrast the performance of the proposed multimodal scheme with existing schemes. Initial local features l_1, l_2 and l_3 are extracted from each trait of datasets 1-4. Further, score distributions of each trait are obtained by matching initial local features of enrolment images with test images. In the next step, initial local features l_1, l_2 and l_3 are used to generate proposed cancellable features. Score distribution of cancelable features is generated for each dataset. The final score of cancelable features is obtained from proposed multistage score fusion model. Decidability of each score distribution is calculated.

In the second experiment, proposed approach is contrasted with existing score fusion techniques. Matching scores of initial local features l_1, l_2 and l_3 are combined using techniques such as SUM [69], MIN [69], MAX [69, Hamacher t-norm, Sugeno weber t-norm [70]. Accuracy and EER of each method are calculated for multimodal datasets. Accuracy and EER of the proposed multimodal system is calculated for each dataset. Experiments have been carried out on MATLAB 2016, on 2.40 GHz, CORE i7 CPU.

In order to overcome sampling bias, all the experimental validation is carried out using a three-fold cross validation. In each dataset, three images have been randomly chosen for every subject for the three modalities. For each validation, two images

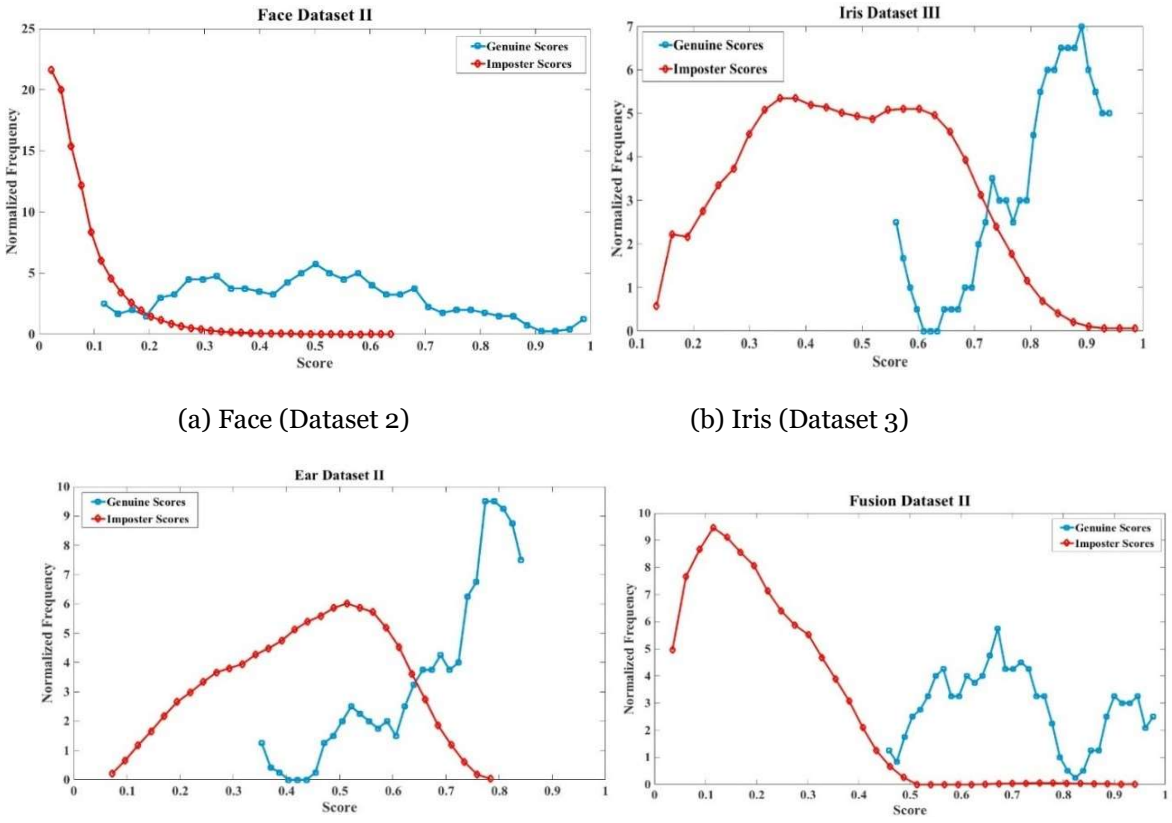
were utilized to obtain cancellable templates and the other image is used for testing. Reported results are average value that is obtained from three-fold cross validation. Further, proposed biometric system involves stochastic nature of cuckoo search optimization which is used for determining classifier confidence factor. Hence, the average results for the proposed multistage score fusion model have been computed over the 25 runs of algorithm.

3.4 Qualitative Analysis

Qualitative analysis has been carried out by score distribution analysis and security analysis of the proposed model. Initially, the model is analysed quantitatively on the basis of the decidability of various score distributions, followed by the description of non-invertibility of proposed cancellable features along with various attacks possible in current context.

3.4.1 Score Distribution Analysis

Qualitative analysis of the proposed model is carried out by observing Score distribution and their decidability. Figure 3.2(a)-(c) typical score distributions calculated from unimodal data of face, iris and ear. The typical score distribution of multimodal systems is shown in Figure 3.2(d) and Decidability of each score distribution is listed in Table 3.3.



(a) Face (Dataset 2) (b) Iris (Dataset 3)

(c) Ear (Dataset 2) (d) Proposed fusion model (Dataset 2)

Figure 3.2: Sample comparison of score distribution: (a)Face modality for dataset 2 (b) Iris modality for dataset 3 (c) Ear modality for dataset 2 (d) Proposed fusion model for dataset2

Table 3.2 : Comparison of decidability values for Face, Iris and Ear biometrics

Biometric model	Face	Iris	Ear	Proposed Method
Dataset 1	3.6038	2.7289	2.8082	**3.9066**
Dataset 2	2.7808	1.9578	2.2200	**4.0604**
Dataset 3	2.9648	2.6053	2.9132	**3.4308**
Dataset 4	1.7106	2.6994	2.4552	**3.8601**
	2.7650	2.4978	2.5991	**3.8144**

Normalized frequency distributions of imposter and genuine scores are correlated with the reliability of biometric trait. Highly localized imposter score distribution below the threshold and similar genuine score distribution above the threshold

indicates higher reliability. In Figure 3.2(a), score distribution of face local features reveals that imposter score distribution of local face features is highly localized below 0.2 in a hyperbolic form. However, the genuine score distribution is distributed in the domain 0.1 to 1. Distributed genuine distribution indicates very little reliability of face local feature. This is mainly due to the limitations of simple PHOG operator in giving abundant information about face of the subject which is a 24-bit true colour image. Further, this proves the limitation of local face feature in identifying the subject with reliability. On the other hand, distributions of local iris feature in Figure 3.2(b) show comparatively localized genuine score distribution with the peak value at 0.9 but higher imposter score variance with frequency values greater than zero occurring from 0.2 to 0.9. This indicates less reliability in recognizing the subject and hence, iris feature vector obtained by LBP is inadequate for recognition of the subject when unaided by another useful modality. This is due to less discernibility of the iris binary patterns by the unimodal matcher. Similarly, from Figure 3.2(c), high variance is observed in genuine and imposter score distributions.

Hence, similar to face and iris, Ear local features are unreliable for unimodal authentication, mainly due to the overlap between genuine and imposter score distributions. However unimodal system requires low computational cost. Consequently, they can be useful in a multimodal system where information from multiple feature vectors is pooled for further processing. Using multimodal feature vectors with low computational cost in efficient fusion schemes can lead to faster operation without any trade-off in performance. This can be validated from Figure 3.2(d) where overlapping between the scores of genuine and imposter is trivial in nature, from which clear threshold for genuine input can be obtained. For genuine scores, distribution is restricted from 0.5 to 1 with peak value at 0.7, whereas

imposter score distribution is contained below threshold making the overlap between genuine and imposter score distributions is minimal. Further, this verifies the capability of proposed model in successfully combining unimodal features by utilizing cross diffusion with optimal score fusion. In addition, classifier score optimization which scales the scores based on their confidence factors leads to a well-defined threshold as seen in Figure 3.2(d) which is not the case of unimodal matchers as seen in Figure 3.2(b) and 3.2(c).

Average decidability values of traits face, ear and iris are 2.765, 2.599 and 2.497 when histogram intersection is used to calculate the score. In contrast to unimodal system, proposed multimodal biometric system gives the decidability value of 3.814. Increase in decidability validates the capability of proposed biometric model in combining multimodal data. Optimization of classifier scores by confidence factor leads to a well-defined threshold as the scores with lower confidence values are suppressed by cuckoo search optimization and similarly, the scores with higher confidence values are boosted. This leads to a well-defined decision boundary between genuine and imposter class.

Security analysis of the proposed model along with the success ratio of different attacks possible on the proposed biometric system is discussed in the following section.

3.4.2 Security Analysis

Proposed scheme has been assessed from various security aspects namely non-invertibility, diversity and revocability of cancelable templates and robustness of

system against possible attacks under worst case scenarios. The image features are protected using image transformation as described in section 3. Cancelable features are highly non-invertible after conversion due to the nature of transformation techniques, as cancellable features retain only a small part of the transformed feature concatenation matrix. This is due to the random projection of the initial features from the modalities using key features. The transformation of initial features is done by calculating similarity between keys and input feature, followed by generation of sparse matrix and finally, cross diffusion. Three initial features are cross-diffused and only required information is selected from the final matrix to generate the template for a modality. Thus, the K-NN process for generating sparse matrices followed by the reduction in dimensionality from cross-diffusion is a lossy process which retains only the necessary information. Therefore, it is not possible to estimate the three initial features from the template as only minimal information is retained from template.

Best attempt at retrieving the original biometric is by obtaining the minimum norm solution using brute force. However, this is highly unlikely if the attacker is not in possession of key features as the total number of combinations will be proportional to the number of keys. Hence, the generated templates are mostly non-invertible. In addition, processing of image features with respect to pre-defined key images lead to high diversity among features of different subjects as its final values are generated from a set of sample space. Finally, one of the major attractions of the proposed approach is high revocability. In case of a breach in the template database, *k* features can be changed by changing the key images. Further, Cross diffusion based upon similarity metrics of modalities can enhance the performance and increasing robustness. Generally, a biometric system is relatively secure against spoofing attack.

However, under worst case scenario, many other attacks could be used to gain unauthorized access. Robustness of the proposed biometric system against various attack under worst case scenarios is as follows.

a) **Brute Force Attack at initial point of authentication:** In this case, the imposter is not in possession of any genuine biometric. Therefore, it is necessary to search all the combinations of input space. Assuming the size of a single image is mn, the total brute force complexity will be v^{jmn}, where v is the range of a single pixel and j is the number of modalities. Using the values of $v = 256$, $j = 3$, $m = n = 150$, the maximum complexity is 540K bits. Hence, this attack is highly impossible to mount on the proposed biometric system.

b) **Known Key Attack:** This attack can also be referred to 'insiders attack' as the imposter is in possession of the keys but the genuine biometrics are concealed. Imposter offers his/her biometric instead of the original biometric. However, the success rate of this attack in terms of error rate is only 2.32 % as shown in Table 3.4. Hence, the error rate of this attack is equal to the false acceptance ratio, which can be reduced by changing the threshold.

c) **Key Substitution Attack with recorded biometrics:** In this attack, the imposter is in possession of the original biometrics but the keys are secure from the attacker. For a successful attack, the imposter will have to find majority of keys such that the biometric attack is successful. For the proposed biometric system, the success of this attack is very unlikely, as the attacker will have to estimate all the bits with high accuracy making the maximum complexity of this attack equal to $3Kmn$ bits. Where K is the number of keys and mn is the image

size. The EER obtained in this case is 0% due to the transformation provided by key features.

d) Template Substitution Attack with unknown keys: In this case the imposter who has access to the database can substitute a fake template to gain unauthorized access. However, in the proposed biometric system, this attack will not be successful, as the transformed feature vectors will not match the substituted template. This is because the keys used to transform the features are different than the keys used to construct the substituted template. The EER in this case will be 0%, as the imposter will not be authenticated.

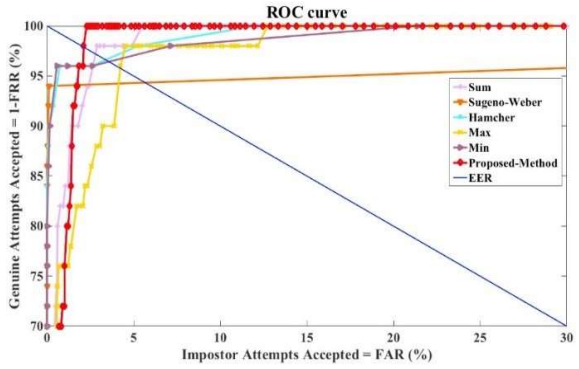
e) Template Substitution Attack with known keys: This is also an 'insiders attack' and the worst-case scenario, in which an imposter is in possession of the keys as well as the database. In this attack, this imposter will substitute a false template generated using the original keys. This success rate of this attack is equal to the accuracy of the biometric system. The keys should be replaced and database should be secured as soon as this attack is discovered. However, in the proposed biometric system, it is still not possible to retrieve the original biometrics from the database.

Therefore, the proposed biometric system is relatively secure from brute force and substitution attacks due to utilization of keys and the transform the initial features using the cross-diffusion process. In addition, generated cancelable templates for the proposed biometric system are not only non-inevitability but also revocability. The qualitative results are also augmented by various quantitatively results. In the next

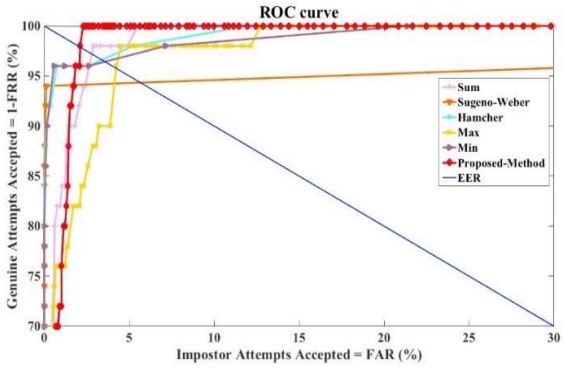
section, quantitative analysis of proposed biometric authentication system is given. Also various existing score fusion techniques viz. SUM, Sugeno-weber, Hamacher, MIN, MAX were implemented on local feature vector scores and compared with proposed multimodal system, which uses cancelable features.

3.5 Quantitative Analysis

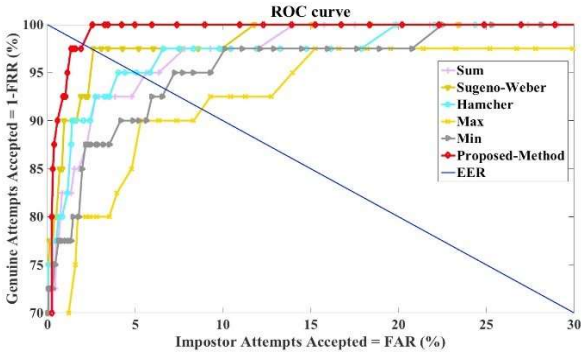
Biometric systems are compared and characterized quantitatively using Equal error rates (EER)obtained from ROC curves and accuracy. High accuracy and low EER is favourable when high performance is required during deployment of the biometric system. For comparing the performance of the proposed multimodal fusion technique, various existing score fusion techniques on local feature vectors scores are evaluated. Local feature vector scores are calculated by matching local features of the object with similar templates stored. Finally, proposed multi-stage multimodal fusion scheme is evaluated on four virtual datasets. Table 3.4 and Table 3.5 show EER and Accuracy of various score fusion techniques. Further, ROC curves shown in Figure 3.3 are plotted for different score fusion techniques.



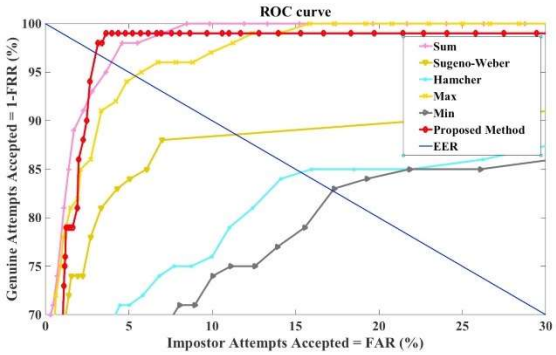
(a) Dataset 1



(b) Dataset 2



(c) Dataset 3



(d) Dataset 4

Figure 3.3 : Comparison of ROC curves for different fusion models viz. SUM, Sugeno-Weber, Hamacher, MAX, MIN, Proposed Method: (a) Dataset 1 (b) Dataset 2 (c) Dataset 3 (d) Dataset 4

Table 3.3 : Comparison of EER values for different fusion models

Modality	Sum[45]	Sugeno-Weber[46]	Hamacher[21]	Max[45]	Min[45]	Proposed Method
Dataset 1	2.4	3.0	3.7	4.0	3.6	**2.00**
Dataset 2	6.2	4.6	4.9	8.6	6.3	**2.50**
Dataset 3	5.3	2.5	5.0	9.1	7.0	**2.20**
Dataset 4	4.32	9.5	15.48	5.38	17.16	**2.58**
Average	4.5	4.9	7.27	6.77	5.15	**2.32**

Table 3.4 : Comparison of Accuracy values of different fusion models

Modality	Sum	Sugeno-Weber	Hamacher	Max	Min	Proposed Method
Dataset 1	97.632	97.938	97.776	96.877	97.755	**98.878**
Dataset 2	94.849	96.748	95.546	92.271	94.201	**97.832**
Dataset 3	95.32	97.500	95.833	92.468	94.199	**98.814**
Dataset 4	96.82	91.86	85.28	95.10	83.28	**97.74**
Average	96.15	96.00	93.60	94.179	92.35	**98.316**

EER is obtained from ROC curves of different fusion techniques. As shown in Table 3.4, On Dataset 1, Proposed method gives lowest EER of 2.0 followed by SUM score fusion method which gives an EER of 2.4, MAX performs worst in this case with an EER of 4.0, Further, optimal fusion of scores obtained by enhanced features lead to less equal error rate. Similar trend is observed in Dataset 2, Proposed fusion model gives an EER of 2.50, followed by Sugeno-Weber which gives an EER of 4.6, MAX fusion rule gives worst fusion performance with EER of 8.6. In dataset 3, the EER of statistical fusion methods vary from 2.5-9.1. Finally, in Dataset 4, maximum EER of 17.16 and minimum of 4.5 among multimodal fusion techniques as compared to proposed approach which gives a value of 2.58

Further, proposed method gives an average EER of 2.32. Worse performance in case of statistical fusion method can be explained by the fact that the scores of local features are unreliable. As shown in previous section, Variance in genuine and imposter score distribution is high in case of local feature scores. Hence, low genuine and high imposter scores limit the performance of Statistical score fusion. In contrast, proposed method uses cancelable features obtained using cross diffusion.
Average accuracy of proposed method is 98.316. Different fusion methods follow by 97.395 achieved by Sugeno-weber, MAX achieves worst performance giving an average accuracy of 93.872 only. Enhanced performance of proposed fusion method can be explained by usage of reliable cancellable features. Also, multistage Score fusion further increases the performance. The experiments prove that proposed model effectively combines modalities. However, the increase in accuracy and does not come with a significant trade-off in computational time. The computational time for different fusion models are tabulated in Table 3.6. In order to overcome stochastic nature, computational time for 25 runs of the proposed algorithm have

been determined. The average computational time for the proposed algorithm is 2.119 sec which depicts its real time application. This marginal increase in computational time of the proposed algorithm is mainly attributed to cross diffusion process for generation of cancelable features and to iterative cuckoo search optimization as used in fusion model. This small addition in computational time comes with a significant increase in performance of biometric system in terms of both accuracy and security. However, this computational time can be reduced either through usage of high end dedicated embedded system or through source code optimization.

Table 3.5 : Comparison of Computational time of different fusion methods

Biometric system	Total computational time(s)
Sum[45]	1.634
Sugeno-Weber[46]	1.854
Hamacher[21]	1.894
Max[45]	1.753
Min[45]	1.784
Proposed method	2.119

3.6 Significant Findings

The significant highlights of this research work are as follows:

- A multimodal biometric system has been proposed which is based on the combination of multiple modalities and optimal score level fusion.

- The proposed scheme is highly secure and hence, suitable for real time application.

- The generated cancelable templates are easily revocable and the use of Graph random walk cross diffusion achieves high security in the proposed biometric system.

- In addition, multistage fusion model determines optimal confidence factors for each classifier. Classifier beliefs are suppressed for discordant classifiers, boosted for concurrent classifier and conflict is optimally resolved among conflicting classifier beliefs using PCR-6 rules to achieve a final score.

- The proposed multimodal biometric system shows an expert system with applications where security is critical to the usage.

- Optimal score fusion applied on cross-diffused features produce better results than existing state-of-the-art multimodal fusion schemes.

The experimental results along with other findings were published in [71].

Chapter 4

Biometric Cryptosystems based on Key Binding

The objective of this work is to introduce novel approach for protection of data using biometric crypto system. For this, the secret key is bound with the biometric data of the legitimate user by minimizing the chosen objective function. New objective function has been defined in such a way that if the cryptographic key is split in several parts, then each part could be associated to one of the local minima of the objective function under certain conditions.

4.1 Introduction

Biometric cryptosystem provides a solution for securing the cryptographic key by binding the secret key with user biometric data. Protection of data has been recently investigated extensively due to proliferation of digital communication. Key binding based crypto systems have emerged as promising solution due to ease of usage and its adaptability. The scientific community all over the world have proposed various key binding mechanisms to secure the key from unauthorized persons by using user biometrics.

The first method for biometric key binding 'Mytec1' was developed by using fingerprint images [72]. This method was not very robust in providing security and accuracy. So, an enhanced version of Mytec 1 named as Mytec 2 was developed using a different filter function. Filter function was determined by finding the degree of similarity between a given biometric image and query image. Juels and Wattenberg introduced fuzzy commitment scheme based on binary biometric features to protect cryptographic keys [73]. In this method Reed-Solomon codes were used for error correction. Juels and Sudan proposed Fuzzy Vault scheme in which a cryptographic key was protected by binding it with fingerprint data [74]. In this scheme, a vault was created with the help of ECC and a polynomial based encoding method. Coefficients of the polynomial were taken from the secret-key that is to be secured. Additionally, some chaff points were randomly generated and merged with vault so that the original points could be secured. These chaff points should not overlap with the original points. Various methods for generation of distinct chaff points are given in [75] [76] [77]. The first such method for generation of Chaff points were given by Juels and Sudan [74]. Clancy et al., proposed a method in which chaff points were generated in such a way that the Euclidean distances among themselves as well as with previously generated chaff points and original points, exceed a pre-defined threshold value [78]. Li et al., developed a fingerprint cryptosystem which was alignment-free [79]. In this, minutia structure, minutia descriptor and local features were fused by employing three fusion strategies. Volume of the minutia descriptor was compressed by using Huffman coding. Marino et al., proposed a fuzzy extractor scheme in which key binding was done using iris template of the user [80]. Experimental results reveals that the most optimal size of the secret key that is to be secured is 192 considering FAR and FRR values.

M. Salas proposed elliptic curve cryptography based biometric encryption method for enabling biometric authentication in smart devices [81]. One of the main advantages of using ECC in providing security is that the memory requirement and execution time reduces significantly. Moreover, since instead of using user password it uses hash function which makes it quite resistant to several cryptographic attacks. A biometric based key authentication mechanism using ECC was developed by Yoon and Yoo for wireless sensor network [82]. This method claims to provide a secure and efficient wireless sensor network. Liew et. al. proposed a bio-cryptographic scheme in which chaotic encryption was done using Bernoulli-logistic mapping [83]. Absolute coefficients sum (ASC) of this approach was found to be quite low as compared to logistic map. This method got its wider applications in online biometric data network encryption and information transmission. Eskander et al., presented a fuzzy vault scheme in which offline signature images of the users were taken to resolve the key management issue [84]. Besides this, it can also be used for signature verification in different usage contexts. Another feature of this approach was that signatures could be revoked if they get compromised. Amirthalingam and Radhamani proposed a chaff point based fuzzy vault scheme [85]. In this method, optimal locations of the chaff points were found by employing particle swarm optimization algorithm. Chitra and Sujitha proposed a fuzzy vault scheme in which vault was created using pre-aligned minutia points and secret key [86]. This method was found to be secured against brute force and correlation attacks. Elrefaei et al., proposed a fuzzy commitment method in which gait features of users were extracted through Machine Vision Sensor for providing security [87].

PCA was used for dimensionality reduction and BCH coding scheme was applied to encode the cryptographic key. Ponce-Hernandez et al., proposed a fuzzy vault

scheme in which 15 global features of fixed-length signature template of the user were considered [88]. This method provides a robust solution against cryptanalytic attacks while maintaining a high level of accuracy. Asthana et al., proposed a multimodal biometric system wherein a robust template is generated by diffusion of individual transformed matrices [71]. Walia et al., proposed Deep Feature Unification (DFU) based cancelable biometric system. In this, key images based generic feature extraction has been given to revoke the template [89]. Asthana et al., proposed an adaptive fusion model to cater object rotation and scaling through a random walk state model and rotation invariant features [90]. Non-adaptiveness of multimodal systems to dynamic environment was addressed by adaptively combining the scores from individual classifiers [91].

Chenggang et al., worked on multi-view deep neural network and designed an efficient retrieval model [92]. In this, authors proposed a model which enhances the multi-view information through neural networks. Chenggang et al., also devised an optimized learning strategy to obtain the graph Laplacian matrix, which reflects the topological structure of image [93].

A novel technique to automatically identify the layout topology of an input image, followed by a nonlinear optimization with equality constraints to estimate the final 3D layout of a scene was introduced in [94]. Ouyang et al., developed a model that uses a feature extraction module and a novel distributional up sampling module [95] [96]. Albakri and Mokbel proposed a convolutional neural network face recognition as a tool to extract biometric features that help in a key binding approach to protect the personal data in the wallet [97]. Uludag et al. discussed the challenges involved in

biometric key generation due to imperfect nature of biometric feature extraction and matching algorithms [98].

In summary, although key binding based crypto system for data protection has extensively been studied. Most of the methods could not be adapted to different type and dimension of biometric data along with size of key. For instance, in order to augment the security of any cryptographic system, the secret key should be taken of a large size but an increase in key-size may deteriorate the performance of the system. Therefore, there is a requirement of developing such biometric cryptosystem for key-binding which should be able to bind a large key and retrieve the same efficiently. In order to address these issues, a novel approach for protection of data is proposed. The details of proposed approach are described in the next section.

4.2 Proposed Biometric Cryptosystem

A novel biometric crypto system involving key binding mechanism is proposed here. New objective function has been defined in such a way that if the cryptographic key is split in several parts, then each part could be associated to one of the local minima of the objective function under certain conditions. These conditions are

(i) Biometric traits should have low intra-class variability but high inter-class variability. Therefore, biometric templates for the same subject at multiple instances should not have much dissimilarity while the dissimilarity should be high if templates are taken from different subjects.

(ii) The starting point in the search space should be taken in such a manner that it should lead to convergence to one of the local minima of the objective function.

A block diagram of the proposed biometric crypto system based on key binding is shown in Figure 4.1.

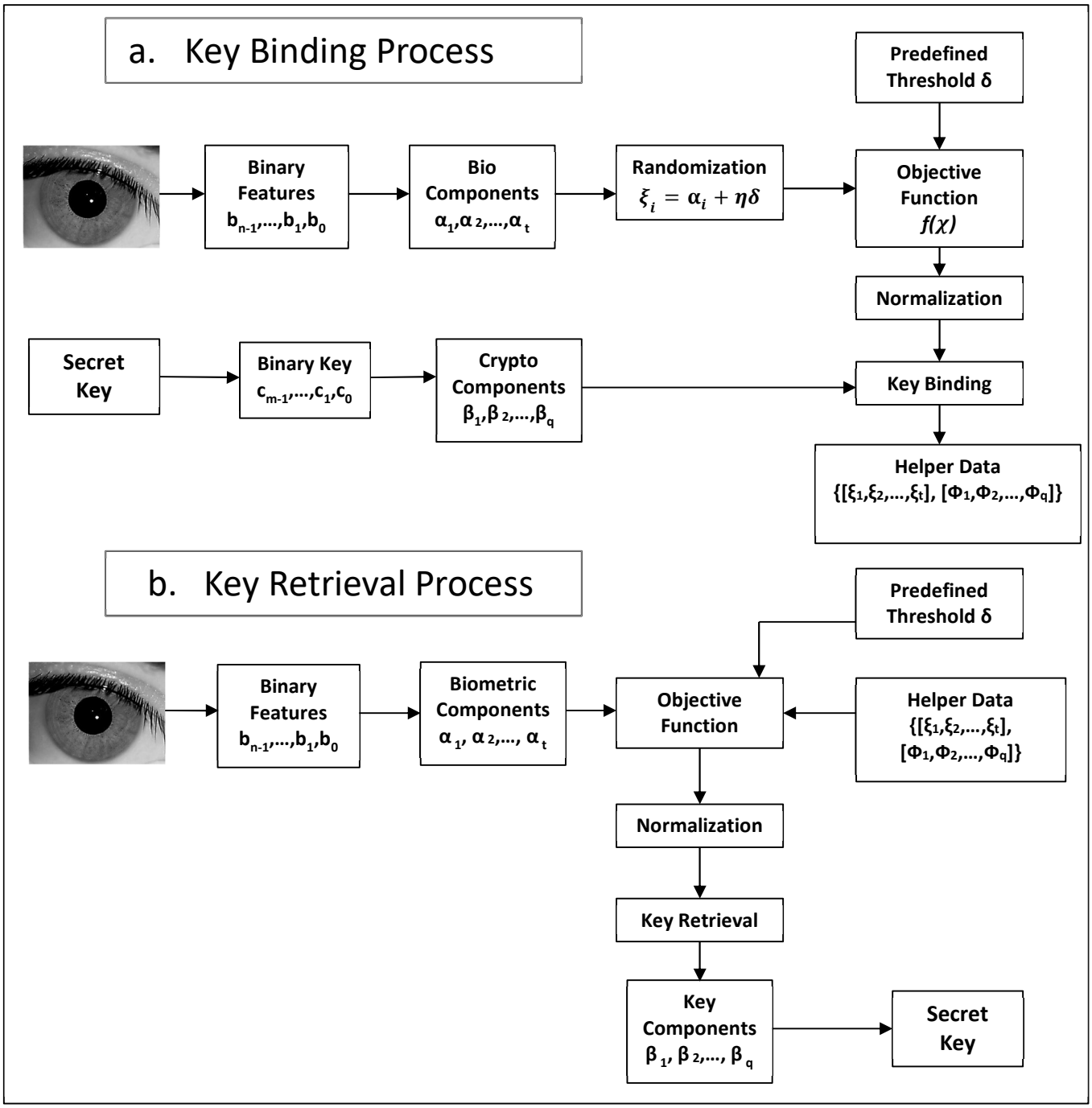


Figure 4.1 : Proposed Biometric Crypto system (a) Key Binding Process takes biometric

In the proposed approach, design of objective function plays a crucial role in convergence to local minima in finite number of steps. So, objective function should be highly regular so that the local minimum of the objective function associated with any segment of biometric data should be indistinguishable from all other minima. These functions should also be numerically stable so that little deviations in the initial data should not lead to different local minimum than the desired one. Moreover, a very few parameters should be required to define the shape of the objective function. Also, biometric bit-stream is divided into several components. Corresponding to each of these components, there are separate objective function defined in such a way that each bit-stream segment will correspond to one of its local minima. This will happen only if the initial points are taken in proximity of the original biometric data. Otherwise, minimization procedure will lead to a different local minimum and an attacker would not be able to notice the error committed. In the proposed approach, an objective function has been formulated as :

$$\varphi = f(\chi) = \frac{1}{\delta}[\chi - (\alpha + \eta\delta)] \sin\left[\frac{1}{\delta}\{\chi - (\alpha + \eta\delta)\}\right] \quad \ldots(1)$$

where 'α' represents a biometric component, 'η' a random value and 'δ' the neighbourhood threshold value for which the value of the function $\boldsymbol{f}$ converges to a local minimum. Since the value of local minima of $f(\chi)$ increases as χ increases, it is normalized using Eq. (2).

$$\psi_i = |\varphi_i| . 10^{-\lfloor log_{10}(|\varphi_i|) \rfloor} \quad \ldots(2)$$

The following two main processes are involved in the proposed biometric cryptosystem : Key Binding Process and Key Retrieval Process

4.2.1 Key Binding Process

In Key Binding process, secret cryptographic key is bound with the user biometric data. Consider the Secret key K which is to be protected is of length m and represented as m-bit sequence $K = c_{m-1}\, c_{m-2} \ldots c_0$. p and q are integers chosen in such a way that $m = p*q$. Further, q sub-sequences K_i each of length p bits are formed by partitioning the key K. Therefore, the secret key is represented as $K = K_q, K_{q-1}, \ldots, K_1$ where each sub-sequence is of length p. By taking integer value β_i referred to as 'Crypto component' corresponding to each of these q sub-sequences a set $\{\beta_1, \beta_2, \ldots, \beta_q\}$ is formed. This set may be referred to as 'Crypto Key'. If m is not multiple of q then the last crypto-component is padded with the required number of random bits to make its size p.

Similarly, consider B is a finite bit sequence of a particular biometric of the user of length n represented as $B = b_{n-1}\, b_{n-2} \ldots b_0$. s and t are integers chosen in such a way that $n = s*t$. Biometric B could be partitioned into t sub-sequences each of length s bits. Therefore, the biometric may be represented as $B = B_t, B_{t-1}, \ldots, B_1$ where each sub-sequence is of length s. By taking integer value α_j referred to as 'Bio component' corresponding to each of these t sub-sequences a set $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ can be formed. This set may be referred to as 'Biometric Key'. If n is not a multiple of s, then the last $(n-s*t)$ bits of the biometric bit-sequence are discarded. Therefore, the Biometric Key $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ and Crypto Key $\{\beta_1, \beta_2, \ldots, \beta_q\}$ are formed.

If α_i is a bio-component, then

$$\xi_i = \alpha_i + \eta\delta \qquad i \in \{1,2, \ldots, t\} \qquad \ldots(3)$$

where 'η' is a random value and 'δ' is the neighbourhood threshold value for which the value of the function *f* converges to a local minimum.

For each α_i , the value φ_i of the objective function is computed as given below

$$\varphi_i = f(\alpha_i) = \frac{1}{\delta}[\alpha_i - \xi_i] \sin\left[\frac{1}{\delta}\{\alpha_i - \xi_i\}\right] \quad i \in \{1,2,\dots,t\} \qquad \dots(4)$$

The values of the local minima increases in proportion to the value α_i , therefore the values ψ_i are normalized as follows

$$\psi_i = |\varphi_i|.10^{-\lfloor log_{10}(|\varphi_i|) \rfloor} \qquad \dots (5)$$

Number of bio-components are required to be equal to the number of crypto-components as each crypto-component is to be bound with a bio-component. In the case where the number of bio-components is larger than the number of crypto-components, methodology is required to form a subset of q bio-components which can be associated with each crypto-component. For this, the median value **v** of the t local minima ψ_i can be calculated using the above defined objective functions. Then the distance between each bio-component and the median is computed and sorted in the ascending order. From this, the first q bio-components which are termed as anchors.

If there are only fewer numbers of bio-components for binding the crypto-components, then the average value of the t local minima μ is computed. Then $\mu.\psi_i$ are taken as the values of the anchors. The normalized values of φ_i are then used to bind the secret key with the biometrics of the user in the following manner

$$\phi_i = \beta_i / \Upsilon_i \quad \ldots(6)$$

$$\text{where} \quad \Upsilon_i = \psi_i . \mu \quad \ldots(7)$$

In this way, the secret key is bound with the biometric data of the user and a helper data HD ={[$\xi_1,\xi_2,\ldots,\xi_t$], [$\Phi_1,\Phi_2,\ldots,\Phi_q$]} is formed which along with the pre-defined threshold value 'δ' is used to retrieve the secret cryptographic key.

Pseudocode of the Proposed Key Binding Method

---

1. **Function** Key_Binding (***B***, ***K***, **δ**)
2. {$\alpha_1, \alpha_2, \ldots, \alpha_t$} = *Derive biocomponent (**B**)*
3. {$\beta_1, \beta_2, \ldots, \beta_q$} = *Derive biocomponent (**K**)*
4. η = Generate random number (seed)
5. for (i = 1 to t)

   Randomize Bio-components α_i using Eq. (3)
   Determine φ_i by computing value of objective function f(α_i) using Eq. (4)
   Determine ψ_i by normalizing objective function output φ_i using Eq. (5)
   end
6. Determine μ = Mean (ψ_i), ν = Median (ψ_i)
7. Calculate L=sort([$\psi_1,\ldots,\psi_t$] wrt |ψ_i-ν|)
8. Determine T = truncate(L,t-q) to keep first q values
9. for (i = 1 to q)

   Compute Υ_i using Eq. (7)
   Compute ϕ_i using Eq. (6)

   end

10. *Generate Helper Data* ***HD*** = {[$\xi_1,\xi_2,\ldots,\xi_t$], [$\Phi_1,\Phi_2,\ldots,\Phi_q$]}

11. Return (***HD***)

4.2.2 Key Retrieval Process

In Key Retrieval process, this process, biometric keys {α_1, α_2, …, α_t} of the user is used to retrieve the key from the helper data *HD* =={[$\xi_1,\xi_2,\ldots,\xi_t$], [$\Phi_1,\Phi_2,\ldots,\Phi_q$]}. For this, pre-defined value of threshold value 'δ' is chosen to ensure optimal retrieval of key.

The process is as follows : Using the user biometric and helper data values φ_i of the objective function are computed using Eq (8).as given below

$$\varphi_i = f(\alpha_i) = \frac{1}{\delta}[\alpha_i - \xi_i] \sin\left[\frac{1}{\delta}\{\alpha_i - \xi_i\}\right] \quad i \in \{1,2,\ldots,t\} \qquad \ldots(8)$$

These values are then normalized as

$$\psi_i = |\varphi_i|.10^{-\lfloor log_{10}(|\varphi_i|)\rfloor} \qquad \ldots(9)$$

In the case where the number of bio-components is larger than the number of crypto-components, methodology is required to form a subset of q bio-components which can be associated with each crypto-component. For this, the median value **v** of the t local minima ψ_i is calculated using the above defined objective functions. Then the distance between each bio-component and the median is computed and sorted in the ascending order. From this, the first q bio-components which are termed as anchors.

If there are only fewer numbers of bio-components for binding the crypto-components, then the average value of the t local minima μ is computed. Then $\mu.\psi_i$ are taken as the values of the anchors. The normalized values of φ_i are then used to retrieve the secret key with the help of the helper data in the following manner

$$\beta_i = \phi_i \,.\, \Upsilon_i \qquad \ldots(10)$$

$$\text{where } \Upsilon_i = \psi_i.\mu \qquad \ldots(11)$$

From all the crypto-components thus computed, the secret cryptographic key K can be reconstructed back whenever required.

Pseudocode of the Proposed Key Retrieval Method

---

1. **Function** Key_Retrieval (***HD***, ***B***, δ)
2. $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ = *Derive biocomponent (**B**)*
3. for (i = 1 to t)

   Determine φ_i by computing value of objective function $f(\alpha_i)$ using Eq. (8)
   Determine ψ_i by normalizing objective function output φ_i using Eq. (9)

   end
4. Determine μ = Mean (ψ_i), ν = Median (ψ_i)
5. Calculate $L = sort([\psi_1, \ldots, \psi_t]\ wrt\ |\psi_i - \nu|)$
6. Determine $T = truncate(L, t - q)$ to keep first q values
7. for (i = 1 to q)
   Compute Υ_i using Eq. (11)
   Compute β_i using Eq. (10)

   end

8. *Generate Key* $\boldsymbol{K} = \{\beta_1, \beta_2, \ldots, \beta_q\}$

9. Return ($\boldsymbol{K}$)

The proposed system has been experimentally validated on benchmark datasets. Details of experimental analysis have been given in the following section.

4.3 Experimental Validation

Qualitative as well as Quantitative analysis of the proposed biometric crypto system have been done on benchmark datasets for Iris and Fingerprint modalities. Security analysis of the proposed method has been performed. Performance metrics which have been used for evaluation of the proposed scheme include False Acceptance Rate (FAR), Genuine Acceptance Rate (GAR), Genuine Wrongly Decoded bit Rate (GWDR) and Imposter Wrongly Decoded bit Rate (IWDR). Proposed scheme has been implemented using MATLAB on a PC having 8GB RAM and Intel i5 processor.

4.3.1 Database for Experimentation

Biometric data chosen for evaluation is benchmark datasets with low intra-class variability. Apart from this, chosen data is considered to be uniformly distributed over the feature space. John Daugman in his study showed that the Iris biometric possesses these two important characteristics [99]. For the experimental validation of the proposed method, iris biometric taken from IIT Delhi Iris database has been considered. This database has been created with iris biometrics of 224 persons IIT Delhi [100]. These images are in bitmap (*.bmp) format. The fingerprint biometric

database CASIA-Fingerprint V5 have been taken for performance analysis of the proposed method [101]. The sample images from these datasets are shown in Figure 4.2(a) & 4.2(b).

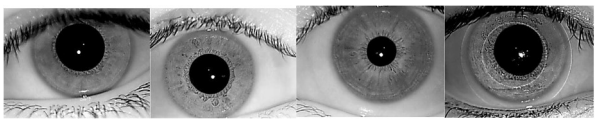


Figure 4.2(a): Sample images from IIT Delhi database

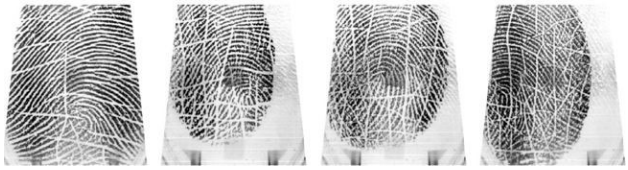


Figure 4.2(b): Sample images from CASIA-FingerprintV5 database

4.3.2 Performance Evaluation Metrics

The proposed scheme has been quantitatively analysed by using following performance evaluation metrics :

(a). False Acceptance Rate (FAR): FAR is the measure of the error committed by the system when an unauthorized user is given access. [Refer Section 2.7.1]

(b). Genuine Acceptance Rate (GAR): This metric assesses the capability of the system in correctly matching the biometric data from the same individual. [Refer Section 2.7.3]

(c). Genuine Wrongly Decoded bit Rate (GWDR): This is the wrongly decoded bit rate between the actual secret key K and the reconstructed key K' by

the genuine user [102]. To calculate this the hamming distance between K and K' is considered as per the following formula

$$GWDR = \frac{HD(K, K')}{|K|}$$

(d). Imposter Wrongly Decoded bit Rate (IWDR): This is the wrongly decoded bit rate between the actual secret key K and the reconstructed key K' by an imposter [103]. To calculate this the hamming distance between K and K' is taken into account as per the following formula

$$IWDR = \frac{HD(K, K')}{|K|}$$

4.4 Performance Analysis

Performance analysis is performed both qualitatively and quantitatively. The two main parameters of the proposed technique are neighbourhood threshold and random noise. The first experiment was carried out to study the effect of noise η_i and neighbourhood threshold δ on the convergence stability of the objective function. For this, noise η_i in the range [1,40], neighbourhood threshold δ in the interval [1,40] and biometric-components a_1, a_2 ,..., a_{128} in the range [0,240] were taken. Secret key K of four different lengths viz., 256, 512, 1024 and 2048 were randomly generated for binding with the biometric data. The cryptographic key was bound with the biometric data through the proposed method and helper data was created. Then the cryptographic key was reconstructed by using noisy bio-components ($\alpha_i + \eta_i$). This whole process was performed several times and the success rates of the proposed methodology were recorded. The results have been shown in the Figure 4.3 for

cryptographic keys of sizes 256, 512, 1024 and 2048 bits. The 3D plots of the success rate, amount of noise and neighbourhood threshold values have been shown.

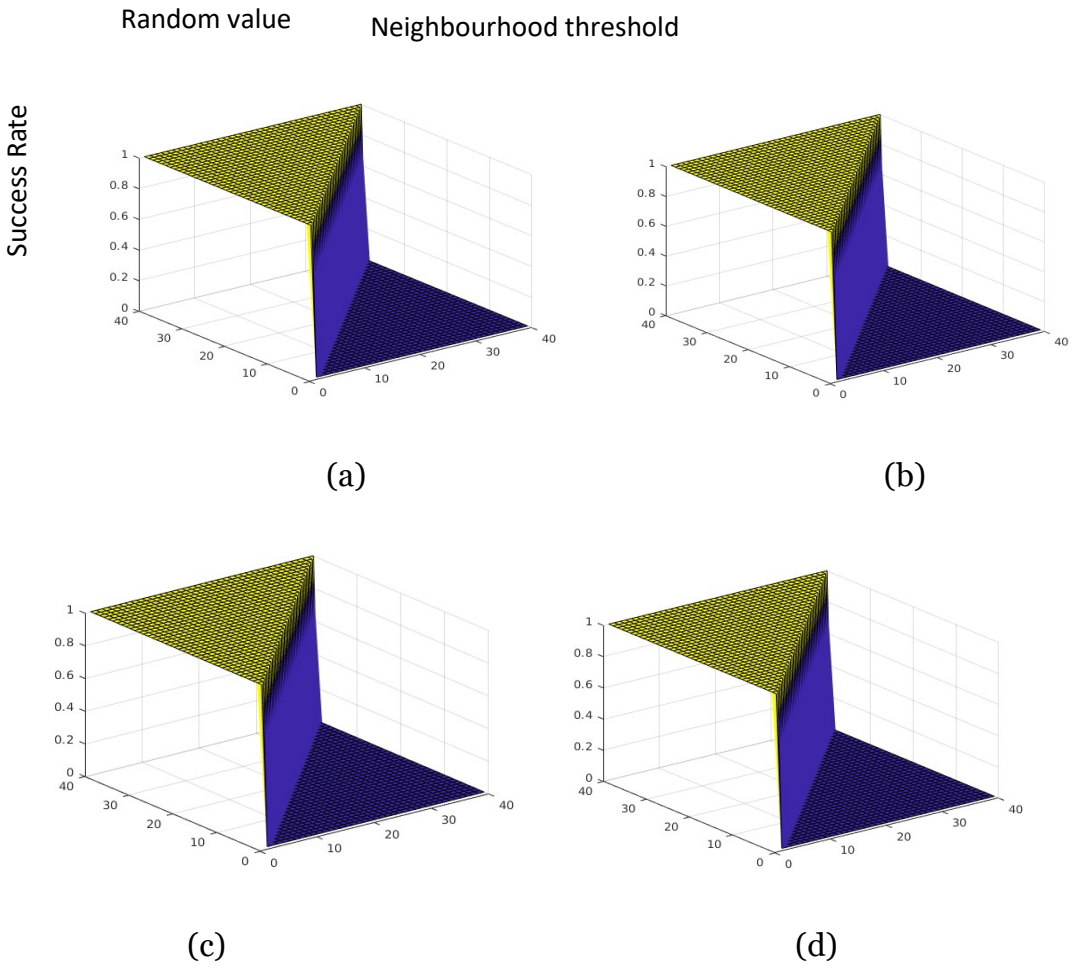


Figure 4.3: Effect of change in neighbourhood threshold and random value on the success rate of the proposed method for key sizes of (a) 256 bits (b) 512 bits (c) 1024 bits, (d) 2048 bits

The above results show that the proposed method consistently achieves good success rate even with some changes in the neighbourhood threshold values and some amount of randomization in the input values to the objective function. This means that the technique offers flexibility with regard to variation in the input biometric feature values, caused by different environmental and physical conditions. The two main parameters of the proposed technique are neighbourhood threshold and

random noise. An assessment was done as to how these parameters affect the success rate of the biometric crypto system and the result is shown in the Figure 4.3.

In the second experiment, the effect of the neighbourhood threshold values on the accuracy of the proposed method was studied for genuine users and impostors. Here, Chebyshev distances were computed for comparing each query template with all the available gallery templates. These comparisions were used for determining the optimum value of the threshold which helped in separating gennine from the imposters. Experimentation was performed on four key sizes viz., 256, 512, 1024 and 2048 bits. The results are shown in Figure 4.4.

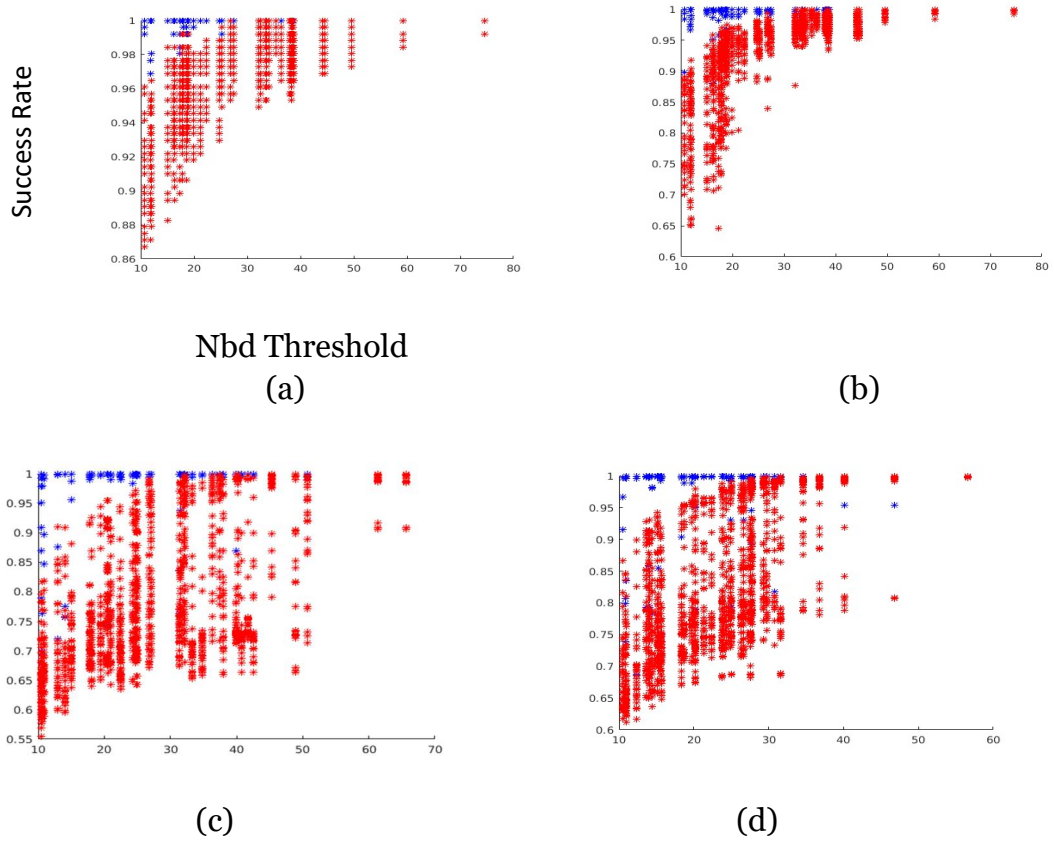


Figure 4.4: Effect of change in neighbourhood threshold on success rate for genuine users (blue dots) and impostors (red dots) for key sizes of (a) 256 bits (b) 512 bits (c) 1024 bits and (d) 2048 bits

The results obtained in this experiment illustrates that the success rate for genuine user is unaffected upto a certain value of neighbourhood threshold and there is a clear separation of correct key retrieval between genuine user and imposter. Results demonstrate the fact that the proposed key binding method ensures that the secret key can be retrieved successfully by the genuine user whereas the imposter is unable to get the secret key which was bound with the biometrics of the authorized user.

In the third experiment, performance analysis of the proposed method was done with respect to various performance metrics like FAR, GAR, Genuine WDR and Imposter WDR for various sizes of the secret cryptographic keys viz., 256, 512, 1024 and 2048 bits. These performance metrics have been computed for various neighbourhood values δ ranging between 28 and 32. Performance results in terms of FAR, GAR, GWDR and IWDR plotted for secret key of size 256 bits have been shown in Figure 4.5 for the IIT Delhi dataset.

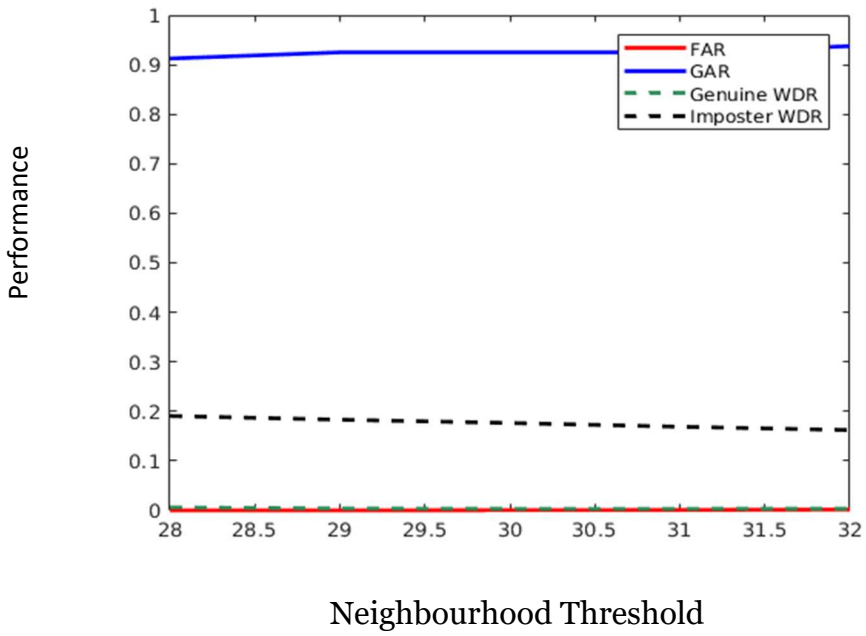


Figure 4.5: Performance results: FAR, GAR, GWDR and IWDR for neighbourhood threshold in the range [28, 32] for 256 bits keysize

The results obtained shows that there is not much variation in the FAR, GAR, GWDR and IWDR values if the neighbourhood threshold lies in the range [28, 32].

In the fourth experiment, the values of performance metrics like FAR, GAR, GWDR and IWDR were computed by fixing the neighbourhood threshold value δ to 30. These were computed for all the four key sizes and shown in the Table 4.1.

Table 4.1: Performance results on Iris datasets for different key sizes with δ = 30

Key-size	GAR (%)	FAR (%)	Genuine WDR (%)	Imposter WDR (%)
256 bits	95.00	0.0475	0.0391	1.81
512 bits	91.25	0.210	0.1100	3.38
1024 bits	86.25	1.95	0.7900	10.61
2048 bits	86.25	7.83	0.9400	17.62

This experiment was also carried out on another fingerprint database namely, CASIA-V5. Values obtained for performance metrics like FAR, GAR, GWDR and IWDR by fixing the neighbourhood threshold value to 30 are shown in the Table 4.2.

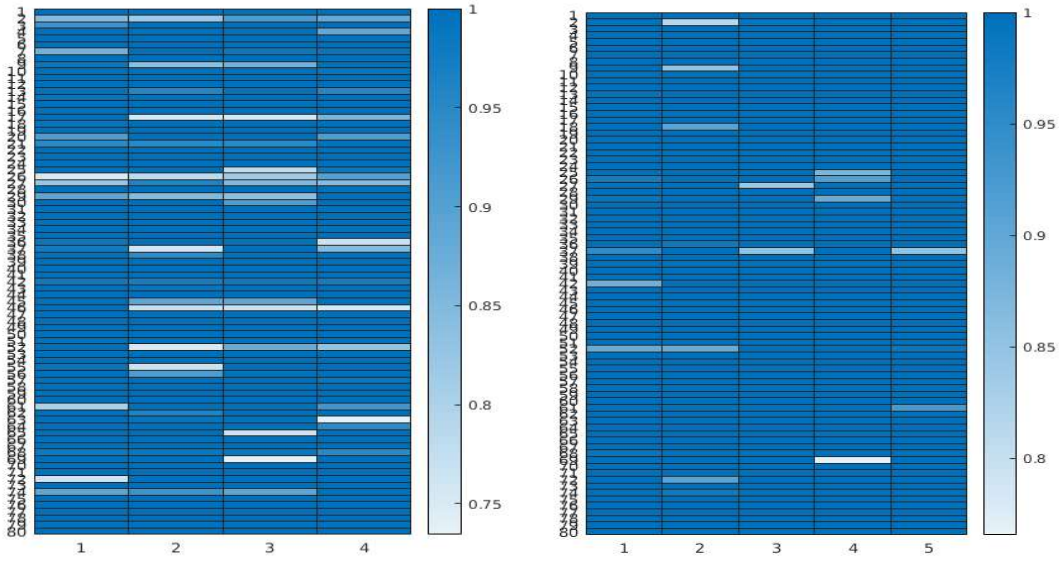
Table 4.2: Performance results on CASIA-V5 datasets for different key sizes with δ = 30

Key-size	GAR (%)	FAR (%)	Genuine WDR (%)	Imposter WDR (%)
256 bits	94.00	0.0509	0.0407	2.17
512 bits	90.63	0.316	0.1403	3.96
1024 bits	87.34	2.09	0.8300	11.54
2048 bits	86.55	8.543	0.9614	18.13

The result shows a high genuine acceptance rate and a very low false acceptance rate which is highly desired for such biometric cryptosystems. Moreover, wrongly decoded bit rate for genuine user is quite low which ensures retrieval of correct key.

Further, the heat maps were generated to assess how selection of gallery items i.e., templates stored in the database, affects reconstruction of secret key. For this, two cases were investigated. In the first case, five different bio-components were taken for each user. Out of these, one bio-component was used as gallery item whereas remaining four bio-components were used as probe items. The gallery item was used for binding the secret key whereas the probe items were used for reconstruction of secret key. The reconstructed key was compared with the original secret key. Heat map as shown in Figure 4.6(a) represents the respective scores of the comparison made in the interval [0,1]. Darker shade represents higher score. In this, each row represents a user's matching score for key regeneration using his 4 probe bio items.

In the second case, five different bio-components for each user were taken. But unlike the first case, here gallery bio item was formed by taking mean of the five bio-components of the user. This gallery bio item was used to bind the key and all the five bio-components were used to reconstruct the secret key. The recovered key was compared with the original key and corresponding heat map was generated with the help of the respective scores as shown in Figure 4.6(b). As shown, darker shade depicts higher obtained score.



(a) (b)

Figure 4.6: (a) Heat maps when gallery item is the actual bio-component (b) Heat maps when gallery item is the mean of the bio-components

Results show that performance of the proposed system is better when the mean of the bio-components are taken as the gallery item i.e., representative template, in comparison to the case where an individual bio-component was taken as the gallery item. Hence, the proposed approach for mean value of bio-components is appropriate solution.

4.5 Security Analysis

In security analysis of the proposed method, the robustness of the method against brute force attack and correlation attack has been investigated.

4.5.1 Resistance against Brute Force Attack

From equation (3), it is quite evident that the random value $\boldsymbol{r}$ plays a significant role in the value of $\boldsymbol{h_i}$ which ultimately leads to formation of helper data HD. As the

helper data is in public domain, the adversary tries to derive the cryptographic key with the help of the helper data. Attacker has access to values of $\boldsymbol{h_i}$ but in the absence of knowledge of random value $\boldsymbol{r}$, he would not be able to derive the values of bio-components $\boldsymbol{a_i}$ correctly. Values of $\boldsymbol{a_i}$ lies in the range [0, A], so the objective function has at least $n_{min} = \lfloor A/4\delta \rfloor$ local minima in this range. But only a particular minimum out of those will be corresponding to actual $\boldsymbol{h_i}$. As described earlier the biometric data of a user is split into $\boldsymbol{t}$ bio-components. So, there will be exactly $\boldsymbol{t}$ objective functions each of them having $n_{min} = \lfloor A/4\delta \rfloor$ local minima. Since the value of local minima increases as the value of x increases, there are values which would be some which would be more dominant than the others. Therefore, it is very essential that an attacker should arrive at correct local minimum for each of the $\boldsymbol{t}$ objective functions. This will require $(n_{min})^t$ trials. Therefore, brute force attack complexity will depend on the length of the biometric data of the user which is usually quite large. Hence, proposed approach exhibits strong resistance against brute force attack.

4.5.2 Resistance against Correlation Attack

In this attack, an adversary tries to derive crypto-components or bio-components by exploiting correlation if at all exists in multiple helper data created at multiple instances of protecting a secret key using a particular biometric data [104]. Suppose $HD_1 = \{[\xi_{11},\xi_{12},\ldots,\xi_{1t}], [\Phi_{11},\Phi_{12},\ldots,\Phi_{1q}]\}$ and $HD_2 = \{[\xi_{21},\xi_{21},\ldots,\xi_{2t}], [\Phi_{21},\Phi_{22},\ldots,\Phi_{2q}]\}$ are two such helper data where in the same crypto-component is hidden in two different pairs $(\Phi_1.Y_1)$ and $(\Phi_2.Y_2)$. Therefore, corresponding bio-component is derived by

identifying the correct local minima for which $\Phi_1.Y_1 = \Phi_2.Y_2$. But this is almost infeasible due to the following reasons

(i) It is difficult to identify which q local minima out of total t local minima, are associated with the coefficients.

(ii) Attacker would not be able to test the condition $\Phi_1.Y_1 = \Phi_2.Y_2.Y_{2i}$ for two different pairs $(\Phi_1.Y_1)$ and $(\Phi_2.Y_2)$, as q anchors in both the helper data HD_1 and HD_2 depend on the values of all the local minima.

The security analysis of the proposed method establishes the fact that the proposed approach is robust against brute force attack as well as correlation attack. Here, robustness means system is mathematically so strong that it can survive many cryptanalytic attacks mounted by the cryptanalysts.

4.6 Significant Findings

The significant highlights of this research work are :

- A novel biometric cryptosystem has been proposed for securing the cryptographic key wherein a secret key is bound with the user biometric data.

- New objective functions have been defined for creation of helper data by hiding the secret key. This helper data is subsequently used to retrieve the key.

- Proposed method consistently achieves good success rate even with some changes in the neighborhood threshold values and some amount of randomization in the input values to the objective function.

- Proposed key binding method ensures that the secret key can be retrieved successfully by the genuine user whereas the imposter is unable to get the secret key which was bound with the biometrics of the authorized user.

- The proposed biometric cryptosystem achieves a high Genuine Acceptance Rate and a very low False Acceptance Rate. Moreover, wrongly decoded bit rate for genuine user is quite low which ensures retrieval of correct key.

- Security analysis shows that the proposed biometric cryptosystem is quite robust against brute force attack and correlation attack.

- The helper data exhibits randomness property which ensures that adversary cannot predict or recover the secret key.

- A detailed performance analysis in terms of FAR, GAR, GWDR and IWDR shows that this method is very efficient. Its performance does not get affected with change of length of secret key and upto a certain amount of noise induction in the user biometric data.

The experimental results along with other findings were published in [105].

Chapter 5

Biometric Template Protection Schemes

In recent times, biometric based authentication systems have seen a tremendous growth in various applications. However, if databases in multiple applications are created using the same biometric characteristic and algorithm, then any compromise of the stored template in one biometric system may jeopardise the security of the other biometric systems as well. More importantly, such a compromise may also lead to a permanent loss of the biometric characteristic. Therefore, the cancelability or revocability of biometrics has become quite an essential requirement. The objective of this work is to design a novel biometric template protection scheme, the Random Area & Perimeter Method (RAPM)), in which a biometric characteristic of an individual is transformed into random values which are stored as cancelable biometric templates.

5.1 Introduction

A lot of research is being done in the field of Biometrics and Cryptology to address the vulnerabilities which are there in the biometric based systems. One of the most challenging areas is related to biometric template protection for which several techniques have been developed. Cancelable biometrics is one such concept in which the original biometric features/templates are not stored, rather their transformation

is done by one-way function and then they are stored [106]. Such one-way transformation ensures privacy as recovering the original biometric from the transformed one is computationally difficult. In some schemes the transformation is carried out in the original (raw data) domain while in others it is done in the feature domain [107]. The most important feature of cancelable biometrics is 'revocability'. This feature ensures re-enrolment of the biometric template by another one-way function when an already enrolled biometric template gets compromised [108]. The one-way function should be chosen in such a manner that the statistical characteristics of the resultant features should remain intact so that the matching accuracy does not degrade after transformation [109],[110],[111]. The transformation techniques are broadly categorised into Non-Invertible Transforms and Biometric Salting. One way function based on non-invertible transforms use user-key and biometric as input parameters [112]. In Biometric salting, the templates are distorted by salting them with an auxiliary data. Then some additional operations are performed on the blended data to achieve the condition of non-invertibility [113].

Davida et al. [114] started the work on Cancelable biometrics when they proposed a majority decoding scheme for iris biometrics. Ratha et al. [115] made significant contributions in concretizing the concept of Cancelable biometrics. Juels [116], [117] modified the error-correcting codes of the scheme proposed by Davida et al. and reduced the code size. Clancy et al. [78] developed a technique in which polynomial-based secret-sharing scheme based was used on a locking set created by the minutiae points of the fingerprint. Ratha et al. developed non-invertible transformations based cancelable fingerprint template schemes [39]. A transformation method on fingerprint minutiae using a user defined key, was proposed by Ang et al. [118], whereas a hash-based transformation method was developed by Tulyakov et al. [119].

A new authentication approach called Bio-Hashing was proposed by Teoh et al., wherein a biometric code is generated by combining biometric feature vectors with the tokenized random vectors specific to a user [120]. Biometric cryptosystems are another important concept where in cryptology is blended with biometrics to provide security [121]. Soutar et al. proposed the concept of bioscrypt in which fingerprint image is used to generate a biometric code [122]. Sadhya et al. generated secure, cancelable iris features through locally sensitive hashing [123].

Live fingerprints were determined by exploiting the quality of fingerprint features by Sharma et al. [124]. Minutiae information from fingerprint were modified using a key set by Ali et al. to produce cancelable biometric [125]. Cancelable biometric were generated from fingerprint by Trivedi et al. by using binary key provided by the user [126]. Wu et al. applied the method of signal subspace collapsing on ECG biometric to generate revocable biometric templates [127]. Kumar et al. introduced the concept of Random Permutation Principal Component Analysis (RP-PCA) to generate cancelable biometric using face, iris, and ear modalities [128]. Dwivedi and Dey combined Mean-Closure Weighting (MCW) with Dempster-Shafer (DS) theory to develop a hybrid cancelable multi-biometric system [129]. The concept of cross-diffusion of graphs have been used by Walia et al. [71] to develop a cancelable biometric system. Random distance method for transformation of biometric features was given by Kaur and Khanna [130]. Key images were used by Walia et al. to generate cancelable templates [131]. Gomez-Barrero et al. [132] generated cancelable templates by using bloom filters on face-iris and face-finger vein. El-Samie et al. [133] applied bio-convolving encryption on face image to generate cancelable templates. Zuo et al. [134] proposed Gray salting method which works with

conventional iris recognition systems. A random-projection (RP)-based method was given by Wang et al. to transform biometric data using a random matrix [135].

Maiorana et al. proposed bio-convolving method which is a protected on-line signature-based biometric authentication system [136]. Lu Leng & Jiashu Zhang presented a 2D BioPhasor method in which cancelable palmprint coding frameworks are extended from one dimension to two dimensions [137]. Lu Leng et al. also proposed a novel cancelable palmprint template, called "PalmPhasor" [138]. Random Permutation Maxout (RPM) transform method was proposed by S Cho & A B Teoh wherein a template is transformed into a discrete index code as a means of protected form of face template [139]. H Kaur & P Khanna presented a template protection approach which generates revocable binary features [140]. They also proposed random slope methods for generation of cancelable features [141]. A random distance-based approach was presented by the same authors for protection of biometric templates [142].

Shengmin Xu et al. proposed a cryptographic primitive 'ElGamal type cryptosystem' which derive a variety of attribute-based encryption (ABE) schemes [143]. Yin et al. presented a novel concept of revocability in terms of decryption rights delegation [144]. A partial Hadamard transform to securely protect binary biometric representations in the design of cancelable biometrics was proposed by Wang et al. [145][146].

As described above, various approaches have been adopted for protection of biometric templates. However, there is a great scope for improvement in terms of dimensionality reduction, storage requirement and performance of the cancelable

template generation technique. Thus, a robust, non-invertible and revocable biometric template generation mechanism should be accorded top priority for the maximum usage of biometric based systems.

5.2 Proposed Biometric Template Protection Scheme

A new technique for the template protection is hereby proposed which addresses following security and privacy concerns:

(i) Biometrics are authentic but not secret: Despite the fact that most of the biometrics possess quite a personalized attribute, some of them can potentially be misused without the user's consent. In contrast, tokens and knowledge get compromised when user willingly shares them.

(ii) Biometrics cannot be cancelled or revoked: Knowledge-based authentication entities can be reset if they get compromised. Similarly, token-based items can be replaced if they are stolen. Biometric characteristics of an individual are of permanent nature and therefore they are non-replaceable or non-revocable if they get compromised.

(iii) Biometrics may be compromised forever: Biometrics provide usability advantages as passwords/identities are no longer needed to be remembered and their management becomes easier. However, compromise of a biometric in one application may lead to a compromise of all other applications where the same biometric have been used.

(iv) Individuals can be tracked by Cross-matching of Biometrics: In case, a particular biometric is used repeatedly in a number of applications and locations, there is possibility of tracking of individual when the concerned agencies collude and share the enrolled or registered biometric templates.

The proposed scheme computes area and perimeter of the Bezier curve which are obtained through interpolation of feature points of original biometrics and a random point chosen by the user. The area and perimeter thus computed exhibit pseudo-random properties. An architecture of the proposed cancelable biometric system is shown in Figure 5.1.

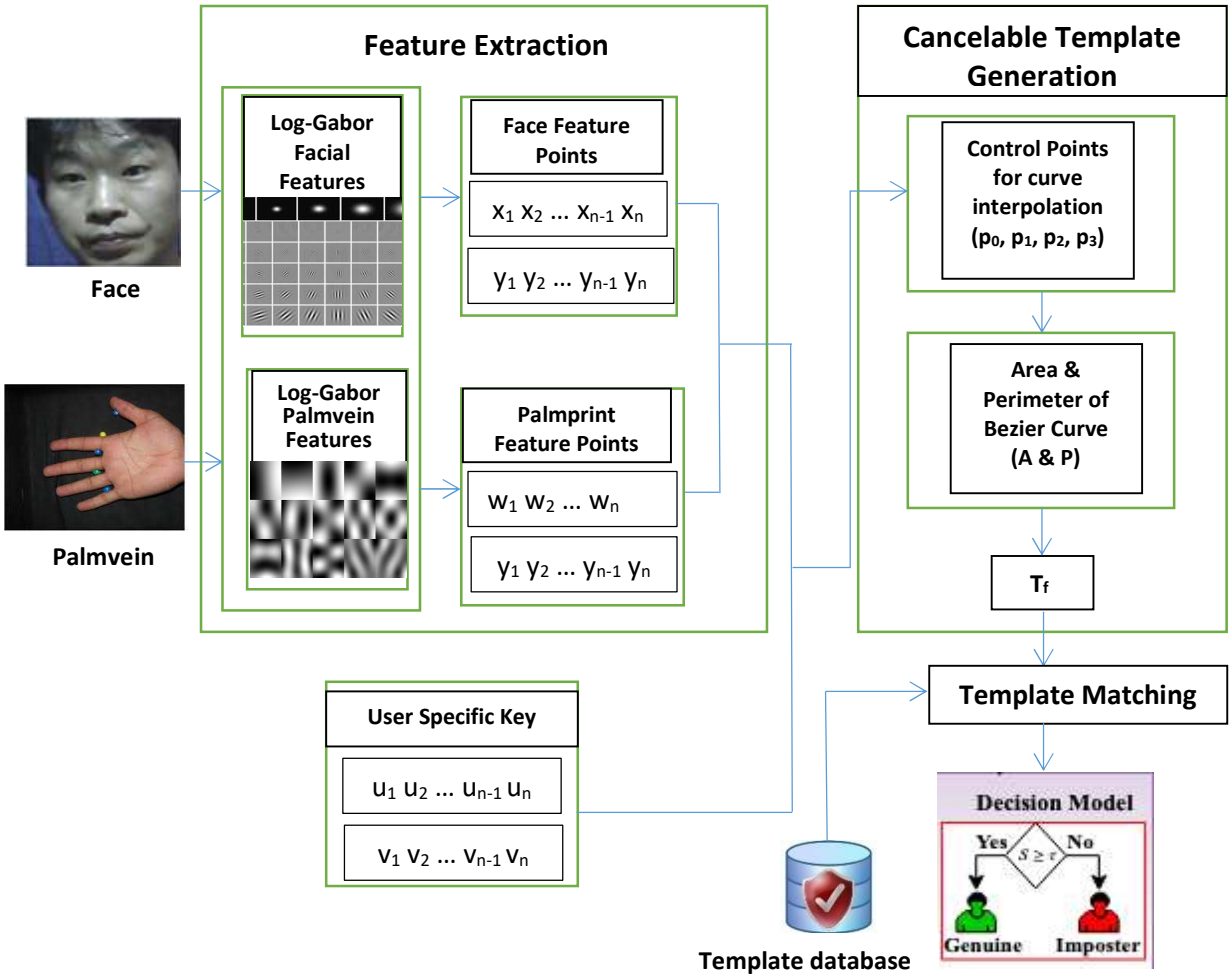


Figure 5.1 : Architecture of the proposed recognition system based on multi-modal biometric

As shown in the above diagram, in the proposed scheme two modalities e.g., face and palmvein, are taken. From these biometrics, features are extracted using Log-Gabor filters. The extracted features for the first modality are divided in to two sets e.g., $\{x_1,x_2,...,x_{n-1}, x_n\}$and $\{y_1,y_2,...,y_{n-1},y_n\}$. The corresponding values from both these sets are used to form features points. Similarly, the extracted features for the second modality are divided in to two sets e.g., $\{w_1,w_2,..., w_{n-1},w_n\}$ & $\{z_1,z_2,..., z_{n-1},z_n\}$ and feature points are formed. User selects a random key which is also divided into two sets e.g., $\{u_1,u_2, ...,u_{n-1},u_n\}$ and $\{v_1,v_2,...,v_{n-1}, v_n\}$. The corresponding values from both these sets are used to form random points. The feature points and the random points are used to interpolate cubic Bezier curves. The perimeters **P** of these curves are computed. Also, the area **A** enclosed by these curves and x-axis are computed. The areas and perimeters are used to derive the transformed templates $\mathbf{T_f}$ after certain steps as described in Section 3.2. These templates are stored in the database at the time of registration of the user. For authentication, user presents his modalities to the system. The above procedure is followed again to get the transformed value T_f. This value is compared with the template already stored in the database and accordingly decision is taken whether the subject is genuine or imposter.

5.2.1 Multi-modal Feature Extraction

For extraction of features from several biometric traits, Log-Gabor filters have been used. The Log-Gabor filters are used for texture analysis. The Log-Gabor filter describes a signal in terms of the local frequency responses. The Log-Gabor filter is quite useful in image processing as it captures the statistics of natural images [147].

5.2.2 Cancelable Template Generation

In the proposed scheme, the random values of the area and perimeter of the Cubic Bezier Curves are used to generate random biometric templates which have the features of revocability. The Cubic Bezier Curves are obtained through interpolation of data points obtained from the extracted features. A key set, which is chosen randomly by the user, is also taken into account while forming the data points. This also ensures the formation of random curves whose area and perimeter are obviously random. The biometric templates thus generated can be revoked and a new template can be generated, just by changing the key set. Apart from being random, the generated cancelable biometric templates are also non-invertible. Therefore, even if the stored cancelable biometric templates get compromised, the original biometric data remain safe in the sense that they cannot be derived from the compromised templates.

The feature vector f_x of n-dimension, generated from a particular biometric trait using Log-Gabor filters is added with another feature vector f_y of the same dimension obtained from a randomly chosen image by the user. The resultant feature vector is divided into two equal parts such that the i^{th} value in the first half forms *abscissa* and the corresponding i^{th} value in the second half forms *ordinate* of a point in Cartesian coordinate system. Thus, an extracted feature obtained from a biometric template is represented as feature points in a 2-dimensional plane. Similarly, a random key chosen by the user is also represented as random points in a 2-dimensional plane. A Cubic Bezier Curve is plotted using four control points out of which three points are taken from feature points whereas one point is taken from the random points. In the proposed approach, area and perimeter of such random curves have been

considered. Moreover, the area of the region bounded by such curves (as illustrated in Figure 5.2) and x-axis has been taken into account. The area and perimeter thus computed are random values. Through this approach, each biometric template is transformed into random values which are stored as cancelable biometric template.

Interpolation of Cubic Bezier Curve

A Cubic Bezier Curve is interpolated using four control points and thus it is built in space as four points lie in a space [148].

Suppose the four control points as mentioned above are $\mathbf{p_0}(x_1,y_1)$, $\mathbf{p_1}(x_2,y_2)$, $\mathbf{p_2}(x_3,y_3)$, and $\mathbf{p_3}(u_1,v_1)$. Let $z \in R$, then by using points p_0 and p_1 the point p_0^1 may be derived as shown in in Eq (1):

$$p_0^1(z) = (1-z)p_0 + zp_1 \quad \ldots(1)$$

Similarly, points p_1^1 and p_2^1 can be derived as shown in Eq (2) and (3) given below:

$$p_1^1(z) = (1-z)p_1 + zp_2 \quad \ldots(2)$$

$$p_2^1(z) = (1-z)p_2 + zp_3 \quad \ldots(3)$$

Using these first order derived points the second order points p_0^2 , p_1^2 and the third order derivative p_0^3 can be computed as per Eq (4), (5) and (6) given below:

$$p_0^2(z) = (1-z)p_0^1(z) + zp_1^1(z) \quad \ldots(4)$$

$$p_1^2(z) = (1-z)p_1^1(z) + zp_2^1(z) \quad \ldots(5)$$

$$p_0^3(z) = (1-z)p_0^2(z) + zp_1^2(z) \quad \ldots(6)$$

By using first three equations i.e. Eq (1), (2) and (3) into the next two equations i.e. (4) and (5) we get

$$p_0^2(z) = (1-z)^2 p_0 + 2(1-z)z p_1 + z^2 p_2 \quad \ldots(7)$$

$$p_1^2(z) = (1-z)^2 p_1 + 2(1-z)z p_2 + z^2 p_3 \quad \ldots(8)$$

By solving equations (6), (7) and (8), we get

$$p_0^3(z) = (1-z)^3 p_0 + 2(1-z)^2 z p_1 + (1-z)z^2 p_2 + (1-z)^2 z p_1 + 2(1-z)z^2 p_2 + z^3 p_3$$

$$p_0^3(z) = (1-z)^3 p_0 + 3(1-z)^2 z p_1 + 3(1-z)z^2 p_2 + z^3 p_3 \quad \ldots(9)$$

The point p_0^3 is a point on the curve at parameter value z. For z = ½, the geometric construction is as shown in the Figure 5.2.

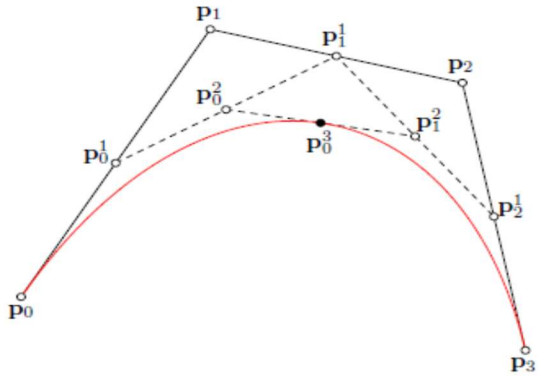


Figure 5.2 : Interpolation of cubic Bezier curve using four control points

In this manner, a cubic Bezier curve is formed using the feature points, obtained from the extracted feature and a random key, chosen by the user.

Template Transformation with Random Area Perimeter Method

Suitable sensors have been used for biometric traits like face, thermal face, palm print, palmvein and fingervein. These biometric images are cropped and resized into 128 x 128 pixels. Then Log Gabor filter feature extraction technique is applied on these images to get an n-dimensional feature vector χ. These extracted features have

values which are in low dynamic range; so they are multiplied by 100 to get reasonably higher values. The entropy of the biometric template is increased by salting the feature vector $\boldsymbol{\chi}$ with an n-dimensional random vector $\boldsymbol{\beta}$. So, we get

$$\boldsymbol{\Psi} = \boldsymbol{\chi} + \boldsymbol{\beta}$$

The vector $\boldsymbol{\Psi}$ is divided into two equal parts $\boldsymbol{\Omega} = \boldsymbol{\Psi}\ \mathbf{(1 : n/2)}$ and $\boldsymbol{\Phi} = \boldsymbol{\Psi}\ \mathbf{(n/2 + 1 : n)}$. A feature point $\mathbf{F_i}$ is defined as ($x_i = \boldsymbol{\Omega}(i)$, $y_i = \boldsymbol{\Phi}(i)$) for i = 1...n/2. A random key $\boldsymbol{K}$ of size n is chosen by the user. The key $\boldsymbol{K}$ is also divided into two equal parts K_1 and K_2. A random point R_i is defined as ($x_i = \boldsymbol{K_1}(i)$, $y_i = \boldsymbol{K_2}(i)$) for i = 1...n/2. Three feature points (say $\mathbf{p_0}$, $\mathbf{p_1}$ and $\mathbf{p_2}$) and one random point (say $\mathbf{p_3}$) are taken as four control points which are used to interpolate a cubic Bezier curve. So, there will be n/6 random cubic Bezier curve corresponding to each set of four control points. The area A_j (where j=1,...,n/6) of the region bounded by the j^{th} curve, x-axis and lines which are parallel to y-axis and passing through end points ($\mathbf{p_0}$ and $\mathbf{p_3}$) is computed. Also, the perimeter P_j (where j=1,...,n/6) is computed for each of these curves. Thus, two arrays of area **A** and perimeter **P** are formed. The size of both these arrays are quite large so in order to reduce the size, the arrays are downsized by 2 to get arrays of size n/12.This downsizing is done by dropping every alternate element of each array. In addition, pairwise mean of the elements of these arrays are taken to form new arrays of size n/24. Now, calculate the mean of each array and add them to all the elements of the array. This will increase the Uniqueness in the vectors. Apply another transformation formula, S=Area/(Perimeter)^2. Calculate the mean m of the resultant vector **S** and then add m^2 to the vector **S** to form $\mathbf{T_f}$, which is the final transformed template. This vector $\mathbf{T_f}$ of dimension n/24 is the cancelable template for the original biometric.

This method ensures a dimensionality reduction of more than 95%. If required, a new cancelable biometric can be obtained using a different key. This complete process is illustrated in Figure 5.3.

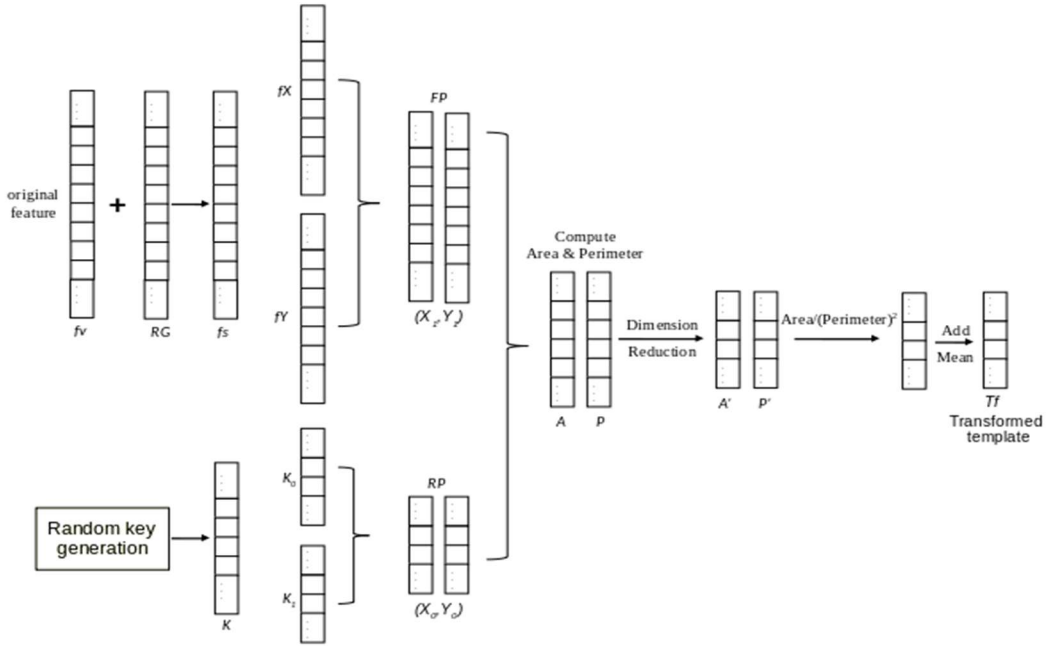


Figure 5.3 : Cancelable template generation process

Pseudocode of the Proposed Method

A pseudocode of the proposed method is given below:

1. **Function** TemplateGeneration (**χ, β, K**)
2. **for** (i = 1 to n)

   Ψ = χ ⊕ β ← Salting by random grid RG

   end
3. **Ω** = **Ψ** (1 : n/2) and **Φ** = **Ψ** (n/2 + 1 : n)

4. **for** (j = 1 to n/2)

   $\mathbf{x_j = \Omega\ (j)}$, $\mathbf{y_j = \Phi\ (j)}$ ← Feature point FP_j

   end

5. $\mathbf{K_0 = K}\ (1 : n/2)$ and $\mathbf{K_1 = K}\ (n/2 + 1 : n)$

6. **for** (j = 1 to n/2)

   $x_j = \mathbf{K_0}(j)$, $y_j = \mathbf{K_1}(j)$ ← Random point RP_j

   end

7. **for** (j = 1 to n/6)

   Constructing Bezier curve C_j using FP_j, FP_{j+1}, FP_{j+2} and RP_j

   Computing the area A_j bounded by C_j

   Computing the Perimeter P_j of C_j

   end

8. $\mathbf{A} = \{A_1, A_2, \ldots, A_{n/6}\}$

9. $\mathbf{P} = \{P_1, P_2, \ldots, P_{n/6}\}$

10. Dropping the alternate elements $\mathbf{A1} = \left\{A'_1, A'_2, \ldots, A'_{\frac{n}{12}}\right\}$

11. Dropping the alternate elements $\mathbf{P1} = \left\{P'_1, P'_2, \ldots, P'_{\frac{n}{12}}\right\}$

12. Taking pairwise mean $\mathbf{A2} = \left\{A''_1, A''_2, \ldots, A''_{\frac{n}{24}}\right\}$

13. Taking pairwise mean $\mathbf{P2} = \left\{P''_1, P''_2, \ldots, P''_{\frac{n}{24}}\right\}$

14. Taking mean of **A2** M_A = Mean (**A2**)

15. Taking mean of **P2** M_P = Mean (**P2)**

16. Adding **A2** with M_A $\mathbf{A3} = \left\{A_1'' + M_A, A_2'' + M_A, \ldots, A_{\frac{n}{24}}'' + M_A\right\}$

17. Adding **P2** with M_P $\mathbf{P3} = \left\{P_1'' + M_P, P_2'' + M_P, \ldots, P_{\frac{n}{24}}'' + M_P\right\}$

18. **for** (j = 1 to n/24)

$$S_j = {}^{A3_j}\Big/_{P3_j^2}$$

end

19. $\mathbf{S} = \{S_1, S_2, \ldots, S_{n/24}\}$

20. Taking mean of **S** m = Mean (**S)**

21. Adding **S** with m^2 $\mathbf{T_f} = \left\{S_1 + m^2, S_2 + m^2, \ldots, S_{\frac{n}{24}} + m^2\right\}$

22. Return ($\mathbf{T_f}$)

5.3 Experimental Validation

The experimental validation of the proposed scheme has been carried out on databases of various modalities like face, thermal face, palm print, palm vein and finger vein. All these modalities have been taken into consideration since these modalities are the one which are extensively been used in various reallife applications. The performance metrics which have been used for the evaluation of the performance of the proposed scheme include Equal Error Rate (EER), Recognition Index (RI), Decidability Index (DI), Receiver Operating Characteristics

(ROC) Curve and Cumulative Matching Characteristics (CMC) Curve. The proposed scheme has been implemented using MATLAB on a PC having 8GB RAM and Intel i5 processor.

5.3.1 Database for Experimentation

For the experimental validation of the proposed scheme, the biometrics that have been considered are palmprint, face, palmvein, thermal face and fingervein. The face biometric has been taken from CASIA Face Image Database Version 5.0 (or CASIA-FaceV5) which contains 2,500 color facial images of 500 subjects. The images show considerable intra-class variations in terms of pose, eye-glasses, illumination, , expression, imaging distance, etc.. Apart from this, 290 face images of 10 subjects have been taken from the IRIS database. The thermal face biometric has been collected from CASIA-NIR-VIS 2.0 database consisting of images of 197 subjects. Besides these, 290 thermal face images of 10 subjects have been taken from the IRIS LWIR database. For the palmprint biometric, 4000 palmprint images have been taken from CASIA Palmprint Image Database. For each subject, images have been collected from both left and right palms. 1200 images have been taken corresponding to 200 subjects from CASIA Multi-Spectral Palmprint Image Database. For palmvein, 1200 images have been taken from CASIA-MS-V1(940). Fingervein biometric data consisting of 3816 images of 636 subjects has been taken from SDUMLA_HMT database. The format of images of vein is .bmp. Of each person, images of both two hands were taken. Data of three fingers (index, middle and ring fingers) were collected for each hand.

The databases of various modalities as shown in Table 5.1 have been considered for the study [149], [150], [151],[152].

Table 5.1 : Databases for various modalities

Modality	Database	No of Subjects	No of Samples
Face	CASIA Face V5	500	5
	IRIS	29	10
Thermal Face	CASIA NIR	197	10
	IRIS(LWIR)	29	10
Palmvein	CASIA MS V1(940)	200	6
Palmprint	CASIA	500	8
	CASIA MS V1(WHT)	200	6
Fingervein	SDUMLA-HMT	636	6

These modalities have also been used for constructing the following four chimeric multi-modal datasets namely D1, D2, D3 and D4, on which the experimentation was performed. D1 contains 1200 face images from CASIA-Face V5 database and 1200 palmvein images from CASIA-MS V1(940) database. D2 consists of 1200 palmvein images from CASIA-MS V1(940) database and 1200 fingervein images from SDUMLA-HMT database. D3 includes 1200 palmvein images from CASIA-MS V1(940) database and 1200 palmprint images from CASIA-MS V1(WHT) database. The chimeric data set D4 contains 290 face images from IRIS database and 290 thermal face images from IRIS(LWIR) database. These chimeric multi-modal datasets are shown in the Table 5.2.

Table 5.2 : Datasets for various modalities

Chimeric Dataset	Multi-Modalities	Databases	Images
D1	Face & Palmvein	CASIA-Face V5 & CASIA-MS V1(940)	1200
D2	Palmvein & Fingervein	CASIA-MS V1(940) & SDUMLA-HMT	1200
D3	Palmvein & Palmprint	CASIA-MS V1(940) & CASIA-MS V1(WHT)	1200
D4	Face & Thermal Face	IRIS & IRIS(LWIR)	290

5.3.2 Performance Evaluation Metrics

The proposed scheme has been quantitatively analysed by using following performance evaluation metrics

(a). Equal Error Rate (EER): EER is the value when FAR and FRR are equal, and is represented as the point at which the plotted curves of FAR and FRR values intersect. EER is also termed as Cross-over error rate between FAR and FRR. [Refer Section 2.7.5]

(b). Decidability Index (DI): The decidability index measures how similar the sample is with respect to the positive class, and classifying the pattern as positive if the similarity score is above some predefined threshold. [Refer Section 2.7.9]

(c). Recognition Index (RI): Recognition Rate or Rank-1 identification is capability of the biometric system in obtaining best matching score with the

correct enrolled template in comparison to other templates in the data base. [Refer Section 2.7.7]

(d). Receiver Operating Characteristics (ROC) Curve: Receiver Operating Characteristic (ROC) curve is a 2-dimensional plot between False Positive Rate (FPR or FAR) and True Positive Rate (TPR). [Refer Section 2.7.6]

(e). Cumulative Matching Characteristics (CMC) Curve: Cumulative Match Characteristic (CMC) curve is drawn by taking rank values on the x-axis and the probability of correct identification upto that rank, on the y-axis. [Refer Section 2.7.8]

A qualitative as well as quantitative analysis has been done for the proposed method for generation of cancelable biometric templates.

5.4 Qualitative Analysis

In the Qualitative analysis, the consistency, non-invertibility, revocability and unlinkability features of the proposed scheme have been studied.

5.4.1 Consistency

A transformation function is considered consistent if the transformed features are able to preserve the intra-class and inter-class variations. The extracted features of the original biometric templates as well as the transformed templates have been converted into 2-dimensional points and have been displayed in the Cartesian plane

as shown in Figures 5.4 & 5.5. Two biometric samples I1 & I2 (Figures 5.4(a) & 5.4(b)) of the same subject have been taken from CASIA face database and their original features have been plotted in Figure 5.4(c). The transformed features for both the samples have been obtain RG and K in order to cater the worst-case scenario. Feature points and random points are shown in Figure 5.4(d). A plot between location and intensity for the transformed features of the images I1 and I2, in the worst-case scenario, is shown in Figure 5.4(e). In another experiment, the biometric samples I1 & I2 (Figures 5.5(a) & 5.5(b)) of the two different users have been taken and their transformed features have been obtained using the same transformation parameters RG and K in the worst-case scenario. Figure 5.5(c) represents the original biometric features whereas Figure 5.5(d) represents Cartesian representation of the random points and feature points. A plot between location and intensity for the transformed features of the images I1 and I2 in the worst-case scenario, is shown in Figure 5.5(e). In both cases, the first 100 features obtained at m = 1 orientation and n = 1 scale have been considered. Then these features have been converted into Cartesian points.

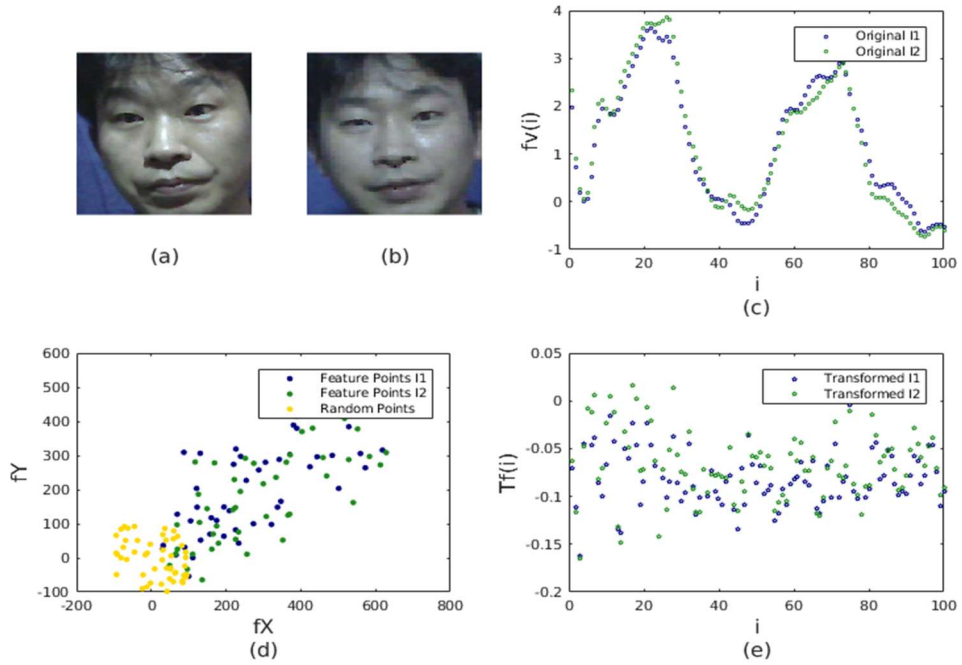


Figure 5.4: (a)-(b) sample images I1 and I2, (c) original features, (d) feature points and random points, (e) transformed features

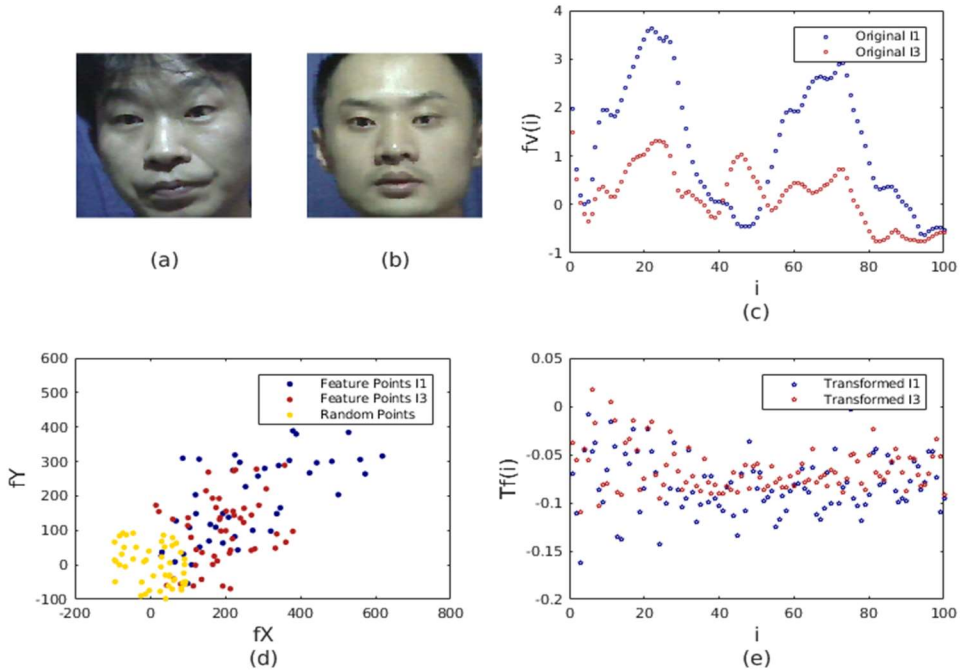


Figure 5.5: (a)-(b) sample images I1 and I2, (c) original features, (d) feature points and random points, (e) transformed features

It is observed that both intra-class and inter-class variations are preserved for the transformation function in both the cases i.e., when samples are taken for the same subject or for two different subjects. Therefore, the proposed method is consistent with respect to different biometric samples and modalities.

5.4.2 Non-Invertibility

An essential requirement for any cancelable biometric template is that it should be non-invertible i.e., the original biometric template should not be recoverable even if the key and the cancelable template get compromised. The proposed method is non-invertible as it is impossible to trace back the Bezier curve from the values of area and perimeter. Even if the curve is obtained, it is impossible to find actual source of interpolation of the Bezier curve i.e., the actual feature points as there are infinite points over the curve. This becomes even more difficult as more than 95% of the information is discarded while generating the cancelable biometric template.

5.4.3 Revocability

The very concept of cancelable biometric system is that in case of loss of the stored templates, it should be able to generate a new template which is to be stored i.e., already stored biometric templates is discarded and in place a new template is stored [92]. In the proposed scheme a random key which is chosen by the user plays a crucial role in generating cancelable template. Using this random key, random point is generated which is used in interpolating a Bezier curve whose area and perimeter is computed. Thus, by just changing the key a new curve is interpolated and new values of area and perimeter are determined. This way a new template is generated

and stored. Therefore, the revocability feature ensures that the stolen template is easily replaceable by a new template, just by using a different set of keys.

5.4.4 Unlinkability

The concept of unlinakbility means that the various templates corresponding to a particular biometric of an individual stored in the databases of various applications must be unlinkable. In the proposed scheme, the user has to choose a random key which is used to generate a random Bezier curve whose area and perimeter are computed for generation of cancelable template. Thus, different user keys lead to generation of different random cancelable templates for a particular biometric. Various test modules have been used to test the randomness of the generated values stored as cancelable template. It is observed that the generated values exhibit a good randomness behaviour which ensures the unlinkability of the cancelable templates. The feature of unlinkability ensures that the identity of the individual is protected even when it is enrolled in multiple applications.

Qualitative analysis of the proposed scheme shows that the system ensures the privacy of each user by means of consistency, non-invertibility, revocability and unlinkability of the cancelable templates.

5.5 Quantitative Analysis

An important criterion for a robust cancelable biometric is that it should preserve the discriminative characteristics in the transformed domain also. Therefore, the

authentication performance of the cancelable biometric must be atleast as good as that of the original biometric. The experimentations have been carried out using eleven state of the art feature transformation techniques viz., Gray Salting, Random Projection with vector translation (RPV), 2D BioHash, BioConvolving, 2D BioPhasor, Random Permutation Maxout (RPM) transform, XOR based salting, Random Slope Version 1, Random Slope Version 2 and Random Distance Method. BioHashing technique has also been applied in two forms BH and BH-50 technique. In BH all the features in the transformed domain have been taken for experimentation, whereas in BH-50 technique only 50% of the features have been considered. The advantage of all these techniques and the proposed RAPM technique is that they can be used for different type of biometrics. All these transformation techniques have been applied on the same biometric template so that their matching performance can be compared on the same scale. Support Vector Machine (SVM) has been applied for measuring the classification and matching performance. Total 5 images per user are transformed using the above method. The training the model has been done using 4 images while testing has been using the fifth image. The prediction scores are generated in the score variable.

Same random points have been used for interpolating Bezier curves for different biometric samples for evaluating the discriminating property of the RAPM. The performance in terms of EER, DI and RI for both the original and transformed biometric templates in the worst-case scenario have been compared with the state of the art techniques as shown in Tables 5.3, 5.4 and 5.5 respectively.

Table 5.3: Comparative Performance in terms of EER

Modalities	**Face**		**Thermal Face**	**Palmprint**		**Palmvein**	**Fingervein**
Databases → Techniques ↓	CASIA-V5	IRIS	IRIS (LWIR)	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
Original Templates	2.17	2.06	0.72	0.50	1.00	0.98	1.10
Gray Salting	4.71	1.27	2.42	0.65	1.02	2.19	1.04
RPV	2.92	1.16	0.38	0.53	0.60	0.81	0.71
BH	3.03	3.56	1.39	0.56	0.60	1.25	1.40
BH-50	4.52	3.62	2.05	0.65	0.70	1.50	1.70
BioConvolving	7.84	2.50	7.20	2.88	5.95	5.50	2.20
BioPhasor	3.50	10.34	4.41	1.36	1.30	2.00	2.27
RPM	9.28	6.75	13.49	4.00	2.91	4.50	1.73
XOR	2.78	1.33	0.41	0.55	0.60	1.03	0.66
Random Slope-V1	2.40	0.99	0.22	0.42	0.48	0.68	0.71
Random Slope-V2	3.08	1.19	0.36	0.52	0.64	1.11	0.78
Random Distance	2.60	2.68	0.09	0.53	0.60	0.99	1.19
Proposed Method (RAPM)	1.21	0.22	0.08	0.11	0.02	0.67	0.77

Table 5.4: Comparative Performance in terms of DI

Modalities	**Face**		**Thermal Face**	**Palmprint**		**Palmvein**	**Fingervein**
Databases → Techniques ↓	CASIA-V5	IRIS	IRIS (LWIR)	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
Original Templates	4.188	4.542	4.946	9.876	5.970	6.635	7.657
Gray Salting	3.596	5.112	4.310	7.896	7.914	4.850	3.921
RPV	4.412	5.309	5.454	7.151	8.120	5.979	4.314
BH	3.442	4.464	6.545	9.851	5.820	5.979	7.314

BH-50	3.074	4.320	5.783	9.621	5.658	5.841	7.101
BioConvolving	2.562	3.980	2.727	3.624	2.628	2.903	3.721
BioPhasor	3.351	2.672	3.857	7.692	5.040	5.117	6.050
RPM	2.577	2.954	2.636	5.351	4.065	3.383	3.747
XOR	4.401	4.432	5.217	7.214	8.118	5.352	4.921
Random Slope-V1	4.456	5.282	5.612	7.523	8.259	6.210	5.498
Random Slope-V2	4.408	5.126	5.388	7.338	8.110	5.280	4.788
Random Distance	3.860	4.244	4.629	9.736	6.684	5.985	7.474
Proposed Method (RAPM)	5.402	4.932	4.461	5.964	13.120	4.768	5.321

Table 5.5: Comparative Performance in terms of RI

Modalities	**Face**		**Thermal Face**	**Palmprint**		**Palmvein**	**Fingervein**
Databases → Techniques ↓	CASIA-V5	IRIS	IRIS (LWIR)	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
Original Templates	92.10	97.85	99.65	99.42	98.60	98.90	98.39
BH	83.89	92.41	97.25	99.34	98.40	98.25	97.48
BioPhasor	79.20	68.96	87.24	98.88	97.10	96.50	95.47
BH-50	73.88	91.37	95.51	98.68	98.20	98.25	96.30
Random Distance	85.88	94.48	99.35	99.33	98.59	98.60	98.30
Proposed Method (RAPM)	99.22	99.70	99.82	99.87	99.65	99.68	99.22

As it is evident from the Table 5.3, the EER values for the proposed RAPM method is quite better in comparison to various state-of-art techniques for all the biometric modalities. The DI values in Table 5.4 suggest that the cancelable biometric templates generated through RAPM retain the discriminating characteristics to correctly identify between the genuine and impostor. Table 5.5 suggests that the

recognizing capability of the proposed RAPM technique is far better than the BioHashing, BioPhasor and Random distance techniques.

Multimodal biometric templates have been obtained from different combination of biometric modalities as described in the Section 4.1. The matching performances of RAPM technique in terms of EER and RI on some multimodal templates have been shown in Table 5.6 and Table 5.7.

Table 5.6 : Comparative Performance in terms of EER for multimodal biometrics

Modalities	**Face + Palmvein**	**Palmvein + Finger vein**	**Palmvein + Palmprint**	**Face + Thermal Face**
Datbases → Parameters ↓	CASIA-V5 + CASIA-MS(940)	CASIA-MS(940) + SDUMLA-HMT	CASIA-MS(940) +CASIA-MS(WHT)	IRIS + IRIS(LWIR)
Random Distance	0.60	0.60	0.39	0.34
Proposed Method (RAPM)	0.09	0.06	0.01	0.06

Table 5.7 : Comparative Performance in terms of RI for multimodal biometrics

Modalities	**Face + Palmvein**	**Palmvein + Fingervein**	**Palmvein + Palmprint**	**Face + Thermal Face**
Databases → Parameters ↓	CASIA-V5 + CASIA-MS(940)	CASIA-MS(940) + SDUMLA-HMT	CASIA-MS(940) + CASIA-MS(WHT)	IRIS + IRIS(LWIR)
Random Distance	99.10	99.40	99.20	99.65
Proposed Method (RAPM)	99.55	99.80	99.76	99.89

Thus, it is observed that the cancelable biometrics obtained through RAPM for both uni-modal as well as multi-modal biometrics, give better result than the original biometrics, in the worst-case as well as in the best-case scenario.

In almost all the results, there is significant reduction in the value of EER, and increase in the values of DI and RI. This shows that the proposed RAPM technique is very effective for generation of cancelable biometric templates for both uni-modal and multi-modal cases.

The ROC curves for various uni-modal biometrics in the worst-case scenario have been shown in Figure 5.6. In the first row, the ROC curves for the databases CASIA-Face V5, IRIS, IRIS (LWIR) and CASIA Palmprint have been shown respectively from left to right. In the second row the ROC curves for the databases CASIA MS V1(WHT), CASIA MS V1(940) and SDUMLA-HMT have been shown respectively from left to right.

Similarly, the CMC curves in the worst-case scenario for various uni-modal biometrics have been shown in Figure 5.7. In the first row, the CMC curves for the databases CASIA-Face V5, IRIS, IRIS (LWIR) and CASIA Palmprint have been shown respectively from left to right. In the second row the CMC curves for the databases CASIA MS V1(WHT), CASIA MS V1(940) and SDUMLA-HMT have been shown respectively from left to right.

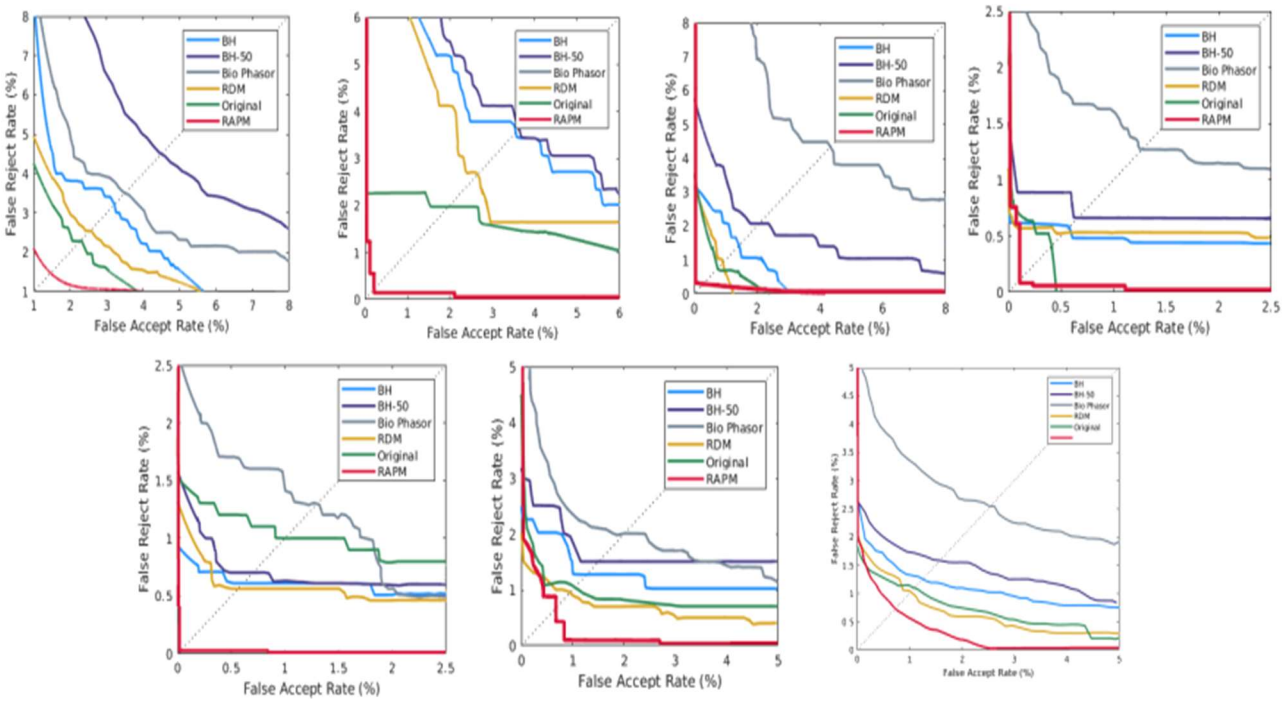


Figure 5.6 : ROC curves for various uni-modal biometrics in the worst-case scenario

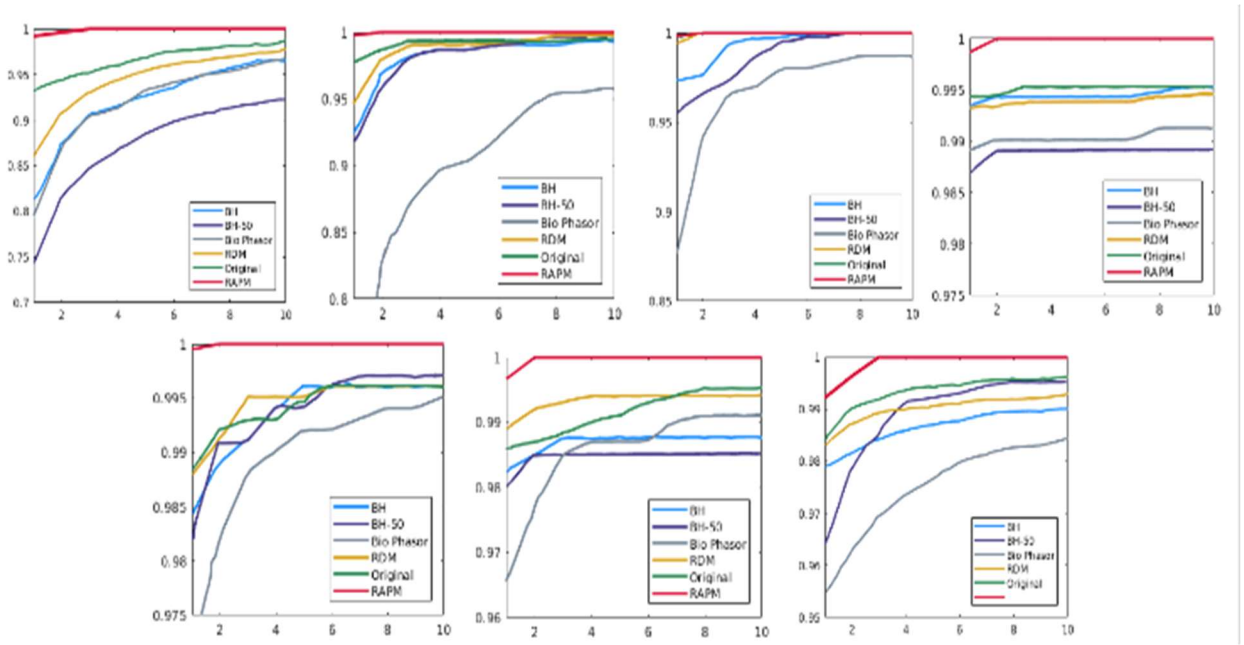


Figure 5.7 : CMC curves for various uni-modal biometrics in the worst-case scenario

The ROC curves in Figure 5.6 and CMC curves in Figure 5.7 show that the proposed cancelable template generation method performs better as compared to other state-of-the-art techniques for uni-modal cases.

The ROC curves and CMC curves in the worst-case scenario for various multi-modal biometrics have been shown in Figure 5.8.

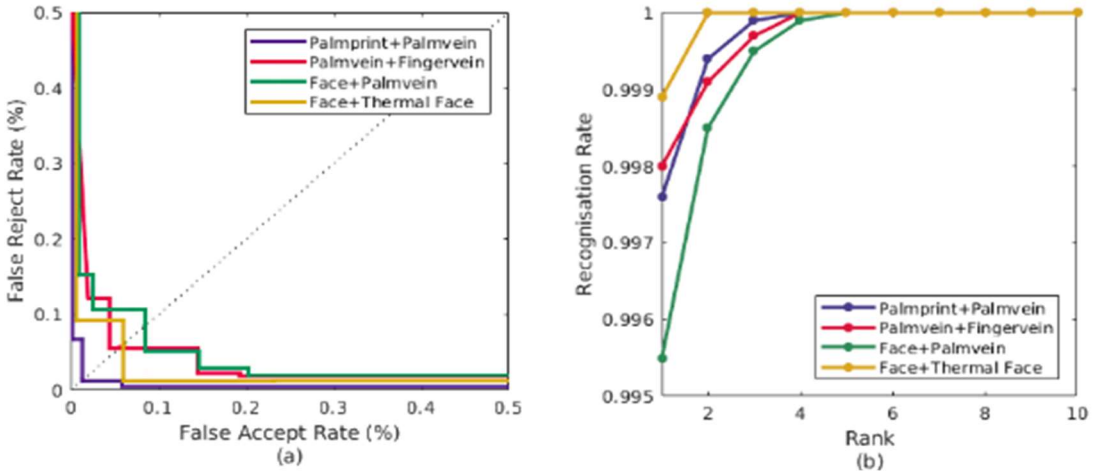


Figure 5.8 : (a) ROC curves (b) CMC curves in the worst-case scenario for various multimodal biometrics

The Roc curves in Figure 5.8(a) and CMC curves in Figure 5.8(b) show that the proposed cancelable template generation method performs better in comparison to other state-of-the-art techniques for multi-modal cases.

5.6 Significant Findings

The significant highlights of this research work are as follows:

- A novel scheme, the Random Area & Perimeter Method (RAPM)) is presented in which a biometric characteristic of an individual is transformed into random values which are stored as cancelable biometric templates.

- The proposed scheme computes area and perimeter of the Bezier curve which are obtained through interpolation of feature points of original biometrics and a random point chosen by the user. The area and perimeter thus computed exhibit pseudo-random properties.

- Uni-modal and multi-modal biometric systems involving biometrics like palmprint, face, palmvein, thermal face and fingervein, have been developed.

- A dimensionality reduction to the tune of more than 95% has been obtained without compromising the matching performance.

- EER values obtained through the proposed RAPM method is quite better in comparison to many state-of-the-art techniques for all the biometric modalities.

- The DI values suggest that the cancelable biometric templates generated through RAPM retain the discriminating characteristics to correctly identify between the genuine and imposter.

- Recognizing capability of the proposed technique is far better than Bio-Hashing, Bio-Phasor and Random distance techniques.

- The ROC curves and CMC curves show that the proposed cancelable template generation method performs better as compared to many state of the art uni-modal and multi-modal biometric systems.

- Cancelable biometrics obtained through RAPM for both uni-modal as well as multi-modal biometrics, give better result than the original biometrics.

The experimental results along with other findings were published in [153].

Chapter 6

Conclusions & Future Directions

This section summarizes the major contributions and achievements that come out of the present work. Despite the significant contributions, no research is said to be complete unless it directs to a few topics for future research. Hence, the potential work that can be explored further is also briefly discussed here.

Summary of Major Contributions

The aim of this thesis work was to develop efficient methods for biometric cryptosystems. In order to address the limitations of various aspects of a robust biometric cryptosystem, several novel contributions have been proposed under present work which are summarized as follows:

- A multimodal biometric system design has been proposed which is based on cancelable features containing complementary information from three modalities viz. Face, Iris and Ear. Key features have been incorporated for each modality to generate cancelable biometric templates. Feature values obtained from individual characteristic have been fused with corresponding key features to transform the features. The transformation process includes generation of similarity and sparse matrices from concatenated feature vector formed with biometric features and key features. Diffusion of transformed matrices using

graph-based random walk cross-diffusion method leads to a robust template. Optimal belief masses for individual classifier are determined using cuckoo search optimization. Optimal classifier beliefs are fused using DSmT based proportional conflict redistribution (PCR-6) rules. Multi-stage fusion model determines optimal confidence factors for each classifier. Classifier beliefs are suppressed for discordant classifiers, boosted for concurrent classifier and conflict is optimally resolved among conflicting classifier beliefs using PCR-6 rules to achieve a final score. The proposed scheme for optimal score fusion produces better results in comparison to many state-of-the-art fusion schemes. Exhaustive random space of key features provides high brute force complexity. In addition, generated templates are highly revocable in case of database breach, making the proposed model highly secure. The accuracy of 98.316 and average EER of 2.32 have been obtained through the proposed method.

- A novel biometric cryptosystem which involves cryptographic key binding by minimizing the objective function has been proposed. Secret key which is to be bound is split into a number of crypto-components. Similarly, the biometric data is also divided into several bio-components and distinct objective functions are defined corresponding to each bio-component. Key binding process has been devised using crypto-components, bio-components and objective functions. Process for reconstruction of secret key from the helper data is also designed. New objective functions have been defined for creation of helper data by hiding the secret key. This helper data is subsequently used to retrieve the key. The effect of noise and neighbourhood threshold have been assessed on the convergence stability of the objective function. The proposed method is extensively evaluated for iris and fingerprint modalities. Also, robustness against

cryptanalytic attacks have been assessed. Performance evaluation of the proposed method have been done using various performance metrics like FAR, GAR, Genuine WDR and Imposter WDR on iris and fingerprint benchmark datasets considering various sizes of the secret cryptographic keys. A detailed performance analysis in terms of FAR, GAR, GWDR and IWDR shows that this method is very efficient. Its performance does not get affected with change of length of secret key and upto a certain amount of noise induction in the user biometric data. Further, heat analysis illustrates that when the mean of the bio-components is taken as the gallery item i.e., representative template, the matching score is better in comparison to the case where individual bio-component is taken as the gallery item. Security analysis of the proposed method shows that this technique is quite robust against brute force attack and correlation attack. Security analysis of the proposed method has been done by investigating the robustness of the method against brute force attack and correlation attack. The helper data exhibits randomness property which ensures that adversary cannot predict or recover the secret key. The proposed method consistently achieves good success rate even with some changes in the neighborhood threshold values and some amount of randomization in the input values to the objective function. The proposed biometric cryptosystem achieves a high genuine acceptance rate and a very low false acceptance rate. Moreover, wrongly decoded bit rate for genuine user is quite low which ensures retrieval of correct key.

- A novel scheme, the Random Area & Perimeter Method (RAPM)) has been proposed in which a biometric characteristic of an individual is transformed into random values which are stored as cancelable biometric templates. The

proposed scheme computes area and perimeter of the Bezier curves which are obtained through interpolation of feature points of original biometrics and a random point chosen by the user. The proposed method is very effective in generation of cancelable biometric templates for various biometric traits like face, palmprint, fingervein, thermal face and palmvein. These templates have been experimentally verified and compared with the transformed templates generated through various other state of the art transformation techniques. Performances of the generated cancelable biometrics measured in terms of various evaluation metrics like EER, DI, RI, ROC and CMC confirm the reliability and robustness of the proposed approach. Proposed scheme is also validated on four multi-modal datasets generated from benchmark databases of face, palmvein, fingervein, palmprint and thermal face. Exhaustive result analysis shows that the proposed scheme also performs well for multi-modal case and surpasses many state-of-the-art fusion methods. Qualitative analysis shows that the proposed scheme exhibits high level of consistency, non-invertibility, revocability and unlinkability resulting in high reliability and accuracy. The average values obtained for EER, DI and RI are 0.0045, 6.28 and 99.64 respectively which are better than those obtained for the available state of the art approaches. Better performance results have been obtained for both uni-modal as well as multi-modal biometric templates and also in the worst-case as well as the best-case scenarios. Moreover, a dimensionality reduction of more than 95% has been achieved for uni-modal biometrics in the worst-case and the best-case scenarios. Recognizing capability of the proposed technique is far better than Bio-Hashing, Bio-Phasor and Random distance techniques. The ROC curves and CMC curves show that the proposed cancelable template generation method

performs better than many state of the art techniques for uni-modal and multi-modal biometric systems.

The development of multi-modal biometric system by optimally fusing the feature values provide reduces the dependence of biometric cryptosystem on a single biometric characteristic thereby increasing its efficiency and robustness. The methodology of secure binding of secret key with the user biometric not only provides secrecy in the system but also reduces the risk of unauthorized access to the biometric cryptosystems. The development of new technique for biometric template protection protects vital personal information of the user from being misused which helps in building confidence among the users of biometric cryptosystems. Thus, the methodologies developed in this research work, cover all the three major aspects of biometric cryptosystems and leads to development of a robust, secure and an efficient biometric cryptosystem.

Future Directions

In the present work, multi-cue object tracking model under various framework were investigated and explored at length to provide novel contributions to the domain. Despite that, there are certain research areas that emerge out of the present work which demand future investigation. These areas are summarized as directions to future work and are detailed as follows :

- The proposed multimodal biometric authentication system can be applied for several other biometric traits. Another possible extension can be made by utilizing the multi-modal information captured from multiple sensors.

- Integration of various image quality factors along with role of a particular trait into the proposed fusion model is another direction for research. Outlier detection procedure can be explored with fuzzy decision boundary for generating the clearer decision discriminability.

- The proposed biometric cryptosystem scheme can further be studied for multi-modal scenarios under dynamic environment. Adaptability of the biometric system to different types and dimension of the biometrics can also be investigated. Any biometric trait whose features can be extracted in binary form can be used in this methodology.

- Also, the issue of image quality may be studied as it plays an important role in the proposed key binding method. When some of the issues viz., data acquisition, sensor efficiency, image quality etc. are properly resolved, it enhances the adaptability of the system to the different type of user's environments. This will pave the way to make a highly reliable and robust biometric cryptosystem based on key binding method.

- This study further entails the possibility of analysis on other databases and application of other performance evaluation metrics.

- In future, the issue of image quality may be incorporated to enhance recognition rates. This will lead the way to make a highly reliable and robust cancelable biometric system.

References

[1]. A. K. Jain, A. Ross & S. Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, Jun.2006, vol. 1, Issue 2, pp 125 – 144

[2]. A. K. Jain, A. Ross & S. Prabhakar, “An introduction to biometric recognition”, IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet, Jan. 2004, vol. 14, Issue 1, pp. 4–20

[3]. M. A. Dabbah, W. L. Woo & S. S. Dlay, "Secure Authentication for Face Recognition", Proc. of IEEE Symposium on Computational Intelligence in Image and Signal Processing, Apr. 2007, pp. 121 - 126

[4]. C. Soutar, D. Roberge, A. Stoianov, R. Gilroy & B. V. Kumar, “Biometric Encryption - Enrollment and Verification Procedures,” Proc. SPIE, Optical Pattern Recognition IX, vol. 3386, 1998, pp. 24–35

[5]. S. Guennouni, A. Mansouri & A. Ahaitouf, “Biometric Systems and Their Applications”, 2019 DOI:10.5772/intechopen.84845

[6]. A. K. Jain, “Biometric Recognition: Overview and Recent Advances”, Progress in Pattern Recognition, Image Analysis and Applications. CIARP 2007. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2007, vol 4756 DOI: https://doi.org/10.1007/978-3-540-76725-1_2

[7]. U. Gawande, Y. Golhar & K. Hajari, “Biometric-Based Security System: Issues and Challenges”, 2017, DOI:10.1007/978-3-319-44790-2_8

[8]. T. Sabhanayagam, V. P. Venkatesan and K. Senthamaraikannan, “A Comprehensive Survey on Various Biometric Systems”, International Journal of Applied Engineering Research ISSN 0973-4562, 2018, vol. 13, Number 5, pp. 2276-2297

[9]. G. Aguilar, G. Sanchez, K. Toscano, M. Salinas, M. Nakano & H. Perez., "Fingerprint Recognition", 2nd International Conference on Internet Monitoring and Protection (ICIMP), 2007, pp. 32-32, doi: 10.1109/ICIMP.2007.18

[10]. P. P. Polash & M. M. Monwar, "Human iris recognition for biometric identification", 10th International conference on computer and information technology, 2007, pp. 1-5, doi: 10.1109/ICCITECHN.2007.4579354

[11]. M. U. Akram, A. Tariq & S. A. Khan, "Retinal recognition: Personal identification using blood vessels", International Conference for Internet Technology and Secured Transactions, 2011, pp. 180-184

[12]. L. Li, X. Mu, S. Li & H. Peng., "A Review of Face Recognition Technology," IEEE Access, 2020, vol. 8, pp. 139110-139120, DOI: 10.1109/ACCESS.2020.3011028

[13]. J. K. Ayeni, K. A. Sadiq & A. Adedoyin, "Analysis of a Hand Geometry-Based Verification System", International Journal of Scientific Research Engineering & Technology (IJSRET), 2013, vol. 2, Issue 6, pp. 352-357

[14]. D. Palma, P. L. Montessoro, G. Giordano & F. Blanchini, "Biometric Palmprint Verification: A Dynamical System Approach," IEEE Transactions on Systems, Man, and Cybernetics: Systems, Dec. 2019, vol. 49, no. 12, pp. 2676-2687, DOI: 10.1109/TSMC.2017.2771232.

[15]. L. Wang & G. Leedham, "A Thermal Hand Vein Pattern Verification System", Pattern Recognition and Image Analysis (ICAPR) 2005. Lecture Notes in Computer Science, vol 3687. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11552499_7

[16]. A. Sajantila & B. Budowle, "Identification of individuals with DNA testing. Ann Med. Dec. 1991, vol. 23(6) pp. 637-42, DOI: 10.3109/07853899109148096

[17]. G. Gupta & A. Mccabe, "A Review of Dynamic Handwritten Signature Verification", 1998.

[18]. M. Kabir, J. Shin, I. Jahan & A. Ohi, "A Survey of Speaker Recognition: Fundamental Theories", Recognition Methods and Opportunities. IEEE Access, 2021, pp. 1-1. DOI: 10.1109/ACCESS.2021.3084299.

[19]. E. Yu & S. Cho, “Keystroke dynamics identity verification - Its problems and practical solutions”, Computers & Security, 2004 vol. 23, pp. 428-440, DOI : 10.1016/j.cose.2004.02.004.

[20]. M. Kumar, “Fingerprint Recognition System: Issues and Challenges”, International Journal for Research in Applied Science and Engineering Technology, 2018, vol. 6, pp. 556-561, DOI : 10.22214/ijraset.2018.2080

[21]. M. Hassaballah & S. Aly, “Face Recognition: Challenges, Achievements, and Future Directions”, IET Computer Vision.2015, vol. 9, pp. 614-626, DOI : 10.1049/iet-cvi.2014.0084.

[22]. D Marsico, M. Frucci & D. Riccio, “Eye biometrics: Advances and new research lines”, Pattern Recognition Letters, 2016, vol. 82, DOI : 10.1016/j.patrec.2016.05.003

[23]. S. Khan, S. Parkinson, L. Grant, N. Liu & S. McGuire, “Biometric Systems utilising Health Data from Wearable Devices”, Applications and Future Challenges in Computer Security, vol. 1, 1 (May 2020).

[24]. J. H. Hong, E. K. Yun & S. B. Cho, “A Review of Performance Evaluation for Biometrics Systems”, International Journal of Image and Graphics, vol. 05, DOI : https://doi.org/10.1142/S0219467805001872

[25]. A. Sundarrajan, A. I. Sarwat & A. Pons, “A Survey on Modality Characteristics, Performance Evaluation Metrics, and Security for Traditional and Wearable Biometric Systems”, ACM Computer Survey, 2019, vol. 52, No. 2, DOI: https://doi.org/10.1145/3309550

[26]. J. A. Unar, W.C. Seng & A. Abbasi, “A review of biometric technology along with trends and prospects”, Pattern Recognition, 2014, vol.47, Issue 8, pp. 2673– 2688

[27]. A. Lumini & L. Nanni, “Overview of the combination of biometric matchers, Information Fusion”, 2017, vol. 33, pp. 71–85

[28]. P. Lee, “Prints charming: how fingerprints are trailblazing mainstream biometrics”, Biometric Technology Today, 2017, vol. 4, pp. 8–11

[29]. P. Tome, J. Fierrez, R. V. Rodriguez & D. Ramos, “Identification using face regions: Application and assessment in forensic scenarios”, Forensic Science International, 2013, vol. 233, (1-3), pp. 75–83

[30]. Z. Huang, Y. Liu, X. Li & J. Li, “An adaptive bimodal recognition framework using sparse coding for face and ear”, Pattern Recognition Letters, 2015, vol. 53, pp. 69–76

[31]. Z. Huang, Y. Liu, C. Li , M. Yang & L. Chen, “A robust face and ear based multimodal biometric system using sparse representation”, Pattern Recognition, 2013, vol. 46, Issue 8, pp. 2156–2168

[32]. L. Mezai & F. Hachouf, “Score-level fusion of face and voice using particle swarm optimization and belief functions”, IEEE Transactions on Human Machine Systems, 2015, vol. 45, Issue 6, pp. 761–772

[33]. R. Raghavendra, B. Dorizzi, A. Rao & G. H. Kumar, “Designing efficient fusion schemes for multimodal biometric systems using face and palmprint”, Pattern Recognition, 2011, vol. 44, Issue 5, pp. 1076–1088

[34]. V. Conti, C. Militello, F. Sorbello & S. Vitabile, “A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems”, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2010, vol. 40, Issue 4, pp. 384–395

[35]. A. Fierrez, J. Ortega, J. Garcia, R. Gonzalez & J. Bigun, “Discriminative multimodal biometric authentication based on quality measures”, Pattern Recognition, 2005, vol. 38, Issue 5, pp. 777–779

[36]. N. Srinivas, K. Veeramachaneni & L. A. Osadciw, “Fusing correlated data from multiple classifiers for improved biometric verification”, 12th International Conference on Information Fusion. (IEEE), 2009, pp. 1504–1511

[37]. T. Tong, K. Gray, Q. Gao, L. Chen & D. Rueckert, “Multi-modal classification of alzheimer's disease using nonlinear graph fusion”, Pattern Recognition, 2017, vol. 63, pp. 171–181

[38]. A. K. Jain, K. Nandakumar & A. Nagar, “Biometric template security”, EURASIP Journal on advances in signal processing, 2008

[39]. N. K. Ratha, S. Chikkerur, J. H. Connell & R. M. Bolle, “Generating cancelable fingerprint templates”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007, vol. 29, Issue 4, pp. 561–572

[40]. A. B. J. Teoh, A. Goh & D. C. L. A., Ngo, D.C.L., “Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, vol. 28, Issue 12, pp. 1892–1901

[41]. C. S. Chin, A. T. B. Jin & D. N. C. Ling, “High security iris verification system based on random secret integration”, Computer Vision and Image Understanding, 2006, vol. 102, Issue 2, pp. 169–177

[42]. T. Connie, A. Teoh, M. Goh & D. Ngo, “Palm Hashing: a novel approach for cancelable biometrics”, Information Processing Letters, 2005, vol. 93, Issue 1, pp. 1–5

[43]. M. Savvides, B. V. Kumar & P. K. Khosla, “Cancelable biometric filters for face recognition”, Proceedings of the Pattern Recognition 17th International Conference on Pattern Recognition (ICPR), 2004, IEEE, vol. 3, pp. 922–925

[44]. M. Oussalah, “On the use of hamachers t-norms family for information aggregation”, Information sciences, 2003, vol. 153, pp. 107–154

[45]. G. S. Walia, T. Singh, K. Singh & N. Verma, “Robust multimodal biometric system based on optimal score level fusion model”, Expert Systems with Applications, 2018

[46]. Y. Wang, W. Zhang, L. Wu, X. Lin & X. Zhao, “Unsupervised metric fusion over multi-view data by graph random walk-based cross-view diffusion”, IEEE Transactions on Neural Networks and Learning Systems, 2017, vol. 28, Issue 1, pp. 57–70

[47]. A. M. P. Canuto, F. Pintro, F. & J.C. Xavier, “Investigating fusion approaches in multi-biometric cancelable recognition”, Expert Systems with Applications, 2013, vol. 40, Issue 6, pp. 1971–1980

[48]. D. Paula, A. M. Canuto, F. Pintro & M.C. Fairhurst, “Ensemble systems and cancellable transformations for multibiometric-based identification”, IET Biometrics, 2014, vol. 3, Issue 1, pp. 29–40

[49]. A. Bosch, A. Zisserman & X. Munoz, “Representing shape with a spatial pyramid kernel”, Proceedings of the 6th ACM international conference on Image and video retrieval, 2007, pp. 401–408

[50]. J.G. Daugman, “High confidence visual recognition of persons by a test of statistical independence”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993, vol. 15, Issue 11, pp. 1148–1161

[51]. W. Zhang, S. Shan, W. Gao, X. Chen & H. Zhang, “Local gabor binary pattern histogram sequence (lgbphs): a novel non-statistical model for face representation and recognition”, 10th International Conference on Computer Vision, IEEE, 2005, vol. 1, pp. 786–791

[52]. L. Liberti, C. Lavor, N. Maculan & A. Mucherino, “Euclidean distance geometry and applications”, SIAM Review, 2014, vol. 56, Issue 1, pp. 3–69

[53]. I. S. Duff, “A survey of sparse matrix research”, Proceedings of the IEEE, 1977, vol. 65, Issue 4, pp. 500–535

[54]. K. Beyer, J. Goldstein, R. Ramakrishnan & U. Shaft, “When is nearest neighbor meaningful ?”, Lecture Notes in Computer Science, Springer, 1999. pp. 217–235

[55]. P. Hall, B. U. Park & R. J. Samworth, “Choice of neighbor order in nearest-neighbor classification”, The Annals of Statistics, 2008, vol. 36, Issue 5, pp. 2135–2152

[56]. X. S. Yang & S. Deb, “Engineering optimisation by cuckoo search”, 2010, arXiv preprint arXiv:10052908

[57]. A. Martin & C. Osswald, “A new generalization of the proportional conflict redistribution rule stable in terms of decision”, Advances and Applications of DSmT for Information Fusion- Collected Works, 2006, vol. 2, Issue 2, pp. 69–88

[58]. J. Dezert & F. Smarandache, “Proportional conflict redistribution rules for information fusion”, Advances and applications of DSmT for Information Fusion-Collected works, 2006, vol. 2, pp. 3–68

[59]. T. Denœux & M. H. Masson, “Dampster-shafer reasoning in large partially ordered sets: Applications in machine learning”, Integrated Uncertainty Management and Applications, Springer, 2010, pp. 39–54

[60]. K. Veeramachaneni, L. A. Osadciw & P. K. Varshney, “An adaptive multimodal biometric management algorithm”, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2005, vol. 35, Issue 3, pp. 344–356

[61]. D. L. Spacek, “Computer vision science research projects”, http://cswww.essex.ac.uk/mv/ allfaces/

[62]. F. S. Samaria & A. C. Harter, “Parameterisation of a stochastic model for human face identification”, Applications of Computer Vision, Proceedings of the Second IEEE Workshop on Computer Vision, IEEE, 1994, pp. 138–142

[63]. A. Kumar & A. Passi, “Comparison and combination of iris matchers for reliable personal authentication”, Pattern Recognition, 2010, vol. 43, Issue 3, pp. 1016–1026

[64]. “Casia-irisv1”, http:// biometrics.idealtest.org

[65]. E. Gonzalez, “AMI Ear Dataset”, http://ctim.ulpgc.es/research_works/ ami_ear_database/

[66]. A. Kumar & C. Wu, “Automated human identification using ear imaging”, Pattern Recognition, 2012, vol. 45, Issue 3, pp. 956–968

[67]. J. Daugman “Biometric decision landscapes”,University of Cambridge, Computer Laboratory, 2000.

[68]. N. Poh & S. Bengio, “Why do multi-stream, multi-band and multi-modal approaches work on biometric user authentication tasks ?”, Acoustics, Speech, and Signal Processing, (ICASSP’04), IEEE, 2004, vol. 5, pp. V–893

[69]. J. Kittler, M. Hatef, R. P. W. Duin & J. Matas, “On combining classifiers, IEEE Transactions on Pattern Analysis and Machine Intelligence”, 1998, vol. 20, Issue 3, pp. 226–239

[70]. E. P. Klement, R. Mesiar & E. Pap, “Triangular norms: general constructions and parameterized families”, Fuzzy Sets and Systems, 2004, vol. 145, Issue 3, pp. 411–438

[71]. R. K. Asthana, G. S. Walia, A. Gupta, S. Rishi & A. Kumar, “A Secure Multimodal Biometric System based on Diffused Graphs and Optimal Score Fusion”, International Journal IET Biometrics, 2019, vol. 08, Issue 4, p. 231 – 242, DOI: 10.1049/iet-bmt.2018.5018

[72]. C. Soutar, D. Roberge, A. Stoianov, R. Gilroy & B. V. Kumar, “Biometric Encryption”, Chapter 22 in ICSA Guide to Cryptography, 1999, McGraw-Hill, pp. 1-28

[73]. A. Juels & M. Wattenberg, “A fuzzy commitment scheme”, 6th ACM Conference on Computer and Communications Security, ACM Press, 1999, pp. 28-36

[74]. A. Juels, & M. Sudan, “A fuzzy vault scheme”, IEEE Int. Symposium on Information Theory, 2002, pp.1-7

[75]. M. Blanton, & M. Aliasgari, “Analysis of Reusability of Secure Sketches and Fuzzy Extractors”, IEEE Transactions on Information Forensics and Security, 2013, vol. 8 Issue 9, pp. 1433-1445

[76]. M. S. Al-Tarawneh, W. L. Woo & S. S. Dlay, “Fuzzy Vault Crypto Biometric Key Based on Fingerprint Vector Features”, 6th International Symposium on Communication Systems, Networks and Digital Signal Processing, 2008, pp. 452-456

[77]. T. K. Dang, Q. Truong, C. Le & H. Truong, “Cancellable fuzzy vault with periodic transformation for biometric template protection”, IET Biometrics, 2016, vol. 5, Issue 3, pp. 229-235

[78]. T. C. Clancy, N. Kiyavash & D. J. Lin, “Secure smartcard-based fingerprint authentication”, Proc. of ACM SIGMM Multimedia, Biometrics Methods and Applications Workshop, 2003, pp. 45-52

[79]. P. Li, X. Yang, K. Cao, X. Tao, R. Wang & J. Tian, “An alignment-free fingerprint cryptosystem based on fuzzy vault scheme”, Journal of Network and Computer Applications, 2010, vol. 33, Issue 3, pp. 207-220

[80]. R. A. Marino, F. H. Alvarez & L. H. Encinas, “A crypto-biometric scheme based on iris templates with fuzzy extractors”, Elsevier, Information Sciences, 2012, vol. 195, pp. 91-102

[81]. M. Salas, “A secure framework for OTA smart device ecosystems using ECC and biometrics”, Springer, Communications in Computer and Information Science, 2013, vol. 381, pp. 204-381

[82]. E. J. Yoon & K. E. Yoo, “A biometric based authenticated key agreement scheme using ECC for wireless sensor networks", International Conference on Management and Service Science, 2014, pp. 699-705

[83]. C. Z. Liew, R. Shaw, L. Li & Y. Yang, “Survey on biometric data security and chaotic encryption strategy with Bernoulli mapping”, International Conference on Medical Biometrics, 2014, pp. 174-180

[84]. G. S. Eskander, R. Sabourin & E. Granger, “A bio-cryptographic system based on offline signature images”, Elsevier, Information Sciences, 2014, vol. 259, pp. 170-191

[85]. G. Amirthalingam & G. Radhamani, “New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization”, Elsevier, Journal of Computer and Information Sciences, 2016, vol. 28, pp. 381-394

[86]. D. Chitra & V. Sujitha, “Security analysis of prealigned fingerprint template using fuzzy vault scheme”, Cluster Computing, 2018, vol. 22, pp. 12817–12825

[87]. L. A. Elrefaei & A. L. Mohammadi, “Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme”, Journal of Computer and Information Sciences, 2019, pp. 1-14

[88]. H. W. Ponce, R. B. Gonzalo, J. L. Jimenez & R. Sanchez, “Fuzzy Vault Scheme Based on Fixed-Length Templates Applied to Dynamic Signature Verification”, IEEE Access, 2020, vol. 8, pp. 11152-11164

[89]. G. S. Walia, K. Aggarwal, K. Singh & S. Kunwar, “Design and Analysis of Adaptive Graph based Cancelable Multi-Biometrics Approach”, IEEE Transactions on Dependable and Secure Computing, 2020, DOI:10.1109/tdsc.2020.2997558

[90]. R. K. Asthana, G. S. Walia & S. Raza, “A Novel Approach of Multi-Stage Tracking for Precise Localization of Target in Video Sequences”, Journal of Expert Systems with Applications, vol. 78, DOI: 10.1016/j.eswa.2017.02.007

[91]. G. S. Walia, K. Gupta & K. Sharma, “Quality based adaptive score fusion approach for multimodal biometric system”, Journal of Applied Intelligence, 2020, vol. 50, pp. 1086-1099

[92]. Y Chenggang, B. Gong, W. Yuxuan & Y. Gao, “Deep Multi-View Enhancement Hashing for Image Retrieval”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020

[93]. Y. Chenggang, L. Zhisheng, Z. Yongbing, L. Yutao, J. Xiangyang & Z. Yongdong, “Depth image denoising using nuclear norm and learning graph model”, ACM Transactions on Multimedia Computing Communications and Applications 2020

[94]. Y Chenggang, B. Shao, H. Zhao, R. Ning, Y. Zhang & F. Xu, “3D Room Layout Estimation from a Single RGB Image”, IEEE Transactions on Multimedia 2020

[95]. K. Ouyang, Y. Liang, Y. Liu, Z. Tong, S. Ruan, Y. Zheng & Rosenblum, “Fine-Grained Urban Flow Inference”, IEEE Transaction on knowledge and data engineering 2020

[96]. Y Zheng, “UrbanFM: Inferring Fine-Grained Urban Flows”, Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2019

[97]. A. Alfaisal & C. Mokbel, “Convolutional Neural Network Biometric Cryptosystem for the Protection of the Blockchain’s Private Key”, ScienceDirect, Procedia Computer Science, 2019, vol. 160, pp. 235-240

[98]. U. Uludag, S. Pankanti, S. Prabhakar & A. K. Jain, “Biometric Cryptosystems: Issues and Challenges”, Proceedings of IEEE conference, vol. 92, Issue 6, Jun. 2004

[99]. J. Daugman, “How Iris Recognition Works ?”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, Issue 1, pp.21-30

[100]. https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm

[101]. http://biometrics.idealtest.org/dbDetailForUser.do?id=7

[102]. A. S. Waisy, R. Qahwaji, S. Ipson, S. Al-Fahdawi & T. A. M. Nagem, “A multi-biometric iris recognition system based on a deep learning approach”, Pattern Analysis and Applications, Springer, 2017, vol. 21, pp. 783-802

[103]. R. Subban, N. Susitha & D. P. Mankame, “Efficient iris recognition using Haralick features based extraction and fuzzy particle swarm optimization”, Cluster Computing, 2017, vol. 21, Issue 1, pp. 79-90

[104]. D. Ricco, C. Galdi & R. Manzo, “Biometric/Cryptographic Keys Binding based on Function Minimization”, 12th International Conference on Signal-Image Technology & Internet-based Systems, 2016, pp. 144-150

[105]. R. K. Asthana, G. S. Walia & A. Gupta, “A Novel Biometric Crypto System based on Cryptographic Key Binding with User Biometrics”, International Journal of Multimedia Systems, Springer, 2021, vol. 27, Issue 5, pp 877-891, DOI: https://doi.org/10.1007/s00530-021-00768-8

[106]. Y. Sutcu, Q. Li & Memon, “Protecting biometric templates with sketch: Theory and practice”, IEEE Transactions on Information Forensics and Security, 2007, vol. 2, Issue 3, pp. 503–512

[107]. J. H. Uhl, A. Uhl & E. Pschernig, “Cancelable iris biometrics using block re-mapping and image warping”, Information Security, Lecture Notes in Computer Science, Spronger, 2009, vol. 5735, pp. 135–142

[108]. K. Takahashi & S Hirata, “Cancelable biometrics with provable security and its application to fingerprint verification”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, vol. 94-A, Issue 1, pp. 233–244

[109]. W. Johnson & J. Lindenstrauss, “Extensions of lipschitz maps into a hilbert space”, Contemporary Mathematics, 1984, vol. 26, pp. 189–206

[110]. K. Nandakumar & A. K. Jain, “Biometric template protection: Bridging the performance gap between theory and practice”, IEEE Signal Processing Magazine, 2015, vol. 32, Issue 5, pp. 88-100

[111]. N. K. Ratha, V. M. Patel & R. Chellappa, “Cancelable biometrics: A review”, IEEE Signal Processing Magazine, 2015, vol. 32, Issue 5, pp. 54-65.

[112]. A. Goh & D. L. Ngo, “Computation of Cyrptographic Keys from Face Biometrics”, Proc. IFIP: Int’l Federation for Information Processing, 2003, pp. 1-13

[113]. N. K. Ratha, J. Connell & S. Chikkerur, “Cancelable Biometrics: A Case Study in Fingerprints”, Proc. Int’l Conf. Pattern Recognition, 2006

[114]. G, I. Davida, Y. Frankel & B. J. Matt, “On enabling secure applications through off-line biometric identification”, IEEE Symposium on Security and Privacy, 1998, pp. 148–157

[115]. N. K. Ratha, J. Connell & R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM System Journal, 2001, vol. 40, Issue 3, pp. 614–634

[116]. A. Juels & M. Sudan, “A fuzzy vault scheme”, Designs, Codes and Cryptography, 2006, vol. 38, Issue 2, pp. 37–257

[117]. A. Juels A & M. A. Wattenberg, “Fuzzy commitment scheme”, ACM Conference on Computer and Communications Security, 1999, pp. 28–36

[118]. R. Ang, S. N. Rei & L. McAven, “Cancelable key-based fingerprint templates”, Information Security and Privacy, 10th Australasian Conference, ACISP, 2005, pp. 242–252

[119]. S. Tulyakov, F. Farooq & V. Govindaraju, “Symmetric hash functions for fingerprint minutiae”, Proc. Int. Workshop Pattern Recog. for Crime Prevention, Security and Surveillance, 2005, pp. 30–38

[120]. A. B. J. Teoh, D. C. Ngo & A. Goh, “Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number”, Pattern Recognition, 2004, vol. 37, Issue 11, pp. 2245-2255

[121]. C. Rathgeb & A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics”, EURASIP Journal of Information Security, 2015

[122]. C. Soutar, D. Roberge, A. R. Stoianov, B. V. Gilroy & V. Kumar, “Biometrics encryption”, ICSA Guide to Cryptography, McGraw-Hill, 1999, pp. 649–675

[123]. D. Sadhya & B. Raman, “Generation of cancelable Iris templates via randomized bit sampling”, IEEE Transactions on Information Forensics and Security, 2019, vol. 14, Issue 11, pp. 2972-2986

[124]. R. P. Sharma & S Dey, “Fingerprint liveness detection using local quality features”, The Visual Computer, 2019, vol. 35, Issue 10, pp. 1393-1410

[125]. I. I. Ganapathi, S. S. Ali, S. Prakash, P. Consul & Mahyo, “Securing biometric user template using modified minutiae attributes”, Pattern Recognition Letters, 2020, vol. 129, pp. 263-270

[126]. A. K. Trivedi, D. Thounaojam & S. Pal, “Non-Invertible cancellable fingerprint template for fingerprint biometric”, Computers & Security, 2020, vol. 90

[127]. S. C. Wu, P. T. Chen, A. L. Swindlehurst & P. L. Hung, “Cancelable biometric recognition with ECGs: subspace-based approaches”, IEEE Transactions on Information Forensics and Security, 2019, vol. 14, Issue 5, pp. 1323-1336

[128]. N. Kumar, S. Singh & A. Kumar, “Random permutation principal component analysis for cancelable biometric recognition”, Applied Intelligence Journal, 2018, vol. 48 Issue 9, pp. 2824-2836

[129]. R. Dwivedi & S. Dey, “A novel hybrid score level and decision level fusion scheme for cancellable multi-biometric verification”, Applied Intelligence Journal, 2019, vol. 49, Issue 3, pp. 1016 – 1035

[130]. H. Kaur & P. Khanna, “Random distance method for generating unimodal and multimodal cancellable biometric features”, IEEE Transactions on Information Forensics and Security, 2018, vol. 14, Issue 3, pp. 709-719

[131]. G. S. Walia, G. Jain, N. Bansal & K. Singh, “Adaptive Weighted Graph Approach to Generate Multimodal Cancelable Biometric Templates”, IEEE Transactions on Information Forensics and Security, 2019, vol. 15, pp. 1945-1958, DOI: 10.1109/TIFS.2019.2954779

[132]. C. Rathgeb et al., “Multi-biometric template protection based on bloom filters”, Information Fusion, 2018, vol. 42, pp. 37-50

[133]. E. Abdellatef, N. A. Ismail, S. A. Elrahman, K. N. Ismail, M. Rihan & F. E. A. El-Samie, “Cancelable multi-biometric recognition system based on deep learning”, The Visual Computer, 2019, pp. 1-13

[134]. J. Zuo, N. K. Ratha & J. H. Connell, “Cancelable iris biometric”, 19th International Conference on Pattern Recognition (ICPR), IEEE, pp. 1–4, DOI: 10.1109/ICPR.2008.4761886.

[135]. Y. Wang & K. N. Plataniotis, “An analysis of random projection for changeable and privacy-preserving biometric verification”, IEEE Trans. Syst. Man, Cybern. Part B (Cybernetics), vol. 40, pp. 1280–1293, DOI: 10.1109/TSMCB.2009.2037131

[136]. E. Maiorana, P. Campisi & A. Neri, “Bioconvolving: cancelable templates for a multi-biometrics signature recognition system”, IEEE International Systems Conference (SysCon) 2011, pp. 495–500, DOI:10.1109/SYSCON.2011.5929064

[137]. L. Leng & J. Zhang, “PalmHash code vs. PalmPhasor code”, Neurocomputing, Elsevier, 2013, vol. 108: 1–12, DOI: 10.1016/j.neucom.2012.08.028

[138]. L. Leng, “Two Dimensional PalmPhasor Enhanced by Multi-orientation Score Level Fusion”, Communications in Computer and Information Science book series (CCIS), Springer, 2009, vol. 186, DOI: https://doi.org/10.1007/978-3-642-22339-6_15

[139]. S. Cho & A. B. Teoh, “Face template protection via random permutation maxout transform”, Proceedings of the International Conference on Biometrics Engineering and Application (ICBEA), ACM International Conference Proceeding Series; vol. Part F128052, pp. 21–27, DOI : https://doi.org/10.1145/3077829.3077833

[140]. H. Kaur & P. Khanna, “Cancelable features using log-gabor filters for biometric authentication”, Multimedia Tools Applications, 2017, vol. 76, pp. 4673–4694, DOI: 10.1007/s11042-016-3652-3

[141]. H. Kaur & P. Khanna, “Random Slope method for generation of cancelable biometric features”, Pattern Recognition Letters, Elsevier, 2019, vol. 126, pp. 31–40, DOI : https://doi.org/10.1016/j.patrec.2018.02.016

[142]. H. Kaur & P. Khanna, “Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features”, IEEE Transactions on Information Forensics and Security, 2019, vol. 14, Issue 3, pp. 709-719, DOI : 10.1109/TIFS.2018.2855669

[143]. Z. Yinghui, Xu S, Li Yingjiu, L. Ximeng & Y. Guomin, “Generic Construction of ElGamal-Type Attribute-Based Encryption Schemes with Revocability and Dual-Policy”, Proceedings of the 15th EAI International Conference, SecureComm 2019, Springer, vol. 10, pp. 184-204, DOI : 10.1007/2F978-3-030-37231-6_10

[144]. K Liang, W. Yin, Q. Wen, Z. Zhang, L. Chen, H. Yan & H. Zhang, “Delegation of Decryption Rights With Revocability From Learning With Errors”, IEEE Access, 2018, vol. 6, pp. 61163-61175, DOI : 10.1109/ACCESS.2018.2875069

[145]. S. Wang, G. Deng & J. Hu, “A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations”, Pattern Recognition, 2017, vol. 61, pp. 447-458, DOI :10.1016/j.patcog.2016.08.017

[146]. R Redondo, F. Sroubek, S. Fischer & G. Crist´obal, “Multifocus image fusion using the log-Gabor transform and a multisize windows technique”, Information Fusion, Elsevier, 2007, vol. 10, Issue 2, pp. 163–171, DOI : https://doi.org/10.1016/j.inffus.2008.08.006

[147]. W. Wang, J. Li, F. Huang & H. Feng, “Design and implementation of log-gabor filter in fingerprint image enhancement”, Pattern Recognition Letters, 2008, vol. 29, pp. 301–308, DOI : 10.1016/j.patrec.2007.10.004

[148]. G. Farin, “Curves and Surfaces For Computer Aided Geometric Design : A Practical Guide”, Academic Press, 2nd edition, ISBN 978-0-12-249052-1, 1999, DOI : https://doi.org/10.1016/C2009-0-22351-8

[149]. T. Tan, H. Zhaofeng & Z. Sun, “Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition”, Image and Vision Computing, 2010, vol.28, Issue 2, pp. 223-230

[150]. T. Tan & L. Ma, “Iris Recognition: Recent Progress and Remaining Challenges”, Proc. of SPIE, 2004, vol. 5404, pp. 183-194

[151]. Z Sun & T. Tan, “Ordinal Measures for Iris Recognition”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2009, vol. 31, Issue 12, pp. 2211 - 2226

[152]. Y Yin, L. Liu & X. Sun, “SDUMLA-HMT: A Multimodal Biometric Database”, CCBR 2011, LNCS 7098, Springer, pp. 260–268

[153]. R. K. Asthana, G. S. Walia & A. Gupta, “Random Area-Perimeter Method for Generation of Unimodal and Multimodal Cancelable Biometric Templates”, International Journal of Applied Intelligence, Springer, 2021, DOI : https://doi.org/ 10.1007/s10489-021-02201-z

Appendix-A

List of Publications

1. Rajesh Asthana, G. S. Walia & A. Gupta, "A Novel Biometric Crypto System based on Cryptographic Key Binding with User Biometrics", International Journal Multimedia Systems, Springer, SCI, 2021, vol. 27(5), pp 877-891
   DOI: https://doi.org/10.1007/s00530-021-00768-8

2. Rajesh Asthana, G. S. Walia & A. Gupta, "Random Area-Perimeter Method for Generation of Unimodal and Multimodal Cancelable Biometric Templates", International Journal of Applied Intelligence, Springer, SCI, 2021, vol. 51(10), pp. 7281-7297
   DOI: https://doi.org/ 10.1007/s10489-021-02201-z

3. Rajesh Asthana, G. S. Walia, A. Gupta, S. Rishi & A. Kumar, "A Secure Multimodal Biometric System based on Diffused Graphs and Optimal Score Fusion", International Journal IET Biometrics, 2019, vol. 08, Issue 4, p. 231 – 242, SCIE
   DOI: 10.1049/iet-bmt.2018.5018

4. Rajesh Asthana, G. S. Walia & A. Gupta, "Score Level Fusion for Optimal Multi-Modal Biometric Authentication System", International Conference on Recent Developments in Computer & Information Technology - (ICRDCIT-21) (Presented)

5. Rajesh Asthana, G. S. Walia & A. Gupta, "A Novel Scheme for Efficient Biometric System based on Fusion Techniques", International Conference on Recent Developments in Computer & Information Technology - (ICRDCIT-21) (Presented)

6. Rajesh Asthana, G. S. Walia, D. Singh & A. Dube, "A Framework for Evaluation of Biometric based Authentication System". 3rd International Conference on Intelligent Sustainable Systems (ICISS 2020) (Presented)

Appendix-B

Biodata

Rajesh Kumar Asthana completed his graduation (B. Sc.) from DDU University, Gorakhpur (UP) in 1995. He received his Master's Degree (M. Sc.) in Mathematics from DDU University, Gorakhpur (UP) in 1997. Presently, he holds the position of Scientist 'E' in Scientific Analysis Group, DRDO, Ministry of Defence, Government of India. He has worked in the field of Cryptography, Machine Learning and Statistical Analysis. He has published more than 30 research papers, prepared more than 50 technical reports and obtained 02 copyrights on statistical analysis software tools. He joined Delhi Technological University, New Delhi as part time Ph.D Scholar in Applied Mathematics department under the supervision of Prof. Anjana Gupta and Dr. Gurjit Singh Walia in 2016. His current research focuses on biometric authentication systems, biometric template protection mechanisms and biometric cryptosystems. He has proposed various robust and efficient methods in these research areas.