SEQUENTIAL SUBSPACE ESTIMATOR FOR AN EFFICIENT MULTIBIOMETRICS AUTHENTICATION AND ENCRYPTION

By

MD. OBAIDUL MALEK

M.A.Sc, McMaster University 2009

B.Sc (Honors), University of Dhaka 1994

A Dissertation

presented to Ryerson University

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

in the program of

Electrical and Computer Engineering

Toronto, Ontario, Canada

Author's Declaration

I hereby declare that I am the sole author of this dissertation. This is a true copy of the dissertation, including any required final revisions, as accepted by my examiners. I authorize Ryerson University to lend this dissertation to other institutions or individuals for the purpose of scholarly research I further authorize Ryerson University to reproduce this dissertation by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my dissertation may be made electronically available to the public.

Abstract

SEQUENTIAL SUBSPACE ESTIMATOR FOR AN EFFICIENT MULTIBIOMETRICS AUTHENTICATION AND ENCRYPTION

Doctor of Philosophy 2015

Md. Obaidul Malek

Department of Electrical and Computer Engineering

Ryerson University

The principal challenge in biometric authentication is to mitigate the effects of any noise while extracting biometric features for biometric template generation. Most biometric systems are developed under the assumption that the extracted biometrics and the nature of their associated interferences are linear, stationary, and homogeneous. When these assumptions are violated due to nonlinear, nonstationary, and heterogeneous noise, the authentication performance deteriorates. As well, demands for biometric templates are on the rise in the field of information technology, leading to an increase in the vulnerability of stored and dynamic information. Thus, the development of a sophisticated authentication and encryption method is necessary to address these challenges.

This dissertation proposes a new Sequential Subspace Estimator (SSE) algorithm for biometric authentication. In the proposed method, a sequential estimator is being designed in the image subspace that addresses challenges arising from nonlinear,

nonstationary, and heterogeneous noise. The proposed method includes a subspace technique that overcomes the computational complexity associated with the sequential estimator. In addition, it includes a novel MultiBiometrics encryption algorithm that protects the biometric templates against security, privacy, and unlinkability attacks. Unlike current biometric encryption, this method uses cryptographic keys in conjunction with extracted MultiBiometrics to create cryptographic bonds, called "*BioCryptoBond*". To further enhance system security and improve authentication accuracy, the development of a biometric database management system is also being considered. The proposed method is being tested on images from three public databases: the "Put Face Database", the "Indian Face Database", and the "CASIA Fingerprint Image Database Version 5.1". The performance of the proposed solution has been evaluated using the Equal Error Rate (EER) and Correct Recognition Rate (CRR). The experimental results demonstrate the superiority of the proposed method in comparison to its counterparts.

Acknowledgements

First and foremost, my praise and gratitude goes to Almighty God, *Allah*, our Creator, the Most Merciful, the Most Compassionate. Without the help of *Allah*, none of the work in my life would have come to light. I am simply very thankful to *Allah* for allowing me to recognize these rewards. By the grace of *Allah*, I have had the opportunity to be blessed with several extraordinary people in my life whose presence, love, cooperation, and contributions have helped me to achieve my goals. I humbly acknowledge their undeniable contributions and dedication to my success.

I would like to express my special thanks to my supervisors, Prof. Anastasios Venetsanopoulos and Prof. Dimitrios Androutsos. They have been instrumental in the development of my academic expertise, and in organizing me to establish myself as a graduate research fellow. I have benefited tremendously from their leadership, and interest in developing the intellectual and personal growth of their high profile team members. The results in this dissertation would not have been possible without their

engaging and insightful discussions. They have always been committed, supportive, and flexible, and have shown understanding during hard times. Certainly, they have left an indelible mark upon me, and there is still much I can learn from them. In fact, their leadership, support, expertise, and openness were vital to the successful completion of my PhD degree. I am honoured to have had Prof. Venetsanopoulos and Prof. Androutsos as my supervisors. In a nutshell, they are much more than supervisors to me; perhaps I have blessed by *Allah* to have had the opportunity to work with these two extraordinary supervisors.

My deepest gratitude and appreciation goes to my Mother Sofia Malek and my Sister Dr. Laila Alamgir, MD. Their uninterrupted love and encouragement have been tremendous in inspiring me to pursue this higher study. They have taught me to make my own decision. Without their love, motivation, and support, I wouldn't be what I am today.

From the bottom of my heart, I would like to thank my wife Salma, and my two daughters Sophia and Sadia. During my time of study, they have always shown patience, perseverance, and continuous understanding. No one has been impacted by my PhD degree more than them.

I would also like to sincerely thank my father Prof. A. Malek, father-in-Law A. Hoque, brother A. Malek, and brother-in-law Attorney M. Alamgir for their continuous support, motivation, and cooperation.

I have been surrounded by numerous great friends, group members, lab members, our program administrator, and our technical staff who are hard to forget; my sincere thanks for all of their support.

Special thanks to all of the faculty members of Ryerson University; especially Prof. S. Krishnan, Prof. Anpalagan, Prof. Zhao, Prof. Guan, Prof. Alirezaie, Dr. M. Kyan, and Dr. J. Smith whose direct and indirect contributions helped me explore my research in this area. I would also like to extend my special thanks to Prof. E.

Petriu and Prof. A. Sadeghian.

Finally, I am grateful to all my school teachers, faculties of University of Dhaka, and to every individual who has taught me in some way.

Dedications To My

Mother Sofia Malek

Sister Dr. Laila Alamgir, MD

and

Wife Salma, and Two Daughters Sophia and Sadia

Contents

List of Figures

List of Acronyms, Keys and Bonds

BE	Biometric Encryption
BDMS	Biometrics Data Management System
CRR	Correct Recognition Rate
DOS	Department of State
EER	Equal Error Rate
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FOB	Forward Operating Base
FOV	Field of View
FRR	False Rejection Rate
i.i.d	Independent and Identically Distributed
MLE	Maximum Likelihood Estimator
NGI	Next Generation Identification
PCA	Principal Component Analysis
ROC	Receiver Operating Characteristics

Digital	**Random Keys**
K^s	Subject -Facial or Fingerprint Biometric Features
$K^{s'}$	Subject -MultiBiometrics (Facial and Fingerprint)
K^u	User -Fingerprint Biometric Features
Cryptographic	**Bonds**
BioCryptoBond_u	Cryptographic Bond -User
BioCryptoBond_F	Cryptographic Bond -Facial Features
$\text{BioCryptoBond}_{FF}$	MultiBiometrics Cryptographic Bond -Facial and Fingerprint
$\text{BioCryptoBond}_{FP}$	Cryptographic Bond -Subject Fingerprint Features

List of Special Characters, Databases, and Notations

(α)	Noise due to Non-Cooperative Moving Target
(μ)	Expected Value or Mean
$(\digamma)$	Fourier Transformation
(Ω)	Noise Vector
(θ)	Orientation Angle
(Π)	Orthogonal Matrix
(Υ)	Output of Segmentation Operation
(Γ)	Output of Tensor Operation
(β)	User and Subject Interface Pointer
(σ)	Variance of Desired Signal
$Encryption_u$	Database -Encrypted User Fingerprint Features
$Encryption_F$	Database -Encrypted Subject Facial Features
$Encryption_{FF}$	Database -Encrypted Subject MultiBiometrics
$Encryption_{FP}$	Database -Encrypted Subject Fingerprint
Subject Database dB_s	Subject Master Database
Temp Tracking Database	Temporary Tracking Database
User Database dB_u	User Master Database

List of	**Notations**
j	the unit imaginary number $j = \sqrt{-1}$
$(\cdot)^*$	the conjugate operator
$(\cdot)^T$	the transpose of a vector or a matrix
$(\cdot)^H$	the Hermitian transpose of a vector or a matrix
$(\cdot)^{-1}$	the inversion of a matrix
$\lvert \cdot \rvert$	the determinant of a matrix
$\lVert \cdot \rVert$	the Euclidean norm of a vector
$\otimes$	the Kronecker matrix product
∇	the gradient operator
λ	the operating wavelength

Chapter 1

Introduction

The rapid evolution of information technology has rendered the traditional token-based authentication and security management system no longer be sophisticated enough to handle the challenges of the 21^{st} century. As a result, biometrics has emerged as the most reasonable, efficient, and ultimate solution to authenticate the legitimacy of an individual. The origin of the word ′biometric′ comes from the two Greek words ′bio′ and ′metrics′, which mean ′life′ and ′to measure′. The main objective of biometrics is to uniquely authenticate a known or unknown individual by using their physiological characteristics. However, the concept of authentication using behavioral characteristics, such as gait and voice, has also become popular over the last several decades, since an individual uses these characteristics somewhat instinctively. Thus, the study of biometric systems became a science that statistically analyzes and measures both human physiological and behavioral characteristics [1],[2].

The physiological and appearance-based biometric traits including facial, fingerprint, and gait are the oldest, simplest, and most reliable sources of biometric characteristics. These traits have been used to authenticate known and unknown individuals since the beginning of civilization. The advent of computer technology along with the rise in security and privacy concerns led to the emergence of biometric systems in the

late 20^{th} century. However, the growing demands of an ever-increasing population has caused the once simple task of authentication to become more challenging due to computational complexity, intra-class variations, and inter-class similarities. The potential of biometric technology is ever-increasing after the tragic 9/11 attacks on the United States [3],[4]. As a result, the Federal Bureau of Investigation (FBI) officially launched a state-of-the-art face recognition project at a cost of one billion US dollars, a milestone in the development of the Next Generation Identification (NGI) program. This program is a compilation of initiatives that serve to improve or expand the existence of biometric systems, and accelerate information processing and sharing demands in support of anti-terrorism. In November 2012, the FBI also revealed a new request to produce a mobile biometric hand-held software solution to become a part of their biometric identification. This mobile methodology would allow them to capture biometric and biographic information in real time, anywhere in the world [3]. This dissertation systematically investigates the challenges associated with the biometric systems and proposes a novel method to overcome them.

This chapter is organized as follows: Section 1.1 presents an overview of biometric systems; Section 1.2 discusses the challenges associated with biometric systems; Section 1.3 examines the proposed method and its objectives, contributions, and application areas; and Section 1.4 includes the organization of the remaining chapters.

1.1 Biometric Systems

The fundamental architecture of the biometric system is based on the extraction of irrevocable physiological and behavioral features, their conversion into useful information, and the utilization of that information for its intended purpose, such as verifying the authenticity of an individual. Ideally, it is an automated method for identifying an individual using computer-aided algorithmic formulations. With the unprecedented

growth of biometric systems, concerns about security, privacy, and unlinkability attacks are the crucial issues for the 21^{st} century. Not only does the biometric template (another term for biometric features) contain the unique and sensitive physiological and behavioural traits of an individual, it is also unary, and cannot be revoked or reissued if compromised.

The most common biometric traits are fingerprint, face, iris, hand geometry, gait, voice, signature, and keystrokes. Each biometric trait has its own strengths and weaknesses [5],[6]. However, fingerprint, iris, face, and gait biometric traits are widely used in the field of biometrics and are discussed in the following subsections.

Fingerprint

As mentioned earlier, the fingerprint is the most reliable and secure biometric trait in the field of biometric systems. A fingerprint is made up of a series of ridges and furrows on the surface of the finger. Ridges are the segments in the upper skin layer of the finger, consisting of minutiae points, ridge endings, ridge bifurcations, and core points. These components determine the uniqueness of the fingerprint. This biometric is comparatively cost effective, non-intrusive, and easy to use. Application areas include: cell phones, access control, law enforcement, background checks, and notebook computers. The most common fingerprint biometric patterns are shown in Fig. 1.1 [7-11].

Iris

The iris as a biometric identifier is a new, but efficient and robust biometric trait. It is the thin circular structure in the eye responsible for controlling the diameter and size of the pupil, and is the only visible internal human organ that uniquely identifies an individual. The iris is protected by the cornea and gives the eye its color. Glasses, contact lenses, and even eye surgery can′t change the pattern of the

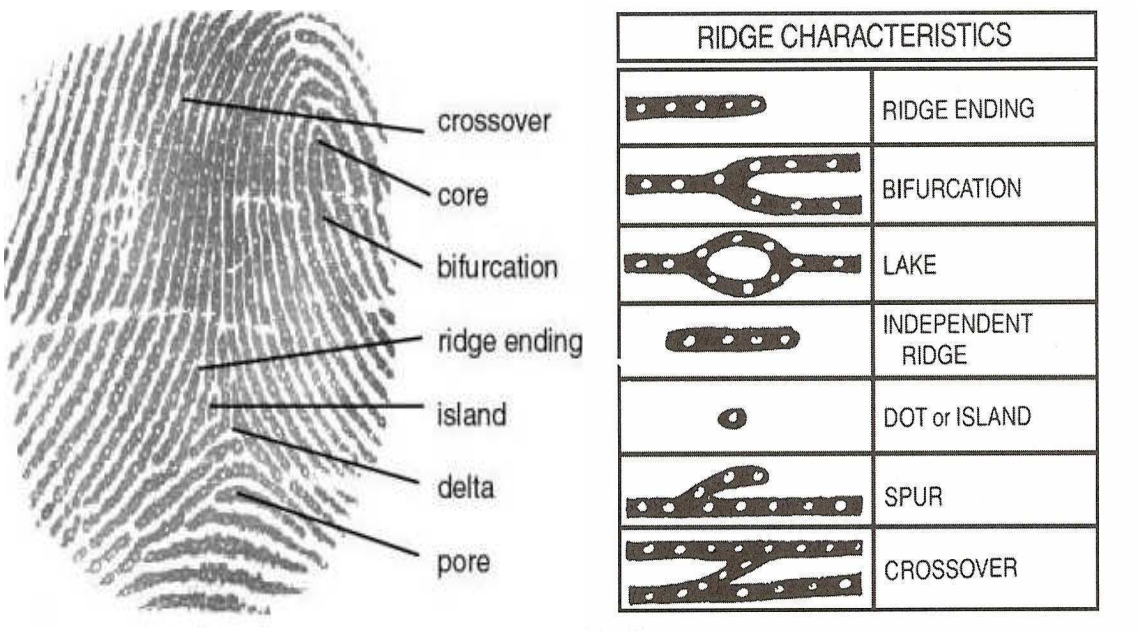
iris. Typically, camera technology with subtle infrared illumination can be used to scan and even analyze over 200 points of the iris (i.e. rings, furrows, and corona). The main advantages of iris technology are its processing speed and very low false matching rate; however, the user must hold still at the time of scanning. Typical application areas are in identification cards, passports, and security systems. The most common iris biometric patterns are shown in Fig. 1.2 [12-15].

Face

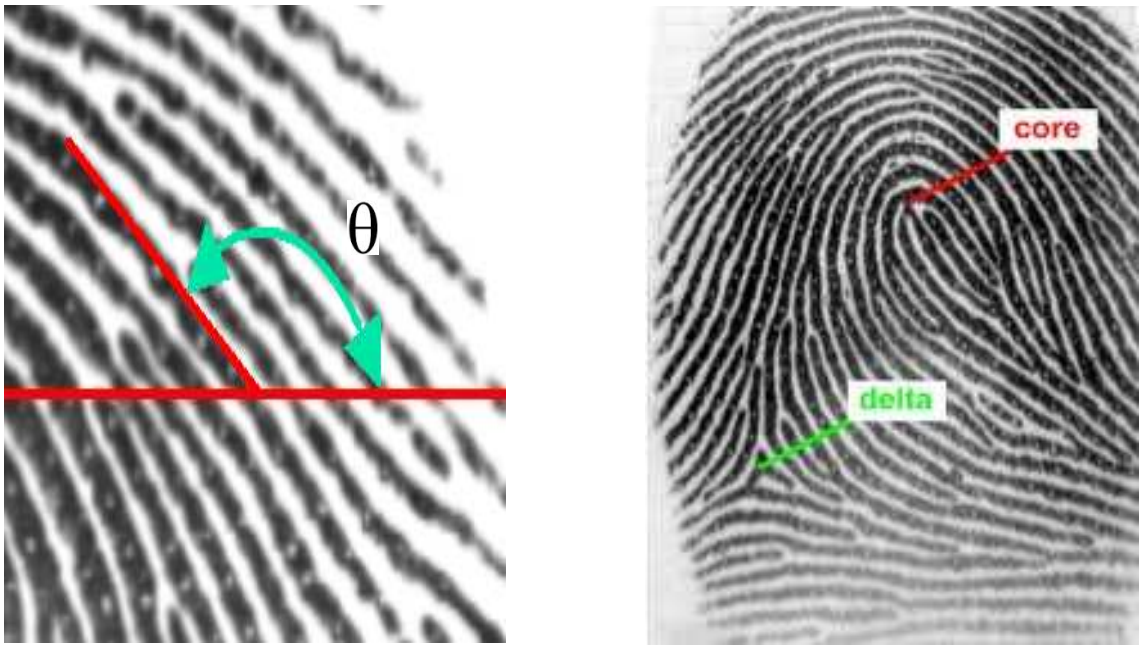
Identification of an individual by facial geometrical physiology can be achieved by extracting facial biometric features, including size or shape of the eyes, nose, lips, cheekbone, and jaw, as well as their relative distance and orientation. Authentication typically uses an algorithm that compares input data with the biometrics stored in the database. The authentication process based on facial features is fast and accurate under favorable constraints, and as a result this technology is evolving rapidly. Biometric authentication using facial biometrics can also be accomplished easily in public or noncooperative environments; the subject's awareness is not required. Typical application areas for facial biometrics are in passports, voter ID cards, driver's licenses, access control, and surveillance zones. The most common facial biometric patterns are shown in Fig. 1.3 [16-20].

Gait

The gait is a behavioral characteristic used to recognize an individual by the particular way they move on foot. Unlike other biometrics, it is based on the dynamic movement of the target. Gait biometric authentication can also be done easily in noncooperative environments. However, gait features are not robust enough. Studies show that the fusion of face and gait biometric features can improve the overall performance of a biometric system. Typical application areas of the fusion of these biometrics are in



(a) Fingerprint Ridges



(b) Orientation Angle, Core, and Delta Points

Figure 1.1: Fingerprint Biometric Patterns [7-11]

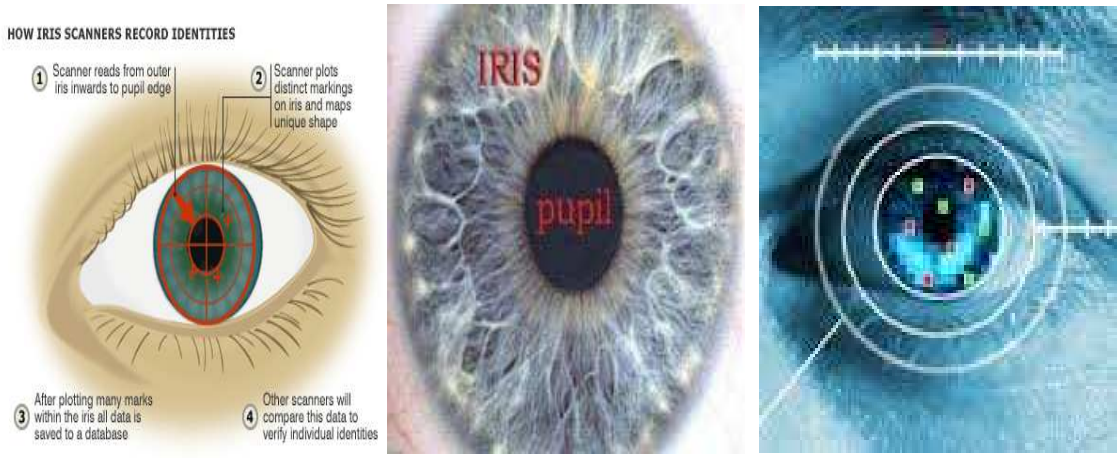


Figure 1.2: Iris Biometric Patterns [12-15]

access control and surveillance zones. The implementation method for the surveillance zone presented in Chapter 5 is based solely on facial biometrics, however. The most common gait biometric patterns are shown in Fig. 1.4 [21-26].

Soft Biometrics

Soft biometric traits are physical and behavioral characteristics that provide information about a subject but lack distinctiveness and permanence. They are easily collected, but cannot uniquely and reliably authenticate an individual. The most common soft biometrics are age, height, gender, and ethnicity. These biometrics in conjunction with the primary traits including face, fingerprint, and iris can enhance authentication accuracy. Authentication performance can be further improved by tuning or narrowing the parameters. These biometrics are not vulnerable to the individual's personal security and privacy. More importantly, soft biometrics can be used as a filtering tool in order to segment the large scale database, as well as to enhance the performance of the searching and authentication process of the biometric systems

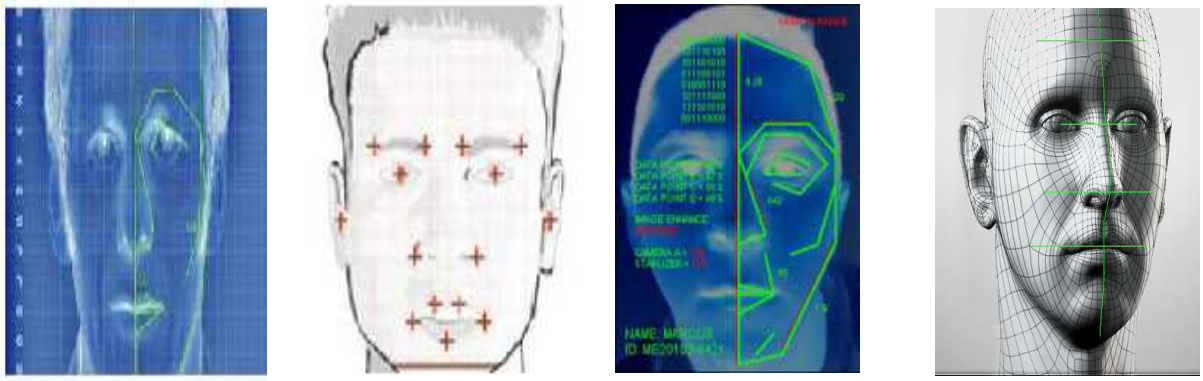


Figure 1.3: Facial Biometric Patterns [16-20]

[27].

The main operations performed on a biometric system can be categorized as encryption, enrollment, and authentication. These three operations are integral parts of each other and are briefly stated below.

1.1.1 Encryption and Enrollment

Encryption in a biometric system is essentially a mathematical or algorithmic formulation. It is used to cryptograph the plain biometric features in such a way that encoding or decoding should not require too much effort for the legitimate user but must be hard enough for the unintended user. The whole point of encryption is to keep biometric features out of the hands of unauthorized individuals. The strength of the encryption system is proportional to its ability to protect itself. An enrollment is a straightforward process where the system takes images or photographs of the user or subject. Afterwards, it detects and locates the area of interest to collect the necessary biometric information (features). The received information is then analyzed, and the useful biometric features are extracted and encoded based on certain algorithmic formulations. These encoded features or templates are then stored in the database

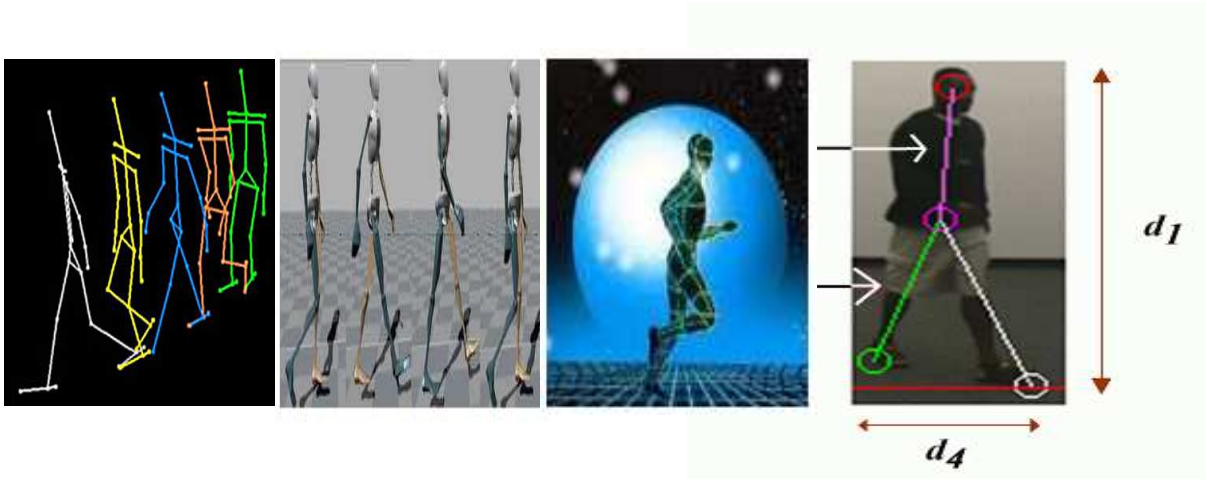


Figure 1.4: Gait Biometric Patterns [21-26]

system for future use.

1.1.2 Authentication

Biometric authentication (verification and identification) is an automated computer-aided algorithm for authenticating an individual based on their physiological and behavioural characteristics. Depending on the application context, a biometric authentication system can operate in either verification mode or identification mode. In the verification mode, the system performs a 1:1 comparison between the captured live biometric template and a specific template previously stored in the database system during the enrollment process. First, the system captures live biometrics from the claimed individual and creates a biometric template with the same algorithm used during the enrollment process. This new biometric template is used as a key to retrieve a specific template from the storage system. Using the matching algorithm, the two templates are compared to verify that the individual is the person they claim to be. On the other hand, in identification mode, the system performs 1 : *many*

comparisons. In this process the system compares the captured live biometric template with all of the stored templates in the databases in an attempt to establish the identity of the unknown individual [28],[29]. A simplified block diagram of the biometric encryption, enrollment, and authentication processes is shown in Fig. 1.5.

1.1.3 Biometric Modalities

Biometric modality is a method that ensures the type and number of biometrics that are used to analyze and create biometric templates. The effectiveness of the biometric system depends on the appropriate selection of this modality. Modality can be classified as monomodal or multimodal [28-30]. Typically, monomodal or monomodality uses a single sample from a single biometric trait captured by a single device. The probability of having noise using the monomodal technique is very high due to its imperfect and limited data acquisition facilities. Furthermore, the physiological and behavioral characteristics of an individual are always influenced by anatomical, pathological, emotional, and environmental factors. As a consequence, a monomodal biometric system faces authenticity, privacy, and security challenges due to biometric spoofing attacks, intra-class variation, inter-class similarities, inaccuracy, non-universality, and unreliability. More importantly, studies found that no single modality can achieve the optimal performance level required for a biometric system [28],[31].

On the other hand, multimodalities (multimodal or MultiBiometrics) represent a biometric authentication system that uses more than one biometric trait and source. In MultiBiometrics, biometric information is extracted from the multiple traits and sources (sensors, samples, backgrounds, algorithms, or/and units), and this information is manipulated, combined (or fused) for the exploitation of biometric encryption, enrollment, and authentication processes. The biometric system usually processes the biometric traits sequentially until the system achieves an acceptable recognition

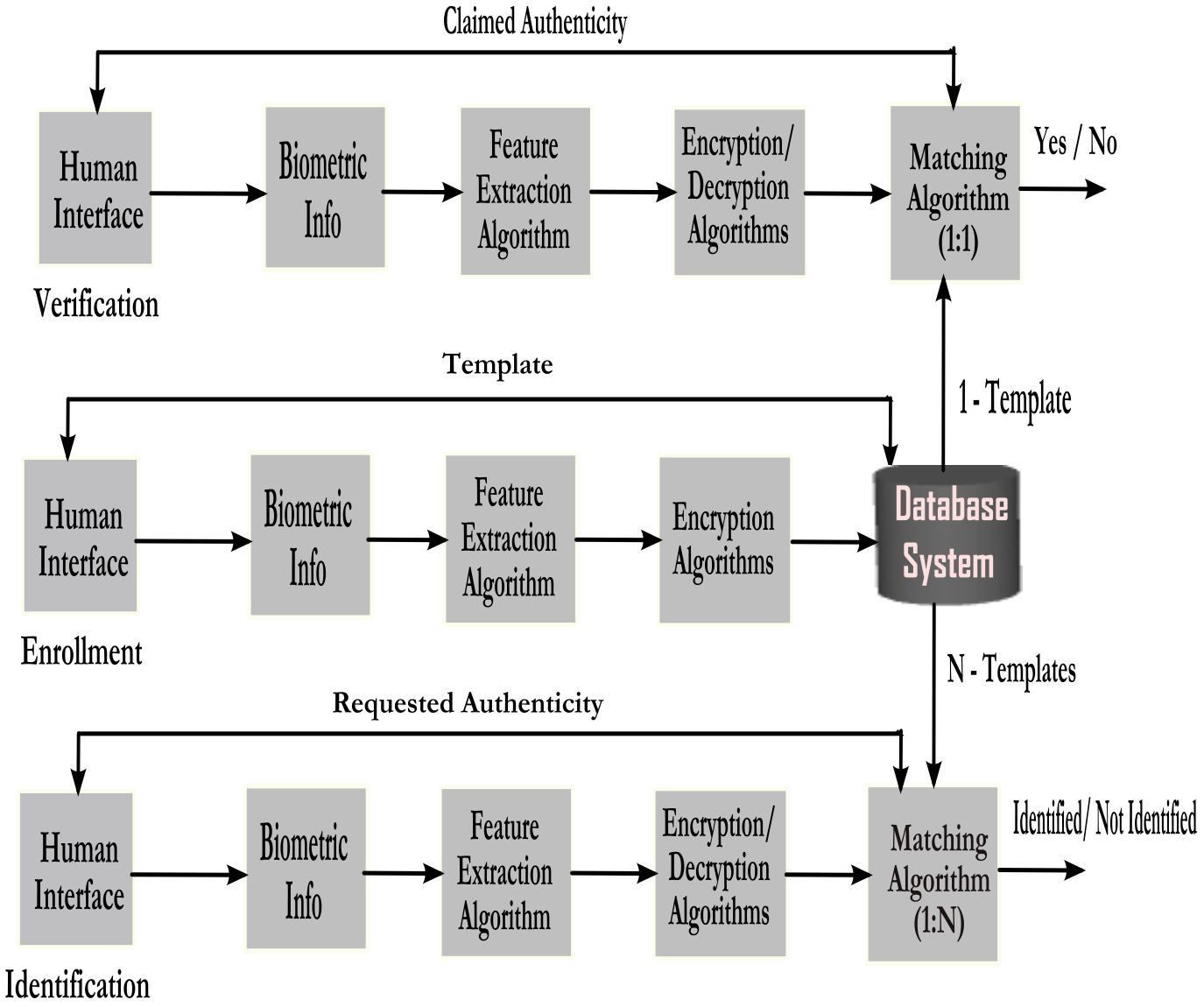


Figure 1.5: Biometric Verification, Enrollment, and Identification

score. MultiBiometrics in general and fusion in particular is a useful class of biometric recognition systems. It relies on the evidence presented by multiple sources and can overcome the challenges experienced by the monomodal biometric technique [28], [32-34].

1.1.4 Performance Analysis

A biometric is a measurable quantity. In fact, any measurable physiological or behavioral characteristic is a potential candidate for a practical biometrics system as long as it satisfies the following requirements [35],[36]:

- Universality: Every individual under consideration should possess the biometric characteristics.
- Measurability: Ease of measurement; quantitative analysis can be performed on the biometric characteristics.
- Distinctiveness: Two individuals should have sufficient distinguishable characteristics.
- Permanence: The characteristics should be time invariant.
- Performance: Achievable authentication accuracy, efficiency, and robustness of the biometric systems.
- Acceptability: An individual's willingness to accept a particular biometric.
- Circumvention: How easy it is to imitate a biometric.

A comparison of several biometric traits based on these properties is illustrated in Table 1.1.

More importantly, the performance of the biometric system depends on the percentages of the Correct Recognition Rate (CRR), False Acceptance Rate (FAR), and

Table 1.1: *A Comparison of Biometric Traits*

Traits	*Fingerprint*	*Face*	*Iris*	*Gait*	*Voice*
Universality	Low	High	Low	Medium	Low
Performance	High	Medium	High	Low	Low
Uniqueness	High	Low	High	Low	Low
Measurability	Medium	High	Medium	Low	Medium
Acceptance	Medium	High	Low	High	High
Circumvention	Low	High	Low	Medium	High

False Rejection Rate (FRR). The performance of a biometric identification system is evaluated based on CRR, which is the measure of the number of samples being correctly classified. CRR can be stated as:

$$CRR = \frac{\text{Number of samples being correctly classified}}{\text{Total number of test samples}}$$

whereas the performance of the verification algorithm can be evaluated by the FAR and FRR. In biometrics, the instance in which a biometric security system incorrectly authenticates an unauthorized person is known as a False Acceptance Rate (FAR), and can be stated as:

$$FAR = \frac{\text{Number of successful attempts by imposter}}{\text{Total number of attempts by imposter}}.$$

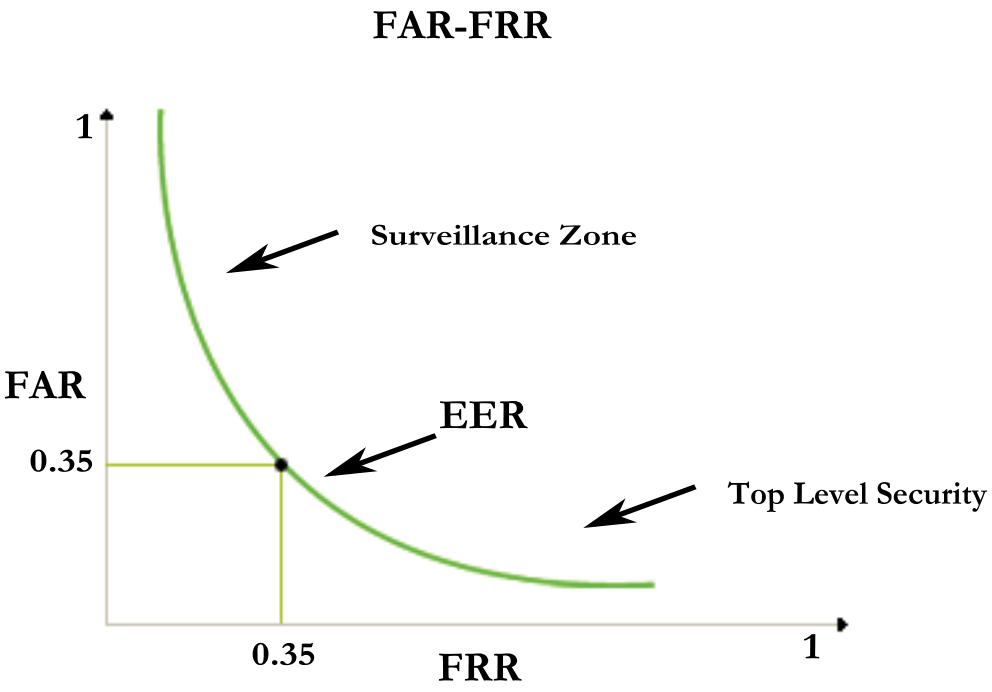
On the other hand, the failure to authenticate a legitimate user is known as a False Rejection Rate (FRR), and can be stated as:

$$FRR = \frac{\text{Number of failed attempts by legitimate user}}{\text{Total number of attempts by legitimate user}}.$$

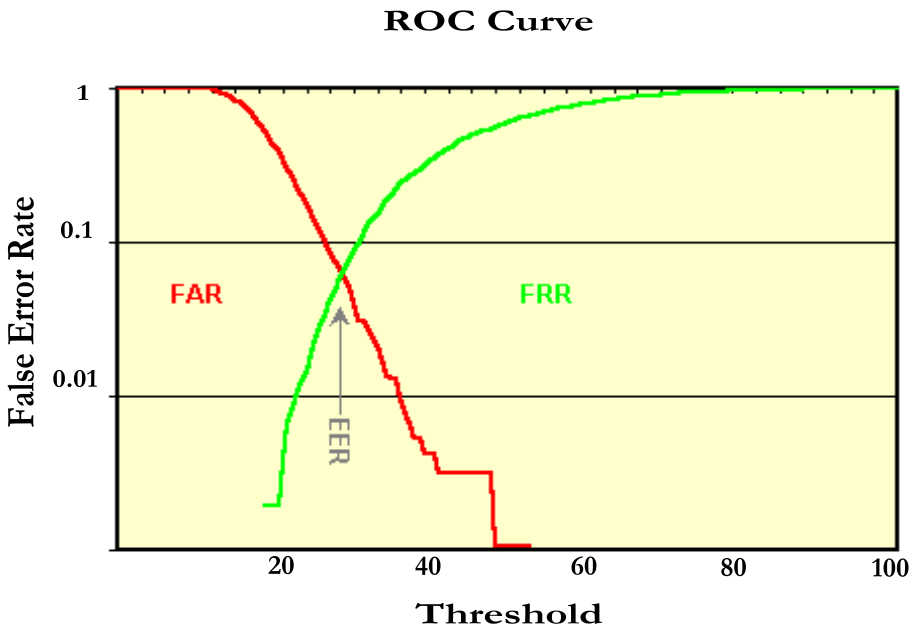
These are the crucial measures to evaluate the performance of a biometric system. If the system does not require a very close match, fewer subjects will be rejected, meaning FRR will be low but FAR will be high. This type of setup is useful in surveillance applications. For the system requiring a close match it is the reverse, and is useful in top level security (i.e. forensic applications). However, at some point biometric security needs to compromise by making FAR and FRR equal. This is known as the Equal Error Rate (EER), which is the measurement of the performance of the biometric verification process. The performance evaluation graph is presented in Fig. 1.6 [37].

1.2 Challenges

With a few prominent successes and continuous challenges in mind, authenticity and the protection of confidential information are considered to be the vital issues for different government and law enforcement organizations–including military, civil aviation, Secret Service, border security, and financial institutions. The stakes are so much higher if classified information falls into the hands of unintended recipients. Current conventional authentication and data protection schemes are dependent on passwords or shared secret keys (something an individual knows) and identity cards (something an individual has), which can easily be forgotten or stolen. These algorithms can also be traced using guesswork, social engineering attacks, or a simple password cracking program. In addition, organizations such as law enforcement are often required to track or authenticate a noncooperative subject to verify that they are the same person who had entered a room or crowd. As a result, biometrics (something an individual is) is regarded as a conclusive solution in this area. Biometrics offers unique physiological and behavioral characteristics for authenticating an individual that are secure, efficient, and accurate. Importantly, these characteristics



(a) FAR and FRR



(b) ROC Curve

Figure 1.6: Performance Evaluation [37]

cannot be forgotten, handed over, or lost.

Most biometric systems are developed under the assumption that extracted biometrics and the nature of their associated noise is linear, stationary, and homogeneous. The performance of the biometric authentication deteriorates when the underlying assumptions are violated due to nonlinear, nonstationary, and heterogeneous noise. Secrets have always been hard to keep. Due to the proliferation of changing technologies, demands from public and private institutions to protect these secrets in digital form have risen higher than ever. A limited number of biometric traits also possess sensitive human information that is vulnerable to security, privacy, and unlinkability attacks. Furthermore, after biometric data acquisition, the method of biometric data manipulation and representation techniques is almost the same as any other traditional data management system. Therefore, concerns about the vulnerability of the extracted biometric template have become of paramount importance.

Biometric systems are increasingly used to recognize individuals and regulate access to physical spaces, information, services, and other rights or benefits, including the ability to cross international borders. The motivations for using biometrics are diverse and often overlap. They include improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security.

The efficacy and applicability of a biometric system can be affected by the cultural, social, and legal considerations that shape the way in which people engage and interact with these systems. One's deliberate choices how or whether to engage, as well as their unintended actions all affect system performance. For example, some people may choose not to place their fingers on a fingerprint scanner for fear of contracting a disease, or may be unable to do so. It is therefore incumbent upon those who conceive, design, and deploy biometric systems to consider the cultural, social, and legal contexts of these systems. Failure to attend to these considerations and social

impacts diminishes their efficacy and can bring forth serious unintended consequences. Ideally, authenticity and security of the templates are achieved based on mathematical algorithms that must be efficient, accurate, and acceptable, and difficult to decrypt by the unintended recipient. In addition, a template protection algorithm should be irreversible, robust, diverse, revokable, and secure. Therefore, a sophisticated biometric system needs to be developed to deal with these challenges.

1.3 Proposed Method

The proposed method addresses the predominant deficiency of the biometric system and systematically investigates a MultiBiometrics authentication and encryption system. In this method, a novel Sequential Subspace Estimator (SSE) for biometric authentication is presented in the image subspace that considers the effect of nonlinear, nonstationary, and heterogeneous noise on the extracted biometric features. As well, a new MultiBiometrics encryption algorithm is proposed that protects the biometric features against security, privacy, and unlinkability attacks. To further enhance the security protection and to improve authentication accuracy, a Biometric Data Management System (BDMS) is being developed, and the implementation of this method is also presented. In this case, biometric features from facial and fingerprint images found in the approved public databases have been used. Finally, the performance of the model is evaluated by the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Correct Recognition Rate (CRR); this is compared with the other state-of-the-art algorithms.

1.3.1 Objectives

The main objectives of this research are to:

- Propose a novel biometric authentication system that produces quality biometrics and reduces computational complexity, and execution time.

- Mitigate the effects of noise from nonlinear, nonstationary, and heterogeneous noise while extracting biometric features for template generation using a novel SSE algorithm. In the experiment, the received image is first analyzed in the image subspace to reduce noise levels and overcome the associated computational complexity. Afterwards, the biometric features are extracted and templates are created and stored in the database. This template is then compared with other encoded biometric templates to authenticate the legitimacy of an individual.

- Improve the current two-stage independent biometric encryption system, first to authenticate and then to release the secret key. This method includes a multilayered, MultiBiometrics secret key-bond algorithm for the cryptographic bond, so that the encryption system can protect the biometric features from security, privacy, and unlinkability attacks. A biometric data management system is also being developed using the cryptographic bond in conjunction with the hash function and the data segmentation technique. This system improves authentication accuracy and ensures better protection of the biometric features.

- Design and implement an integrated system based on the proposed MultiBiometrics authentication and encryption method in order to track and authenticate the legitimacy of a single individual under surveillance.

1.3.2 Contributions

Over the last decade, the demand for biometric systems has grown steadily in the field of information technology, leading to increased template vulnerability. The production of quality biometric features and associated computational complexity are

vital challenges for the exploitation of biometric systems. In most cases, biometrics deals with large volumes of datasets. Noise associated with these datasets is very likely to be present due to misalignment, illumination, position orientation, and facial expression effects. This dissertation discusses two important aspects of a biometric system: MultiBiometrics encryption and authentication; these ensure the high quality of biometric features and reduce the computational complexity.

The main contributions of this research are to:

- Develop a novel Sequential Subspace Estimator (SSE) algorithm in the image subspace that overcomes the challenges associated with computational complexity, reduce execution time, and mitigates the noise of the extracted biometric features.

- Develop a novel MultiBiometrics encryption algorithm to provide multilayered protection for biometric features against security, privacy, and unlinkability attacks.

- Integrate the SSE and MultiBiometrics encryption methods and implement the integrated method as a single biometric system.

1.3.3 Application Areas

The potential application areas of this integrated method are in the Lottery and Gaming Corporation's (or Casino) self exclusion program, airport security, and financial institutions (i.e. Biometric Banking). Here, continuous authentication, access control, and surveillance are necessary to ensure the security and legitimacy of a single individual in real time domain. The SSE method can be used as an authentication system, whereas the encryption method can be implemented to protect the stored and dynamic biometric features against security, privacy, and unlinkability attacks.

1.4 Organization

The organization of this dissertation is as follows:

Chapter−2: Chapter 2 includes prerequisites and a comprehensive literature review relating to the proposed authentication and MultiBiometrics encryption method.

Chapter−3: Chapter 3 presents the proposed Sequential Subspace Estimator (SSE) algorithm based on the underlying authentication challenges. The computational complexity, experimental results, and analysis are also presented in this chapter. The method is made independent of biometric traits; however, it is tested on facial and fingerprint biometric features.

Chapter−4: Chapter 4 introduces a MultiBiometrics encryption method that can protect biometric features against security, privacy, and unlinkability attacks. In this case, facial and fingerprint biometric features have again been used. The computational complexity, experimental results, and analysis are also presented in this chapter.

Chapter−5: Chapter 5 presents the proposed SSE and MultiBiometrics encryption method as an integrated system. Afterwards, this integrated method is implemented as a single system.

Chapter−6: Chapter 6 includes conclusions and the recommendation for this dissertation.

Chapter 2

Literature Review and Prerequisites

2.1 Introduction

The future of biometrics has continuously grown since the 9/11 attacks, as the world is facing more complex and diverse terrorist threats than ever before. As a consequence, in 2004, the Department of State (*DOS*) started adding biometric facial recognition features from more than 90 million photographs into their database to identify individuals that were previously denied entry into the United States. It is of paramount importance for government and private organizations–including Secret Service, military, and civil aviation–to establish an accountable, robust, efficient, and secure surveillance zone for their field of view (FOV). As well, there are always concerns about acceptability and adaptability with new technologies, especially when the vulnerability of the useful and sensitive biometric features to security, privacy, and unlinkability attacks increases with demand in the field of information technology. In fact, the performance, robustness, and vulnerability of the biometric system depends on the quality of the extracted features, its encryption method, its intra-class

similarity, and its extra-class variations. Despite the underlying challenges arising from these demands, advancements in biometric systems have lead to significant accomplishments in a number of areas, including public safety, national security, and border patrolling over the past few decades [3],[4]. The proposed MultiBiometrics authentication and encryption system is a novel state-of-the-art method in this regard. The main focus of this chapter is to present a comprehensive literature review related to the method introduced in this dissertation and discuss prerequisites, before getting into the detailed analysis, formulation, implementation, and execution of this method.

This chapter is organized as follows: Section 2.2 presents a detailed literature review; Section 2.3 presents the prerequisites of the proposed model; and discussions and conclusions are drawn in Section 2.4.

2.2 Literature Review

A comprehensive literature review is presented in this section for the two parts of the proposed method: authentication and encryption.

2.2.1 Authentication

Most authentication systems are based on linear, stationary, and homogeneous systems, though a few studies have addressed the challenges due to nonlinear, nonstationary, and heterogeneous noise. D. Zizhe et al. [35] developed a new algorithm in the nonlinear PCA domain termed the adaptive Strong Tracking Filter (STF). The authors showed that the model is a special case of Kalman Filter and Recursive Least Squared algorithms, and is immune to system model mismatch. The algorithm converges quickly and is robust at the cost of computational complexity. One study conducted by the National Science and Technology Council [36] proposed a Linear

Discriminant Analysis (LDA) method for facial authentication. The author used LDA to maximize the inter-class and minimize the intra-class variations, since PCA performance deteriorates if a full frontal face can't be presented. However, this model was designed for linear and homogeneous systems and faces challenges if there are an inadequate number of data samples in the received dataset. L. Chan et al. [38] proposed a linear facial biometric authentication (identification and verification) system using PCA in conjunction with LDA. In that approach, the authors used PCA for dimension reduction, while LDA was used to improve the discriminant ability of the PCA system in order to overcome the challenges associated with illumination and facial expression effects. The main problem with this model is that it is inadequate to deal with noise under consideration.

P. Selvi et al. [39] proposed an algorithm based on fingerprint and iris biometrics to overcome dictionary attacks, and used the image processing method to extract biometric characteristics. In this case, minutiae points and texture attributes are extracted from the fingerprint and iris biometric features, then are encrypted and stored in the server database. During the authentication process, a symmetric key is generated based on mutual authentication between the server side and the user; this key is used for further biometric transactions between them. In this model, the authors claimed that the system does not need any additional computational power if it is directly applied to the existing password and biometric-based system. This multimodal encryption system is simple, but the authors didn't mention the cryptographic process or the achievable FAR and FRR. G. Lakshmi [40] introduced another fingerprint identification and encryption system, and used a Wiener and a digital transformed filter to mitigate the noise. However, the authors addressed the issues based only on a linear and homogeneous system. C. Nandini et al. [41] proposed a biometric authentication based on vein patterns. The authors used the length of the vein and the angle of the bifurcation points as the key features. To enhance

the quality of the vein pattern, the authors used different filtering techniques including the Wiener and the Median filter. The experimental results were very promising; however, the algorithm is based on linear and homogeneous systems. H. Lu et al. [42], presented a new PCA algorithm in an uncorrelated multilinear PCA domain using unsupervised subspace learning of tensorial data. This system offered a methodology for maximizing the extraction of uncorrelated multilinear biometric characteristics, but it is an iterative process and inadequate to deal with a nonstationary and heterogeneous system. M. Law et al. [43] presented a nonlinear dimensionality reduction algorithm under the assumption that high dimensionality data are available in the mainfold. Hence, dimensionality reduction can be achieved by mapping with respect to certain properties associated with the mainfold. The authors used the sequential processing method, which outperformed the computationally demanding approach, batch processing. Unfortunately, it is very likely to contain misleading information if the system is dependent only on the information contained in the mainfold. J. Suo et al. [44] developed a gender transformation algorithm based on hierarchy fusion strategy. In that approach, the authors used a stochastic graphical model to transform the attributes of a high-resolution facial image into a new image as the opposite gender with the same age and race. The main objective is to modify the gender attributes while retaining facial identity. This is an interesting model; however the authors didn't consider the associated heterogeneity due to the different race and age groups. In addition, E. Carlos et al. [45] developed a new algorithm for covariance estimation for the Bayesian classifier. This method successfully addressed the challenges associated with the Bayesian Estimator due to limited numbers of sample data. However, this model was developed under the assumption that variation in the data class is the same; hence similarities in the covariance shape are highly expected in all classes. As a result, this method is inadequate to deal with a nonlinear and heterogeneous operating environment. L. Lin et al. [46] proposed a hierarchical regenerative

model using an "And-Or Graph" stochastic graph grammar methodology. In that model, the probabilistic bottom-up formulation was used for object detection, and the recursive top-down algorithm was used for the verification and searching process. Here, objects with larger intra-variance were broken into their constituent parts, and linking between the parts was modeled by the stochastic graph grammar technique. The authors also addressed the localization challenges due to the background clutter effect. The proposed verification process was developed in a homogeneous and controlled environment.

K. Nandakumar [47] introduced a Bayesian approach in his M.Sc thesis. In that study, the author considered that the authentication matching scores received from the different modalities were heterogeneous, but overcame this challenge by normalizing the outcome before the fusion process. Unfortunately, the author failed to consider the heterogeneous nature of the received observable data used for the authentication method. Another study concerning the Bayesian Estimator was conducted by M. Nounou et al. [48], addressing the problem associated with the MLE and PCA algorithms. Unfortunately, this method was also developed under the assumption that the system is stationary and homogeneous.

2.2.2 Biometric Cryptography

With the increase in number of constantly evolving electronic technologies, demands from public and private institutions for digital protection have risen higher than ever. Biometric technology is the viable solution for these demands. Typically, in biometric systems, a legitimate user needs to access the system to perform two modes of operations–identification and verification. In the identification process, the received biometrics need to be compared with all of the stored biometrics in the database. During the verification process, the received feature vectors (biometric template) only need to be compared with the biometric template of the claimed individual. Existing

studies on the biometric features protection algorithms can be categorized into: *i*) Biometric Encryption (*BE*), and *ii*) Features transformation based approach; both of which are discussed in the following subsections.

2.2.2.1 Biometric Encryption (BE)

Cryptography uses encryption to send and receive secret messages that can only be decrypted by the intended recipient. It uses algorithmic formulations to protect security and privacy, including confidentiality, integrity, and authenticity of the information. Biometric Encryption is a process that generates a digital secret key that monotonically bonds with the extracted biometric template to create a secret compound cryptographic data block. The secret key can also be derived from the biometric features. In both cases, candidate biometric features are stored in a database known as a helper data, and this key is used as the secret key for the overall biometric transaction [29],[34]. Typically, this data block is stored in a remote location, and neither the biometric features nor the secret key can be retrieved from this data block without a successful biometric authentication. A typical block diagram of a key bond and the retrieval process is shown in Fig. 2.1.

2.2.2.2 Features Transformation Based Approach

In the Features transformation based approach, an algorithm is implemented to create a transformed function, which is then applied to the extracted biometric template. In this case, only the generated transformed template is stored in the database for the biometric transaction. The original template cannot be retrieved if it is compromised, since matching is performed directly in the transformed domain. Fundamentally, parameters of the transformed function (or transformed domain) are derived from the random key or a user-specific password. During the authentication process, the same transformation function is applied to the query and matched to the stored templates

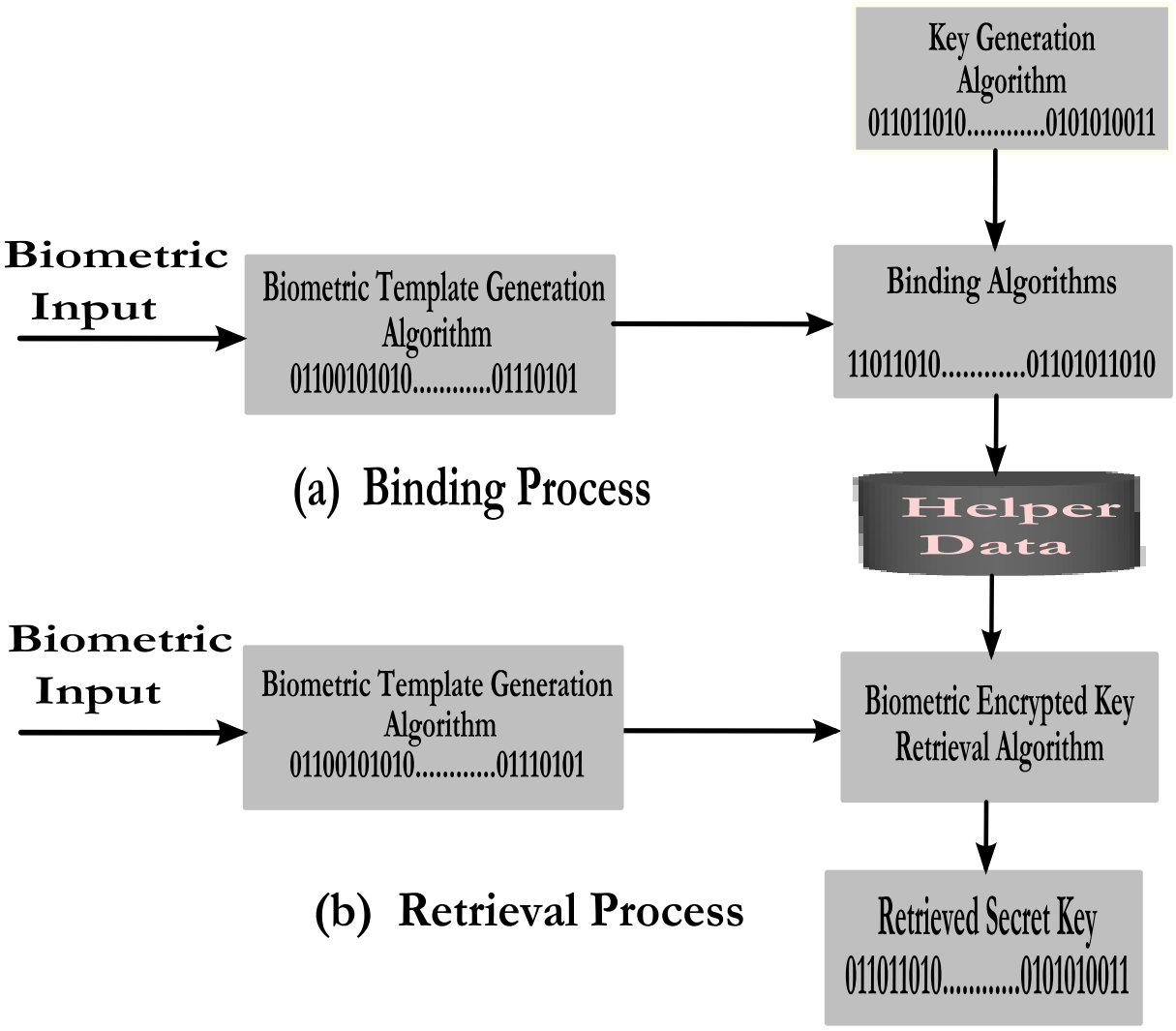


Figure 2.1: Biometric Encryption -Key Binding and Retrieval Process

in the transformed domain. This template is cancelable and revocable. Two of the most widely used features transformation based approaches are cancelable biometrics and biohashing. A typical block diagram of this approach is illustrated in Fig. 2.2.

Biometric Encryption Vs Features Transformation

The proposed study is based on the Biometric Encryption (BE) method. The primary reason this method was chosen was that it provides more privacy and security protection, since the original biometric features cannot be retrieved from the cryptographic bond. Even if the intruder is able to decode the secret key, the original biometric features cannot be retrieved. In contrast, the features transformation technique is based on the template transformation function; by decoding the transformation function, it is possible to decrypt the original biometric features. Since the proposed encryption method is based on Biometric Encryption, most of the discussions will be focused on this particular method.

In the BE method, a system-generated cryptographic key or a generated key from biometrics is securely bound to the biometric features and is stored as an encrypted biometric template. Neither the secret key nor the biometrics can be retrieved from the stored encrypted template [28],[29]. Some of these methods involve a two-stage independent process: authentication, and the release of the secret key. However, biometric features can be retrieved if the cryptographic key, or its location, is obtained by the imposter. Other key binding methods involve using the secret key along with biometric features to secure the biometrics.

In their self-exclusion model, A. Cavoukian et al. [28] proposed a biometric encryption algorithm based on facial biometrics. The system is composed of two distinct stages: i) creation of a watch list consisting of a maximum of five patrons (the top 5 matches), using the traditional 1:many biometric comparison technique based on facial biometric features; and ii) implementation of a biometric encryption module

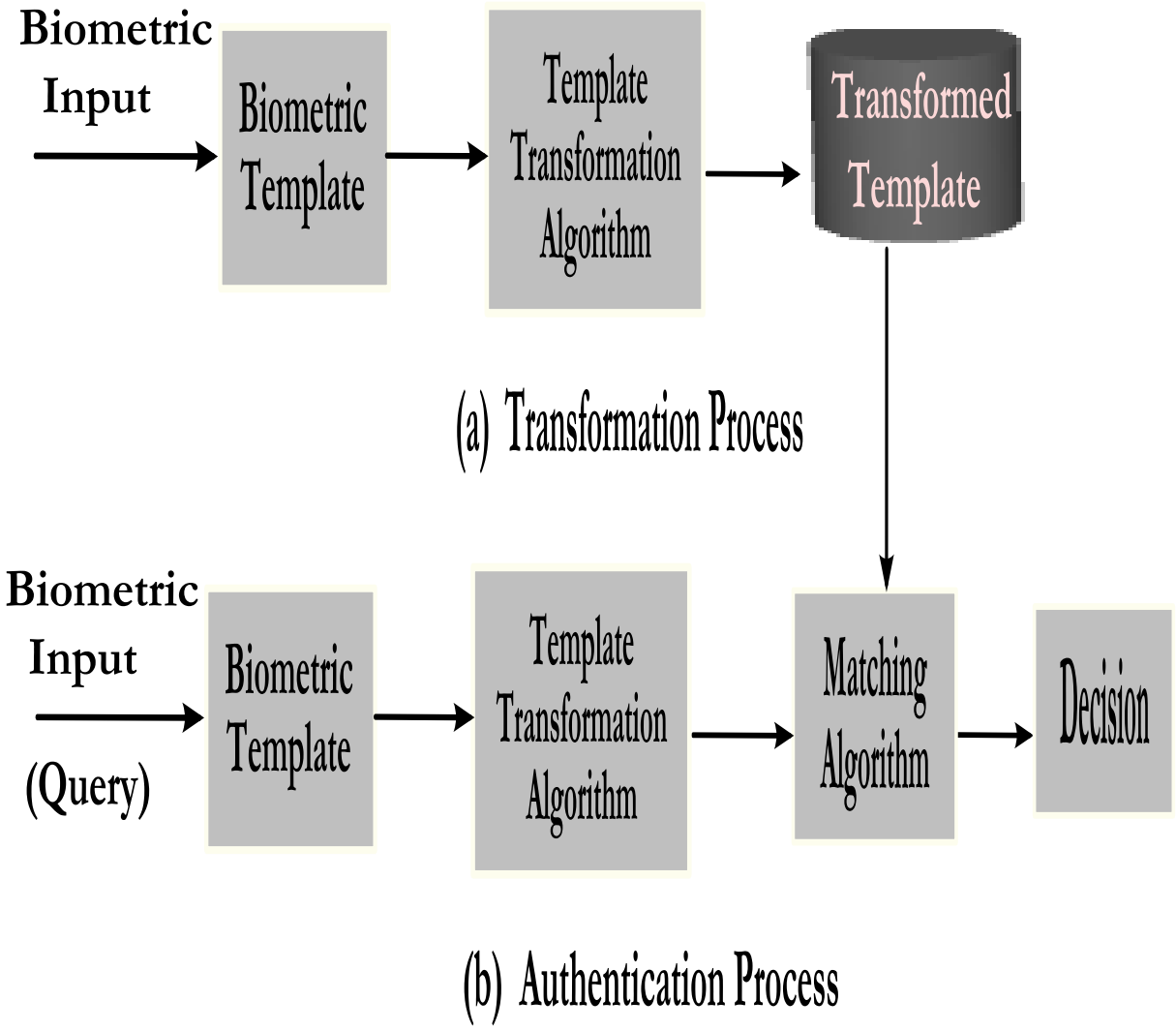


Figure 2.2: Features Transformation -Transformation and Authentication Process

and released keys for each of the top match patrons, and the generation of a match alert by the system that is then reviewed by administrators.

During the enrollment process, the subject's facial image is captured and a non-meaningful unique enrollment ID (id) is created. A commercial recognition process is used to extract the facial features and generate a template $t1$, which is indexed by the enrollee ID and stored into the face recognition database. Another biometric template $t2$ is passed through the biometric encryption (BE) key binding algorithm and helper data (or a private template) is created using a combination of biometric data and a random pointer key. The pointer key represents the location of the subject′s facial image as well as other personal information of the self-excluded individual within the database. Finally, the BE helper data is sorted by the same enrollee ID and stored in another location. For OLG's security reasons, $t1$ and $t2$ use different facial algorithms to extract features, which are not interoperable. The major shortfall of this method is that it is a combination of manual and automated processes, and the authors do not consider the challenges that could occur during the extraction of facial features from the moving subject due to illumination, position orientation, and other environmental interferences.

During the authentication process, a traditional $1 : many$ facial algorithm is used to create a watch list with the top five matching patrons, and the BE algorithm is used to retrieve enrolled IDs of the top match patrons. The final stage of verification is initiated if a key can be retrieved from the BE helper data associated with one of the potential matches. Here, the pointer that stored personal information associated with the potential match is regenerated, and recorded. An administrative operator then manually verifies the retrieved facial images with the live image of the Casino patron in question. The proposed BE method can achieve an optimal FAR with minimal increase in FRR. In their self-exclusion model, K. Martin et al. [48] proposed a biometric encryption algorithm based on a small subset of the subject's

facial biometrics database. The authors here used feature vectors in their key binding process to secure the cryptographic key. This is a novel model, and they achieved low FAR at the cost of FRR.

W. Zhang et al. [50] proposed a robust facial recognition method by synthesizing a facial sketch from a face photo under different pose and lighting conditions. Generally, synthesized approaches have been surpassed in performance by discriminative feature-based approaches. A key advantage of synthesis methods is that once a sketch has been converted to a photograph, matching can be performed using existing face recognition algorithms. The proposed method improved the performance of the authentication process; however, the authors here proposed to further investigate their method with expression variations. K. Nandakumar et al. [51] proposed a fuzzy vault scheme where the authors derived a multibiometrics template from multiple templates of a single user. They used fingerprint minutiae points and iriscodes templates and transformed them into a multibiometrics vault. Both the biometrics and the secret key were secured using the multibiometrics vault as a single entity. The overall security achieved using their proposed method was around 49 bits, as compared to 41 bits for a stored individual template using separate vaults. A. Jain et al. [52] presented a biometric data hiding approach to secure the transmitted as well as stored biometric data. A. Ross et al. [53] proposed a visual cryptography method to protect the privacy of the biometric templates. In their method, an image is decomposed into two host images and stored in the two central databases. The original image can only be revealed when two images are available simultaneously.

B. Klare et al. [54] proposed a heterogeneous facial recognition algorithm based on discriminative features. The author presented a framework termed Local Feature-based Discriminant Analysis (LFDA) in order to identify forensic sketches. This method provides substantial improvements in matching forensic sketches to the corresponding facial images. X. Wang et al. [55] proposed a random sampling method

using the multiple classifiers. The authors here developed an ensemble framework based on random sampling of feature space, training samples, and subspace parameters, and demonstrated the effectiveness of random sampling LDA for facial recognition. This subspace facial authentication method addressed the associated challenges of the small dimensional subspace dataset in comparison to the high dimensional features. In this case, multiple stabilized Fisherface and Null Space LDA (N-LDA) classifiers are constructed and then integrated using fusion, which preserves the discriminative information. Random sampling is also applied to the parameter selection in order to optimize the selection process. Afterwards, the random sampling framework is used for the integration of multiple features. This is a simple and straight forward approach. However, the authors suggested that more complex fusion (Kittler and Roli) algorithms can be used in order to enhance the authentication accuracy.

S. Bucak et al. [56] reviewed the Multiple Kernel Learning (MKL) method for solving optimization problems for object recognition. In their studies, the authors resolved the conflict associated with the MKL method regarding its efficiency and effectiveness in object recognition. The authors argued that the seemingly contradictory conclusions offered by the previous studied were due to different experimental setups. The author here showed that the MKL is an extremely useful tool for visual object recognition, since it provides a methodology for combining the strengths of different object representations. However, the classification accuracy of MKL is more critical to improve without sacrificing the computational efficiency. U. Park et al. [57] proposed a facial tracking and recognition system using static and Pan-Till-Zoom (PTZ) cameras to acquire high resolution images up to a distance of 12 meters. The authors here used a linear prediction model and a pan-tilt motion velocity control method for robust tracking. The outcome of their method showed that the proposed automated facial authentication system could track and authenticate a subject at a distance of up to 12 meters. However, the main limitation of this method is that the

camera needs to be adjusted manually and the system can recognize a face only when it is close to the frontal view.

N. Srinivas et al. [58] proposed a method to differentiate between identical twins based on facial marks. In this case, the authors used high resolution images. This multiscale automated face detection method to distinguish identical twins is solely based on the geometrical distribution of facial marks. The authors detected bright and dark regions with high radian symmetry at different scales, and used this to determine the prominence of facial marks. Facial marks are defined as visible changes in the skin, which differ in texture, shape, and color from the surrounding skin area. The authors suggested that these facial marks could be enhanced to make them more distinguishable, using texture, shape, and color. A. Paulino et al. [59] proposed a new robust fingerprint matching algorithm especially designed for matching latent fingerprints. The authors used a descriptor-based Hough transformation algorithm for aligning fingerprints and measured similarities between them by considering both minutiae and orientation field. Their method is useful for law enforcement and commercial applications, since the orientation field is constructed from minutiae points, which in their method are dependent on the manually marked algorithm.

B. Klare et al [60] proposed Heterogeneous Face Recognition (HFR) in random subspaces. In this study, the authors considered heterogeneity that involved matching two facial images from alternate imaging modalities, such as an infrared image to a photograph or a sketch to a photograph. In this method, both test and training images were represented in terms of nonlinear similarities to a collection of prototype face images. The nonlinear kernel similarity between an image and the prototypes is measured in the corresponding modality. To further enhance recognition accuracy, the random subspace framework is employed in conjunction with LDA subspace analysis. The author tested the method in different heterogeneous environments, however more tests need to be performed to further enhance the recognition accuracy. F. Hao et

al. [61] proposed a handwriting signature-based system where velocity, pressure, altitude, and azimuth are extracted and converted into binary bits. This system has achieved a 1.2% FAR and 28% FRR. A. Teoh et al. [62] proposed a multispace random projection method. The distance-preserving property of multispace random projection is analyzed based on a normalized inner product, and an approximately zero equal error rate (EER) is achieved; however privacy and changeability are the main concerns in this paper. C. Lee et al. [63], introduced a two factor method for generating cancelable fingerprint templates using local minutia information. The transformation function is associated with the randomly generated PIN number, which is used to change the biometric template. The major drawback to this method is that there is a tradeoff between performance and changeability. O. Song et al. [64] tested the Reed-Solomon method on the three different fingerprint databases and found that on average an FRR of below 1% is achievable.

Y. Wang [65] introduced a random projection algorithm for the template transformation method based on facial biometric features. The author implemented a vector translation technique to achieve a strong changeability. To enhance security and privacy as well as to improve recognition accuracy, only the index numbers of the sorted biometric template are stored as vectors. The index framework is then evaluated to produce a reissuable and secure biometric template. This method provides better protection of user privacy, and template revocability if it is compromised, at the cost of EER. The author also mentions that this methodology should be integrated with the biometric encryption system in future work in order to achieve the optimal level for biometric template protection. M. Savvides et al. [66] proposed a template transformation algorithm in the encryption domain. During the authentication phase, a query facial feature is convolved with a random kernel. This same kernel is used during the enrollment process to convolve with the training images, and is then correlated with the stored template in order to check the similarity. The stored template

is revocable and a new random kernel may be applied if it is compromised. However, the author doesn't clearly mention how the system would protect its privacy if the random kernel is compromised, since the original biometric may be retrievable if this occurs. D. Maio et al. [67], implemented a multihashing algorithm, where scores of selected fingerprint matchers and those obtained by a face authenticator are combined. Score level fusion is performed for each new biometric feature and a linear support vector machine is used for the final classification. Furthermore, to enhance the performance of this system, a random subspace based method is further combined with the similarity matching scores. A. Goh et al. [68], proposed a biohashing technique where the eigenprojection method is implemented to extract facial features. Each feature is hashed with a pseudorandom number in order to extract a single bit. A bit string is created and is further reduced to a single cryptographic key using $Shamir's$ secret sharing. The achievable entropy using this method is $80-$bit with 0.93% FRR.

2.3 Prerequisites

The method introduced in this dissertation is developed under the assumption that the noise environment is nonlinear, nonstationary, and heterogeneous. As well, the extracted biometrics features (stored and dynamic) are vulnerable to security, privacy, and unlinkability attacks. This section introduces some fundamental concepts as prerequisites before getting into a detailed analysis of the proposed method.

2.3.1 Resampling

A digital image is a collection of evenly spaced pixels on a rectangular grid in the image space. Different mathematical operations can be performed on these images. One of the most important operations is resampling of the image, which is a mathematical

formulation used to create a new version of the image [69]. The two most commonly used methods in this regard are up-sampling and down-sampling.

Increasing the size of an image by a factor of an integer or a rational fraction greater than unity is called up-sampling. In the case of up-sampling, the number of pixels increases with the size of the image. An up-sampled image usually contains all of the original information, but the image is smoother. On the other hand, reducing the size of an image by a factor of an integer or a rational fraction greater than unity is called down-sampling. In the case of down-sampling, the number of pixels decreases with the size of the image. A down-sampled image usually contains less information than the original image, however the image becomes sharper [69].

2.3.2 Statistical Properties

Statistical properties of the information processing system deal with the mean, covariance, probability, probability density function, autocorrelation, and cross correlation functions. These properties are the backbone of information technology. Parameter estimation, biometrics, and filtering hypothesis are performed based on these properties. But the fundamental limit on performance, based on this hypothesis, deviates from the optimal level due to the insufficient independent and identically distributed (i.i.d) sample data set, errors in receiver elements, and the diverse nature of the noise [70-72]. As a result, adaptive signal processing is now the subject of extensive research due to its capability of reducing the effects from the diversification of the underlining assumptions, in order to work and adapt with the more real world environment. Therefore, it is very important to have a core concept of the information technology from a statistical perspective.

The following subsections state some fundamental statistical properties based on previous work in biometric and estimation theory.

Mean

Now, assume that $\mu_{\mathbf{X}}$ is the mean (also known as expected value) of a random process $\mathbf{X}$. If $\mathbf{x}$ is a vector that contains L samples of the random process $\mathbf{X}$, then it can be written that:

$$\mathbf{x} = [x_1 \quad x_2 \dots x_L]^T \tag{2.1}$$

and the expected value or the mean:

$$\mu_{\mathbf{x}} = \mathbb{E}[\mathbf{x}] = [E[x_1] \quad E[x_2] \dots E[x_L]]^T. \tag{2.2}$$

Now consider another random process Y, where y is vector of length L of that process with mean $\mu_{\mathbf{y}}$; then the mean of the two random variables is the sum of their means and can be stated as:

$$\mu_{\mathbf{x+y}} = \mu_{\mathbf{x}} + \mu_{\mathbf{y}}. \tag{2.3}$$

Covariance

The covariance can be stated as a measure of how two non-identical variables change together. If the two variables are identical, then this property is called the variance. The covariance matrix can be defined as:

$$\begin{aligned} \mathbf{Q_{xy}} &= \mathbb{E}[(\mathbf{x} - \mu_x)(\mathbf{y} - \mu_y)^H] \\ &= \mathbb{E}[\mathbf{x}\mathbf{y}^H - \mu_x\mathbf{y}^H - \mathbf{x}\mu_y + \mu_x\mu_y^H]. \end{aligned} \tag{2.4}$$

In the case of a zero mean, covariance can be stated as:

$$\mathbf{Q_{xy}} = \mathbf{R_{xy}}. \tag{2.5}$$

Using these relationships, variance:

$$\mathbf{Q_{xx}} = \mathbf{R_{xx}} \tag{2.6}$$

where $(.)^H$, R_{xx}, *and* R_{xy} are the Hermitian transpose, autocorrelation, and cross-correlation respectively, and have been defined in the next section.

The standard deviation can be stated as a measure of the variability or dispersion of a data set. It is represented as the square root of the variance (or covariance). Therefore the standard deviation is:

$$\sigma_{\mathbf{x}} = \sqrt{Q_{\mathbf{xx}}}. \tag{2.7}$$

Cross Correlation

Let us consider two stochastic processes X and Y. The correlation between two stochastic processes is called the cross correlation, and can be stated as:

$$R_{\mathbf{xy}} = \mathbb{E}[\mathbf{x}\mathbf{y}^H]. \tag{2.8}$$

The autocorrelation of a stochastic process describes the correlation between the process at different points in time. Thus it can be stated as:

$$R_{\mathbf{xx}} = \mathbb{E}[\mathbf{x}\mathbf{x}^H]. \tag{2.9}$$

Therefore, according to equations $[2.5 - 2.9]$, it can be concluded that at a mean of zero, the variance and covariance are equal to autocorrelation and cross correlation respectively.

Posterior Probability Density Function

Probability theory is concerned with analysis of random phenomena. It is a measure of how likely it is that some event will occur. Typically, probability can be denoted by $P[.]$. Conditional probability on the other hand is defined as the knowledge of an event or occurrence of X, given the occurrence of Y. So, conditional probability can be stated as [48],[71],[73]:

$$P[X|Y] = \frac{P[XY]}{P[Y]} \tag{2.10}$$

where $P[Y] > 0$.

Now, consider the sample vectors $\mathbf{x}$ and $\mathbf{y}$ of the stochastic processes X and Y respectively. The posterior probability density function (pdf) of $\mathbf{x}$ conditioned on $\mathbf{y}$ is:

$$p[\mathbf{x}|\mathbf{y}] = \frac{p[\mathbf{y}|\mathbf{x}]p[\mathbf{x}]}{p[\mathbf{y}]}. \tag{2.11}$$

This is also known as Bayes' theorem.

If the random vector $\mathbf{x}$ follows a multivariate gaussian pdf $p_{\mathbf{x}}(\mathbf{x})$, then it can be written:

$$p_{\mathbf{x}}(\mathbf{x}) = \frac{1}{(2\pi)^{\frac{L}{2}}|Q_{xx}|^{\frac{1}{2}}} e^{-\frac{1}{2}(\mathbf{x}-\mu_x)^H Q_x^{-1}(\mathbf{x}-\mu_x)} \tag{2.12}$$

where $|Q_x|$ is the matrix determinant.

Ergodic Process

A stochastic process is termed to be ergodic if its statistical properties can be deduced from a single, sufficiently long sample of the process. In other words, it is the process when the time average of the samples approaches the ensemble average. For example, in signal processing the process can be considered ergodic if the mean of the snapshot

of the process is equal to the true mean of that process for all of the snapshots when $-\infty < t < \infty$.

Independence, Correlation, and Disjoint

The random events $\mathbf{x}$ and $\mathbf{y}$ are said to be independent if and only if their joint pdf can be written as:

$$p_{xy}(\mathbf{x}, \mathbf{y}) = p_x(\mathbf{x})p_y(\mathbf{y}) \tag{2.13}$$

If x and y have non-zero probabilities, then this implies:

$$p_{xy}(\mathbf{x}|\mathbf{y}) = p_x(\mathbf{x}) \tag{2.14}$$

and

$$p_{yx}(\mathbf{y}|\mathbf{x}) = p_y(\mathbf{y}). \tag{2.15}$$

In the case of disjoint events, it may be considered that:

$$p_{xy}(\mathbf{x} \cap \mathbf{y}) = 0. \tag{2.16}$$

In probability, disjoint and independence do not mean the same thing. However, when either $p_x(\mathbf{x})$ or $p_y(\mathbf{y})$ is zero, then disjoint and independence are the same. Finally, random variables $\mathbf{x}$ and $\mathbf{y}$ are said to be uncorrelated if they satisfy the following relation:

$$\mathbb{E}[\mathbf{xy}]^H = \mathbb{E}[\mathbf{x}]\mathbb{E}[\mathbf{y}]^H. \tag{2.17}$$

2.3.3 ML and MAP

Maximum Likelihood Estimator (MLE) is a sample-based method of estimating non-random parameters, maximizing the known likelihood distribution based on a given

statistic [48],[71],[74]. It requires a distributional assumption for the purpose of summarizing observations.

Using Bayes' law, posterior density function can be stated as:

$$p(\mathbf{w}|\mathbf{x}) = \frac{p(\mathbf{x}|\mathbf{w}).p(\mathbf{w})}{p(\mathbf{x})}$$
$$\text{posterior} = \frac{\text{likelihood.prior}}{\text{evidence}}$$
Using the property of probability function:
$$p(\mathbf{x}|\mathbf{w}) = \frac{p(\mathbf{w}|\mathbf{x}).p(\mathbf{x})}{p(\mathbf{w})}$$
$$\text{likelihood} = \frac{\text{posterior. evidence}}{\text{prior}} \tag{2.18}$$

where evidence $\mathbf{x}$ consists of independent observations $\{\mathbf{x}_1, \mathbf{x}_2, ...\}$. In MLE, the value of $\mathbf{w}$ (prior) is considered to be fixed, which maximizes the likelihood of Eq. (2.18). Therefore, a prior $\mathbf{w}$ needs to be considered that will give the largest possible value of $p(\mathbf{x}|\mathbf{w})$. Hence,

$$\hat{\mathbf{w}}^{ML} = \underset{\mathbf{w}}{\text{Max}}\ p(\mathbf{x}|\mathbf{w})$$
ML solution can be obtained:
$$\frac{dp(\mathbf{x}|\mathbf{w})}{d\mathbf{w}} = 0. \tag{2.19}$$

On the other hand, Maximum a Posterior (MAP) is the corresponding estimate of the random parameter that maximizes the posterior probability density function. Therefore, MAP is represented by:

$$\hat{\mathbf{w}}^{MAP} = \underset{\mathbf{w}}{\text{Max}}\ |p(\mathbf{x}|\mathbf{w})p(\mathbf{w})|. \tag{2.20}$$

2.3.4 Databases

In this dissertation, facial images from two public databases, the "Put Face Database" and the "Indian Face Database", are used [75],[76]. The sizes of the two databases are presented in Table 2.1. The "Put Face Database" is a highly nonlinear and heterogeneous 3D facial database. It contains approximately 20 images per person with a total of 200 people, and stores 2048×1536 pixel images [77]. The main motivation for using the "Put Face Database" is that the diversity of the image subsets allows them to be easily used for training, testing, and cross-validation processes. This can occur because the images in this database have more than 20 orientations for each individual using various lightings, backgrounds, and facial expressions. In addition, the images in this database contain 2193 landmarked images [78].

On the other hand, images in the "Indian Face Database" are less influenced by the facial expression, position orientation, and illumination effects. There are 40 subjects, each having 11 images with the same homogeneous background. The size of each image is $640\times$ 480 and 256 gray level per pixel. The main reason for using two types of databases is to find out the combined effects of two different environments. As well, it is important to show that the proposed method is the optimal solution for not only the images highly influenced by the underlying challenges, but also for the images that are less obstructed by them.

Furthermore, fingerprint images from the public database "CASIA-Fingerprint Version 5.0" have also been used in the proposed method. In this case, 40 fingerprint images of eight fingers were used, each finger with 5 images. All fingerprints are 8-bit gray-level with 328×356.

2.3.5 Nonlinear, Nonstationary, and Heterogeneous Noise

Typically, the presence of any unwanted objects in observations or measurements can be considered noise. Biometrics deals with large volumes of datasets that are

Table 2.1: Two Databases

Databases	Original Image Size (Pixels)	Modified
Put Face	2048x1536 (gray)	256x256 (gray)
Indian Face	640x480 (gray)	256x256 (gray)

obstructed by various noise. The illuminations, position orientations, misalignments, facial expression, noncooperativeness, and induced modalities (multimodal) introduce noise to these datasets in the time domain (change over time). In this dissertation, the noise under consideration is not referring to the classical definition of noise (i.e. Gaussian, Poisson) used in communication and signal processing. Rather it refers to image and feature artifacts caused by these effects. In most cases, the associated noise in the datasets is considered to be linear, stationary, and homogeneous. But, there is very likely to be nonlinear, nonstationary, and heterogeneous noise instead due to misalignment, illumination, position orientation, and facial expression effects. The principal challenge in biometrics is to mitigate the effects of these interferences while extracting quality features from these datasets. This section addresses the biometric system in this regard and systematically investigates the noise associated with the proposed MultiBiometrics authentication and encryption method.

2.3.5.1 Nonlinear

Biometric features are often corrupted by nonlinear noise during feature extraction and processing. This nonlinearity is caused by combining the features with different modalities, deformable templates, noncooperativeness, inter-class similarities, intra-class variations, environmental noise, and randomness of data acquisition systems [79],[80]. These dynamics are one of the most challenging obstructions in the field

of biometric authentication processes. In the context of the proposed method, nonlinearity consideration comes from the use of the several biometric modalities (i.e. multimodality), randomness of data acquisition systems (multi-source, multimodal), and associated variability of the biometrics over time. Nonlinearity adversely effects the noise covariance matrix and hence the reliability and accuracy of the proposed MultiBiometrics method. Furthermore, this noise implies that the output is the nonlinear function of input. Thus, it deteriorates the prediction and estimation process based on the inputted dataset, and hence the performance of the systems.

2.3.5.2 Nonstationary

Nonstationary refers to a process where the statistical properties of a system change over time, which is usually indicative of a dynamic system. In this dissertation, facial images from two public databases have been used [75],[76]. These images have been taken with different orientations and facial expressions. It is a challenge to extract quality biometric features since features availability and accessibility are interrupted due to these effects. In the context of the proposed method, variations of position orientations and facial expressions are being considered in the time domain. This nonstationary image property affects the intra-class similarities and inter-class variations of the extracted features, resulting in variability in mean and covariance estimations over time [81]. This time variant process deteriorates the feature quality and hence the performance of the authentication process. Therefore, consideration of the effects of these interferences on the extracted features due to nonstationary noise is of paramount importance to the proposed method. The variabilities of facial image orientations and expressions (snapshots taken at different times) from time t_1 to t_6 are shown in Fig. 2.3.

These captured images over the time period of time t_1 to t_6 are being compared with the stored images in the database system in order to verify the authenticity of

(a) Changing Position Orientations

(b) Changing Facial Expressions and Position

Figure 2.3: Images in Time Variant Domain -Put Face Database

the subject of interest.

2.3.5.3 Heterogeneous

Heterogeneity refers to the non-uniformity or diversification of a system, where the constituents are of a diverse nature [71-73]. In particular, a heterogeneous entity is the integration of the diverse nature of the dataset, and the data integration process is used to provide uniformity in the heterogeneous dataset. In biometrics, heterogeneous authenticity involves comparison of images from different modalities (i.e. multimodalities). In this case, the stored (or training) and test images are populated with images from different sources [60]. The biometric modalities, previously discussed in Section 1.1.3, refer to the integration of biometric traits (multimodality) collected from images with different backgrounds, samples, sensors, and features. Heterogeneous systems play a vital role in biometric applications, including forensics and surveillance. Interferences in the dataset are largely unavoidable, since in many circumstances only a limited number of images from a particular modality (i.e. due to illumination effects or image collection from different sources) are available for query. In the context of the proposed method, images have been taken from different backgrounds and sources. Multimodal (i.e. MultiBiometrics) biometrics has been used where features from the two different modalities, facial and fingerprint, have been collected and fused. Therefore, heterogeneity is an intrinsic property of extracted features that could largely influence the performance of the proposed MultiBiometrics authentication and encryption method. A sample of heterogeneous images from the public "Put Face Database" is given in Fig. 2.4.

The information theory of biometrics states that the data structure of the extracted features is inherently dynamic in nature, resulting in a higher probability of nonlinearity and heterogeneity in the biometric features. During most of the authentication, the requirements of an independent and identically distributed (i.i.d) sample

(a) Facial Images -Put Face

(b) Fingerprint Images -CASIA v5.0

Figure 2.4: Heterogeneous Images -Multimodal and Milt-Background

dataset increase with the dimension of the covariance matrix. However, in a nonlinear, nonstationary, and heterogeneous operating environment, it would be a challenge for biometric systems to obtain a sufficient number of i.i.d data in the sample dataset. Biometrics are measurable human physiological and behavioral attributes that satisfy the properties stated in Section 1.1.4. These properties change over time and are highly susceptible to the nonlinear and heterogeneous noise associated with biometric features due to effects from illuminations, facial expressions, object orientations, and misalignments. This demonstrates that the nonlinear, nonstationary, and heterogeneous assumptions are extremely important in real world scenarios, especially in the method proposed in this dissertation.

2.3.6 Noncooperative Target

This method (Chapter 5) is designed under the assumption that the moving target in the surveillance zone is noncooperative. It also assumes that the received biometric features from a noncooperative (introduced nonlinearity) moving target contain noise due to background noise, illumination, change in target orientation, misalignment with associated features, and the unawareness or unwillingness of the target. On the other hand, it has also been considered that the cooperative target would have noise due to background noise, illumination, change in orientation, and misalignment effects as well. Thus, this model may also be implementable for cooperative targets. The relation between cooperative and noncooperative considerations can be stated as follows:

$$\begin{aligned} Z_{co} &= s + n \\ Z_{nco} &= s + n + \alpha \\ &= Z_{co} + \alpha \end{aligned} \tag{2.21}$$

where Z_{co} and Z_{nco} are biometric features extracted from cooperative and noncooperative targets respectively, n is the underlying noise associated with the cooperative target, and α is the additional noise due to unawareness or the unwilling nature of the noncooperative target.

2.3.7 Privacy, Security, and Unlinkability

Biometrics deals with sensitive physiological information that is extremely private for an individual. This information is unique and cannot be revoked or reissued once compromised. Security measures to protect an individual's privacy are an extremely important component of biometric systems. The MultiBiometrics encryption method proposed in this dissertation has the objective of providing multilayered protection

for these biometric templates from security, privacy, and unlinkability attacks. The fundamental concepts of this protection in the context of biometrics are presented in this section.

2.3.7.1 Privacy

The term privacy has many meanings in different contexts. The most general is freedom from interference and intrusion. It implies that the collected information cannot be intercepted (i.e disclosed) without valid consent. In the context of the biometric system, privacy settings allow all authorized personnel to update data and access updated data. The purpose of obtaining the collected data must also be reasonable (i.e. lawful) and it must not be used for any reason other than that for which it was collected [82],[83]. It is especially important that the sensitive human physiological information collected for biometrics must not be allowed to be released to or intercepted by unauthorized personnel. Unauthorized retrieval or access to that sensitive information, and identification of an individual using that information, not only intrudes on the privacy of that individual immediately, but also poses immediate threats to the biometric systems [83]. Therefore, protection of privacy along with a guarantee that one cannot be identified is the vital issue for biometric systems, hence the proposed method.

2.3.7.2 Security

Security implies the protection of an object from destruction and the unwanted actions of unauthorized users. As mentioned previously, biometrics offers greater security than any other traditional methods, since a biometric system contains attributes that exclusively represent an individual's identity. These properties are unchangeable, undeniable, and difficult to lose or fake. However, just like any other system, there are security issues inherent to biometrics. Not only are there standard security issues

such as insecure databases or data transmission media, but the presence of a biometric scanner invites other forms of data manipulation. Furthermore, if someone were to gain access to the biometric database systems, the intruder could potentially access a person's unique physiological and biographic information, which an individual needs to keep extremely private [84]. Therefore, the main concern for the exploration of biometric systems is the security protection of these unique features. This cannot be neglected otherwise it can revert the overall process in the opposite direction, since the damage to this system is irreversible and may cost more than the system it is used for.

2.3.7.3 Unlinkability

Unlinkability is the privacy property that holds when an imposter cannot establish the relationship between objects. It is crucial to protect privacy in an authentication system [85]. True anonymity requires unlinkability, which is the ability of the system to perform multiple operations anonymously. Unlinkability also implies the incapability of retrieving the information of one individual based on the information of another. It is the measurement of the strength of a system (or object) to be unlinkable, and is the core property for any authentication process, making it difficult for a third party recipient to be associated with the unauthorized information. More importantly, the emergence of information technology along with the widespread increase in technological abilities poses unprecedented threats to the privacy and security of legitimate users. There is a very high possibility that unauthorized users would be able to overcome the challenges associated with breaking the infrastructure of a traditional unlinkable system. As a result, attacks on the unlinkability of the system have become an important concern in recent years [86]. It has become an especially important phenomenon for biometric systems, because if the system becomes compromised it could lead to unprecedented privacy and security breaches of biometric

systems [see $Appendix - A$].

2.3.8 Data Analysis

Acquiring useful information from the abundance of information sources and protecting its own privacy and security are vital issues for biometric systems. Data analysis is the process of transforming and modeling the data in this regard. This technology would enable the system to explore, visualize, and evaluate very large databases at a high level of abstraction without having any specific hypothesis. Some of the important data analysis techniques are stated in the following subsections [82],[87],[88].

Data Mining

Data mining has attracted a great deal of attention in all areas of research, from business to science; biometrics being no exception. Typically, it is a stochastic data analysis technique that is used for knowledge discovery and evaluation. With advancements in computer technology, the data mining process is able to dig through, analyze, extract, and transform enormous raw data sets into a meaningful set of data. Technically, it allows the system to analyze data received from different perspectives and dimensions and find the correlations or patterns among them. Biometric data mining is the computer-extensive knowledge discovery technique of biometric features used to analyze and recognize underlying patterns. The overall goal of this data mining is to extract images or signals of interest from the background and the sources and transform them into a useful and understandable structure for further use. In general, data mining techniques use algorithmic formulations based on a decision tree, statistical tools, the nearest neighbor, neural networks, and the database system for completing this transformation cycle [87],[88].

Data Segmentation and Foreign Key

Data segmentation is known as data grouping, and is a branch of the data mining operation. It is the process of extracting and segmenting data in such a way that the system would be able to factorize data, reduce data volume, and classify data. It is also capable of storing data in different locations of the database system with the purpose of increasing overall system performance and security. However, prior to carrying out a data segmentation analysis, appropriate care should be taken to decide which key parameters could be used for the segmentation process. This is especially important, since the failure of biometric segmentation means that the system could not detect useful biometric features. Indexing is another technique that can be used in the data segmentation process to put segmented data in order. In addition, a foreign key is used in conjunction with the indexing process to create a link and establish a relationship amongst the segmented data within the database system [see $Appendix - B$].

2.3.9 Tensor

A tensor is the linear transformation or mapping of vector(s) to vector(s). It could be mono or multi dimensional array(s). The rank of the tensor is determined by the dimensionality required to represent the array. A matrix is an example of rank-2 and a vector is an example of a rank-1 tensor [89]. A linear transformation of vectors by rotational angle or projection is an example of a tensor, and the mathematical formulation responsible for this transformation is called tensor algebra. For example, if a linear transformation function $T(.)$ is employed on the vectors S and produces the output vectors A, then:

$$A = T(S) \tag{2.22}$$

where the linear transformation function $T(.)$ performed the tensor operation.

2.4 Discussions and Conclusions

This chapter presents a comprehensive literature review related to the proposed method as well as its prerequisites before examining the detailed analysis and formulation of the method. It is apparent from these studies that most biometric systems have been developed under the assumption that extracted biometrics and the nature of their associated interferences are linear, stationary, and homogeneous. Addtionally, it is found that the vulnerability of the extracted features to security, privacy, and unlinkability attacks is also a vital issue for biometric systems. The core arguments in favor of biometric authentication and cryptography revolve around the quality of extracted features, their uniqueness, and their robustness, to protect privacy and security. Therefore, a more sophisticated authentication and encryption method needs to be developed to deal with the underlying challenges. The proposed MultiBiometrics authentication and encryption method is being developed based on these underlying noise assumptions and vulnerabilities.

Chapter 3

Sequential Subspace Estimator

3.1 Introduction

A biometric system often encounters situations that involve manipulation of a very large number of datasets (features). Robustness and performance of the authentication method are largely dependent on the quality of information in these extracted features; their intra-class similarities and inter-class variations. However, it is very likely that the subset of these extracted data is highly correlated and contaminated by the nonlinear, nonstationary, and heterogeneous noise. Furthermore, in most cases, extracted biometric features and their associated noise is modeled as a linear, stationary, and homogeneous system. The performance of the system deteriorates when these underlying considerations are violated due to nonlinear, nonstationary, and heterogeneous noise. On the other hand, it also introduces computational complexity, redundancy, and deteriorates the overall authentication accuracy [2],[90]. As a result, the principal challenge in biometric authentication is to mitigate the effects of any noise while extracting the biometric features for template generation. Therefore, a vital issue of biometrics is to develop a sophisticated authentication method that would address the underlying challenges associated with the biometric system.

The most commonly used method for biometric authentication, especially for facial biometrics, is the Principal Component Analysis (PCA) [91-93]. Generally, it is a linear transformation under the supposition that an adequate number of independent and identically distributed (i.i.d) data is present in the received dataset. PCA is an optimal method under the assumption that the operating environment is linear, time-invariant, and homogeneous. But, in a realistic operating environment it is very likely that the data model is contaminated by nonlinear, nonstationary, and heterogeneous noise. This leads to a higher probability of the characteristics of the dataset deviating from the underlying assumptions. In this situation, the generated output from the PCA-based technique preserves misleading data that severely distort the data model. This distorted data model in turn affects the detection, recognition, and authentication accuracy. Thus, a more complex system needs to be designed so the system can adapt to challenges due to noise contamination [36].

There are other popular methods for biometric authentication. Maximum Likelihood Estimator (MLE) is a sample-based parameters estimation method which maximizes the known likelihood distribution based on a given statistic. However, it requires a distributional assumption for the purpose of summarizing the observations. As well, it is only optimal for homogeneous and time-invariant systems, and is highly biased with a small amount of error on the initial assumption. The Linear Discriminant Analysis (LDA) method is also used as a linear classifier that maximizes the inter-class variation and intra-class similarities [38]. In the case of the Bayesian Estimator (BE), the likelihood function is combined with the prior density function, which is also known as a posterior density function. Unlike MLE, in the Bayesian method the prior value is not fixed but allows for injection of (likely) prior values during the estimation process. The main challenge of the Bayesian Estimator is to express the prior in the form of a distribution. If the number of sample datasets for a

specific class is limited, the performance of the Bayesian Estimator deteriorates significantly [48]. Least Mean Square (LMS) is a direct gradient descent method. This is an iterative process, where the input data sample is considered to be stochastic. The basic idea of this method is to update the filter weight to find the gradient of the mean square error [74]. In contrast, the Recursive Least Squared (RLS) filter minimizes the linear least square error recursively where the input data sample is considered to be deterministic [35],[94]. Although RLS can be used to solve most of the adaptive filtering problems, it involves more complicated mathematical operations and thus is computationally inefficient [38]. Finally, Wiener is a linear and time-invariant filtering technique which minimizes the Mean Square Error (MSE) between the estimated and the desired dataset.

Typically, the LDA, MLE, Bayesian, LMS, and Wiener filters are optimal for linear and time-invariant systems. The integration of these methods with PCA is used as a solution for adapting to the nonlinear, nonstationary, and heterogeneous noise environment. Another promising solution is the sequential estimator, which has also the capability of adapting to the diverse nature of noise. It is a recursive process and works based on prediction, adaptation (update or adjustment), and estimation [91]. However, the sequential state estimator is computationally inefficient for a higher dimensional dataset since it needs to compute the covariance matrix and perform a matrix inversion operation.

This chapter addresses the predominant deficiency of the biometric system in this regard. It also systematically investigates a biometric authentication in a nonlinear, nonstationary, and heterogeneous noise environment. Importantly, this authentication method is made independent of the biometric traits. The performance of this approach is being tested on facial images from two public databases: the "Put Face Database" and the "Indian Face Database". In the experiment, the facial image is analyzed in the image subspace to mitigate its noise levels before it is encoded and the

biometric template is created. Afterwards, the facial biometric features such as facial area, and size and relative positions of eyes and lips are extracted, analyzed, and encoded to create the biometric template. This template is then stored to compare with the other encoded facial biometrics. The noise associated with this feature is considered to be nonlinear, nonstationary, and heterogeneous due to position orientation, facial expression, and illumination effects. It will be shown that the proposed SSE method outperformed its counterparts: PCA, PCA-Wiener, PCA-MLE, and the sequential estimator; both in linear and homogeneous systems, and nonlinear and heterogeneous systems.

In this chapter, a new recursive sequential estimator algorithm in the image subspace is developed. This method addresses the challenges associated with the extracted features due to nonlinear, nonstationary, and heterogeneous noise (i.e., noise covariance matrix). As well, a subspace method is implemented in the image subspace to overcome the underlying computational complexity and reduce the execution time significantly. The proposed subspace method transforms higher dimensional image space into a set of linearly independent image spaces (image subspace) so that the dimensionality of biometric features reduces from $N \times N$ to $M \times M$, where $M << N$. Using PCA analogy, this method distributes the principal biometric feature vectors to the image subspace. Moreover, in this recursive approach, the extracted data and the associated noise (i.e. noise covariance) update in every iteration using the biometric features (dataset) from the immediate previous state. The SSE approach is based on the minimization of noise and maximization of information contained in the received data, in MSE sense. Therefore, this method would be able to make a close approximation of the desired dataset, which would otherwise be contaminated by nonstationary and heterogeneous noise.

The remainder of the chapter is organized as follows: Section 3.2 introduces the problem formulation and briefly reviews PCA, MLE, Bayesian, and Wiener methods.

Section 3.3 presents the detail analysis and methodology for the proposed solution. Experimental results, analysis, and discussions are presented in Section 3.4. Finally, conclusions are drawn in the final section.

3.2 Problem Formulation and Filtering with Principal Component Analysis

Principal component analysis is a statistical method used to analyze extracted biometric features. It uses orthogonal transformation to convert a set of observations of correlated variables to a set of linearly uncorrelated variables [93]. The purpose of PCA is to reduce the dimensionality of the dataset while retaining as much information as possible. In PCA, each image can be represented as a weighted sum of a small collection of images that define an image basis or eigenimage. The main objective is to calculate the principal components such that they account for the largest possible variance in the extracted dataset. During this process, there is no limit on the value of the weight vector for having the largest possible variance in the dataset, therefore a constraint must be added to the weight vector $\mathbf{w}$ in order to introduce consistency in the estimation process. Furthermore, this methodology is developed under the assumptions that the operating environment is stationary and linear and there are an adequate number of linearly independent variables available in the extracted feature vectors. On the other hand, due to the nonlinear, nonstationary, and heterogeneous noise environment, extracted data always deviate from the underlying assumptions, resulting in poor authentication accuracy. In this section, problem formulation, the PCA architecture, the Wiener filter, the MLE, and the Bayesian Estimator (BE) are examined.

3.2.1 Principal Component Analysis (PCA)

The main operational principles and formulation of PCA are stated below [93]:
1. Receive dataset of size m (vectorized image $N \times 1$ and m << N) at time t, $\mathbf{x}' = \mathbf{x}'_1\ \mathbf{x}'_2\ \mathbf{x}'_3.....\mathbf{x}'_m$.
2. Estimate the zero mean, eigenvalues, and corresponding eigenvectors; and then construct feature vectors with the principal components of size n ($n < m$).

$$Cov_{\mathbf{x}} = \mathbf{x}\mathbf{x}^T$$
$$Cov_{\mathbf{x}}V = \Lambda V$$
$$\mathbf{w} = (\mathbf{w}_1\ \mathbf{w}_2\ \mathbf{w}_3.....\mathbf{w}_n). \tag{3.1}$$

Therefore, the new dataset with principal components:

$$\mathbf{z} = \mathbf{w}^T\mathbf{x} \tag{3.2}$$

where w is the n-dimensional weight or loading vectors, mapped to each row vector of $\mathbf{x}$; $\mathbf{z}$ is considered to be inherited data with the maximum possible variance from the $\mathbf{x}$ dataset; and each weight vector $\mathbf{w}$ is constrained to a unit vector.

Now, the estimation of initial weight vectors that maximize the variance of individual variables of $\mathbf{z}$ can be formulated as the following optimization problem:

$$\mathbf{w} = \underset{\|\mathbf{w}\|=1}{\text{Max}} \left\{ \frac{\mathbf{w}^T\mathbf{x}^T\mathbf{x}\mathbf{w}}{\mathbf{w}^T\mathbf{w}} \right\}. \tag{3.3}$$

Therefore, the PCA estimator can also be formulated as the following optimization problem:

$$\mathbf{z}_{PCA} = \text{Max}\{var(\mathbf{xw})\}$$
$$\text{subject to } \mathbf{w}^T\mathbf{w} = 1. \tag{3.4}$$

Moreover, if measured and estimated observations can be defined as $\mathbf{x}$ and $\hat{\mathbf{x}}$ respectively; then the PCA optimization problem can also be defined as:

$$\mathbf{z}_{PCA} = \text{Min}\{(\mathbf{x} - \hat{\mathbf{x}})^T(\mathbf{x} - \hat{\mathbf{x}})\}$$
$$\text{subject to } \mathbf{w}^T\mathbf{w} = 1. \tag{3.5}$$

The PCA algorithm is optimal under the assumption that there are an adequate number of independent and identically distributed data in the dataset. In this approach the system is considered to be time-invariant and there is no heterogeneity or non-linearity in the data sample. However, an environment where the characteristics of the data deviate from the underlying assumptions is inadequate and results in poor authentication accuracy. Thus a complex dynamic filtering system needs to be modeled that can deal with the nonlinear and heterogeneous noise while also maximizing the amount of useful features in the dataset.

Now, consider that the received biometric feature is the sum of the desired biometric features and the noise. Then the received data sample can be written as:

$$\mathbf{x} = \mathbf{s} + \mathbf{n}$$

Therefore using Eq. (3.2),

$$\mathbf{z} = \mathbf{w}^T\mathbf{s} + \mathbf{w}^T\mathbf{n} \tag{3.6}$$

where $\mathbf{n}$ is the noise, and $\mathbf{s}$ represents the noise-free data or the desired dataset. So, the main objective is to minimize the noise $\mathbf{n}$ while maximizing the useful information

content in the desired dataset.

3.2.2 PCA with Wiener Filter (PCA-Wiener)

The classical Wiener filter is a linear optimal discrete time filter. It is optimal under the assumption that the operating environment is linear and stationary [38]. A schematic presentation of the adaptive Wiener filter is shown in Fig. 3.1.

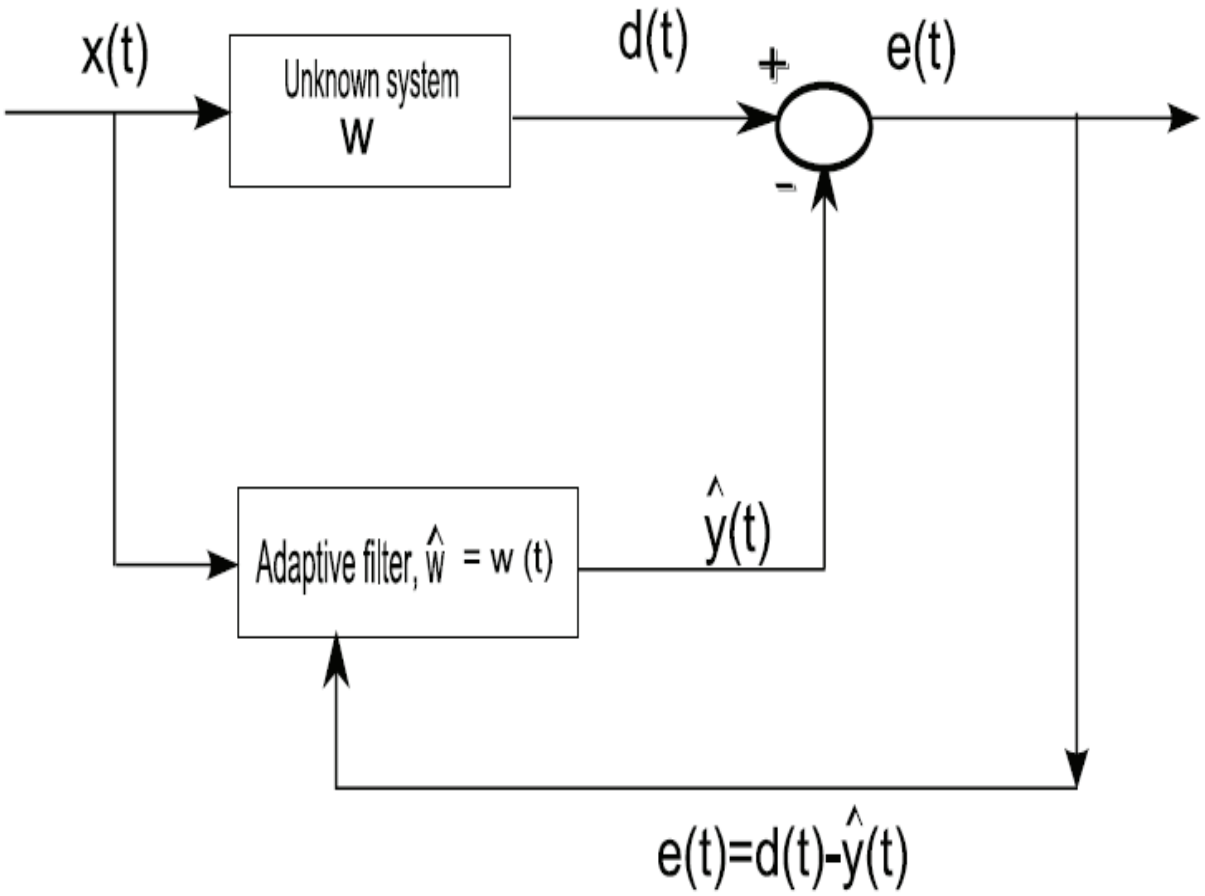


Figure 3.1: Adaptive Wiener Filter

In PCS-Wiener, PCA puts constraints on weight vectors so that the sum of their squared values equals one. Now, the output of the filter at time t can be written as

follows:

$$\mathbf{y}(t) = \mathbf{w}^T(t)\mathbf{x}(t) \tag{3.7}$$

where $\mathbf{x}$ represents observation dataset, $\mathbf{w} = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n)$ are the weight vectors and $(.)^T$ is the transpose operation.

But it is very likely there is noise in the observed data $\mathbf{x}$. If the system considers that the observed sample $\mathbf{x}$ contains desired sample data $\mathbf{s}$ and noise data $\mathbf{n}$, then by using Eq. (3.6) the above equation can be restated as:

$$\mathbf{y}(t) = \mathbf{w}^T(t)\mathbf{s}(t) + \mathbf{w}^T(t)\mathbf{n}(t). \tag{3.8}$$

If the operating environment is stationary, linear, and homogeneous, then the estimate $\hat{\mathbf{y}}(t)$ of the desired data $\mathbf{d}(t)$ at time t can be stated as:

$$\hat{\mathbf{y}}(t) = \hat{\mathbf{w}}^T(t)\mathbf{x}(t)$$

Due to a stationary system, it can be assumed:

$$\hat{\mathbf{w}}^T(t+1) = \hat{\mathbf{w}}^T(t). \tag{3.9}$$

The Mean Squared Error (MSE) is given by:

$$\begin{aligned} MSE &= \mathbb{E}[e^2(t)] = \mathbb{E}[(d(t) - \mathbf{w}^T(t)\mathbf{x}(t))^2] \\ &= \mathbb{E}[d^2(t) - \mathbf{w}^T(t)\mathbf{x}(t)d(t) - d(t)\mathbf{x}^T(t)\mathbf{w}(t) \\ &\quad + \mathbf{w}^T(t)\mathbf{x}(t)\mathbf{x}^T(t)\mathbf{w}(t)] \\ &= \mathbb{E}[d^2(t)] - 2\mathbf{w}^T(t)\mathbb{E}[d(t)\mathbf{x}(t)] \\ &\quad + \mathbf{w}^T(t)\mathbb{E}[\mathbf{x}(t)\mathbf{x}^T(t)]\mathbf{w}(t). \end{aligned} \tag{3.10}$$

The Wiener solution of the optimal weight vector can be found by taking the

second order derivation of Eq. (3.10) with respect to the weight vector $\mathbf{w}$, and equating it with zero. Therefore, the solution for the optimal weight vector $\mathbf{w}_{opt}$:

$$\frac{\partial^2(MSE)}{\partial \mathbf{w}^2} = 0. \tag{3.11}$$

The above equation is known as the Wiener Hopf equation.

The main advantage of the Wiener filter is its computational simplicity and ability to suppress noise in linear and stationary cases. Furthermore, the optimal solution of the Wiener filter involves only second order statistics, which in fact leads to a useful theory of linear filtering for many applications. The main goal of the Wiener is to filter out noise based on the statistical properties. Furthermore, the Wiener filter is an optimal filter under the assumption that the data model and additive noise are stationary and linear stochastic processes. As well, their behavioural characteristics, or auto and cross correlation, are also considered to be known. But, it is very likely to have a time varying nonlinear system with unknown data structure and noise properties; in this case, the Wiener filtering solution is inadequate to deal with this system and its associated noise. However, PCA-Wiener might be an alternative solution to overcome these challenges. It will be shown that the performance of the proposed SSE method is outstanding in comparison to PCA-Wiener.

3.2.3 PCA with Maximum Likelihood Estimator (PCA-MLE)

The objective of PCA with the Maximum Likelihood Estimator (MLE) is to maximize the likelihood of the principal components in the dataset without sacrificing useful information. Using the analogy of section 2.3.3, the PCA-ML estimator needs to maximize the probability density function in order to reduce the noise level. This can

be stated as follows.

$$\hat{\mathbf{w}}^{ML} = \underset{\mathbf{w}}{\text{Max}}\ p(\mathbf{x}|\mathbf{w})$$

ML solution can be obtained:

$$\frac{dp(\mathbf{x}|\mathbf{w})}{d\mathbf{w}} = 0. \tag{3.12}$$

But, noise is very likely to occur in the observed sample dataset, and hence in the distribution. Therefore, the PCA-ML optimization problem can also be formulated as:

$$\mathbf{w}_{PCAML} = \text{Min}\{(\mathbf{x} - \hat{\mathbf{x}})^T Q_x^{-1} (\mathbf{x} - \hat{\mathbf{x}})\}$$
$$\text{subject to } \mathbf{w}^T\mathbf{w} = 1 \tag{3.13}$$

where Q_x, $\mathbf{x}$ and $\hat{\mathbf{x}}$ are noise covariance, measured and estimated observations, respectively.

The MLE is optimal for the linear, homogeneous, and time-invariant system. On the other hand, the PCA-MLE addresses the challenges associated with the PCA estimator due to noise present in the received dataset. In this case, the prior is fixed and this estimator doesn't allow for injection of the prior knowledge during the estimation process. The PCA-MLE method might be a solution to deal with the nonlinear, nonstationary, and heterogeneous noise environment.

3.2.4 PCA with Bayesian Estimator (PCA-BE)

Unlike the Maximum Likelihood Estimator, in the Bayesian Estimator (BE) observable and non-observable quantities are random in nature. If $\mathbf{x}$ and $\mathbf{w}$ are the observations and the weight vectors respectively, then using Eq. (2.18), the posterior density

function can be stated as follows:

$$p(\mathbf{w}|\mathbf{x}) = \frac{p(\mathbf{x}|\mathbf{w}).p(\mathbf{w})}{p(\mathbf{x})}. \tag{3.14}$$

The probability density function $p(\mathbf{w})$ is considered to be a prior density function of unknown quantity $\mathbf{w}$. But, in contrast to MLE, the prior is a random quantity. Furthermore, the Bayesian Estimator can incorporate the external knowledge or prior beliefs in the likely values of $\mathbf{w}$ during the estimation process [45],[48]. Using the analogy and data reconciliation stated in sections 2.3.3, 3.1.1, and 3.1.3, the PCA-BE estimator can be formulated as the optimization problem:

$$\begin{aligned} \hat{\mathbf{w}}_{PCABE}^{MAP} &= \text{Max } |p(\mathbf{x}|\mathbf{w})p(\mathbf{w})| \\ &\text{subject to } \mathbf{w}^T\mathbf{w} = 1. \end{aligned} \tag{3.15}$$

One of the main complexities of the Bayesian Estimator is the probability of evidence, stated by the denominator $p(\mathbf{x})$ in Eq. (3.14). The main goal is to maximize (i.e. $p(\mathbf{x}) \approx 1$) the probability of evidence under the implied constraint. If it is possible to estimate the numerator with good approximation and a well defined prior, then it might be possible to replace the probability of evidence with a normalized constant value. It is found that for a large data sample and a well behaved prior, MLE and BE methods converge to the same point.

The PCA-Bayesian Estimator overcomes challenges associated with the PCA-MLE. The Bayesian method is an optimal estimator for a linear, stationary, and homogeneous environment. However, if the amount of sample data in the extracted biometric features is limited, the performance of the Bayesian Estimator deteriorates significantly. On the other hand, PCA-Bayesian is being used as an alternative solution to overcome the challenges associated with a nonstationary, nonlinear, and heterogeneous noise environment.

3.2.5 Extended Kalman Filter (EKF)

The Extended Kalman Filter (EKF) is an extended version of the Kalman Filter (KF), used for nonlinear, nonstationary, and heterogeneous systems. It is recursive and a branch of the sequential estimator process, so new measurements can be processed as they arrive. Now, assume that a dynamic system can be modeled by the state equation [95],[96]:

$$\begin{aligned} x(t+1) &= F(t)x(t) + v(t) \\ Q(t) &= \mathbb{E}[v(t)v(t)'] \end{aligned} \tag{3.16}$$

where x is the state at time t, F(t) is the state transition matrix, v(t)represents the processed noise, and Q(t) is the covariance of the processed noise.

If observations of the state are made using a set of measurements, then the measurement equation can be stated as follows:

$$\begin{aligned} z(t) &= H(t)x(t) + n(t) \\ R(t) &= \mathbb{E}[n(t)n(t)'] \end{aligned} \tag{3.17}$$

where z(t) is the measurement made at time t, H(t) is the measurement matrix, n(t) is the measurement noise, and R(t) represents the covariance of measurement noise.

Now, given a set of observations $z_1,\ z_2,\ .....z(t+1)$, if an estimate of the state x(t+1) is $\hat{x}(t+1)$, namely $\hat{x}(t+1)|z(t)$, then the expectation of the squared-error

function can be written as:

$$x_{er}(t+1) = \mathbb{E}[|x(t+1) - \hat{x}(t+1)|^2] \quad (3.18)$$

Estimate of predicted covariance:

$$P(t+1|t) = F(t)P(t|t)F^T(t) + Q(t)$$

Measurement Residual:

$$z_{er}(t+1) = z(t) - h(\hat{x}(t+1)|t)$$

Innovation:

$$S(t+1) = H(t)P(t+1|t)H^T(t) + R(t)$$

Gain for Extended Kalman Filter:

$$K(t+1) = P(t+1|t)H(t)^T S^{-1}(t)$$

State Update:

$$\hat{x}(t+1|t+1) = \hat{x}(t+1|t) + K(t+1)z_{er}(t+1) \quad (3.19)$$

The objective is to adjust $K(t+1)z_{er}(t+1)$ to minimize Eq. (3.18). The sequential estimator EKF is computationally inefficient for large values of datasets, since it needs to perform extensive matrix operations including matrix inversions.

3.3 Model Formulation and Sequential Subspace Estimator

The challenges posed by the Wiener, MLE, BE, and EKF can be overcome by the proposed Sequential Subspace Estimator (SSE). The SSE has the ability to deal with estimation challenges in a nonstationary, nonlinear, and heterogeneous operating environment and its associated computational complexity. It is a recursive method based on prediction, adaptation (update or adjustment), and estimation. In other words, the proposed SSE method is the extension of the Wiener, MLE, and Bayesian

approaches, where the operating environment (i.e. SSE) is nonstationary, nonlinear, and heterogeneous. The integration of PCA with these methods is widely used for this type of environment. The relationship between the SSE and the Wiener (or MLE, Bayesian, PCA) can be stated as follows:

$$\textbf{SSE} = \textbf{Wiener} + \textbf{nonlinear or nonstationary} \tag{3.20}$$

This is the core section of the proposed method. In this section a Sequential Subspace Estimator algorithm is being designed to address the underlying challenges and their associated computational complexities.

3.3.1 Subspace

The main objective of this method is to address the challenges associated with extracted biometric features due to nonlinear, nonstationary, and heterogeneous noise. Classical PCA, LDA, MLE, Bayesian, LMS, and Wiener methods are inadequate to overcome these challenges. The sequential estimator and the integration of PCA with Wiener and MLE are widely used when dealing with this type of environment. However, the sequential estimator is computationally inefficient for a higher dimensional dataset since it needs to compute the covariance matrix, perform the matrix inversion operation, and execute the data interpretation process [35],[95],[96]. As well, vectorization of the image would also be a huge computational burden, since a size $N \times N$ (8-bit) matrix becomes a vector of dimension N^2, and thus a size $N^2 \times N^2$ covariance matrix needs to be computed. These inadequacies led to a proposal of a new subspace technique. The SSE subspace method proposed here would overcome the challenges associated with noisy extracted data and the computational complexity. In this subspace method, an image of $L - bit$ is considered; here the image would be a $2^L \times 2^L$ matrix of $(L - bit)$ intensity values in the image space.

Considering that each value of a $2^L \times 2^L$ matrix is a uniquely characterized data point in the image subspace, the collection of these data points is the representation of an image. In this method, image has been segmented into L×2, L, and L/2 datasets in the image subspace by using Eq. (3.21). However, it is also possible to use other segmented datasets in the image subspace in order to achieve different performance and efficiency levels. Under these assumptions, the dimension of $2^L \times 2^L$ is reduced in the image subspace by a factor of L×2, L, and L/2. In the case of an 8-bit image, the dimension of $2^8 \times 2^8$ (L=8) is reduced by a factor of 16, 8, and 4 in the image subspace, respectively. In this study, the proposed SSE method using these three datasets is represented by SSE-16 × 16, SSE-32 × 32 (or SSE), and SSE-64 × 64, respectively.

The subspace method is the segmentation of an $N \times N$ dataset into an L (or L/2, or L×2) number of linearly independent datasets of dimension $M \times M$ (where M=N/L or M=N/(L/2), or M=N/(LX2)). Later in Section 3.4.3, a comparison between subspace datasets L/2 (i.e. SSE-64X64), L (i.e. SSE-32X32 or SSE), and L×2 (i.e. SSE-16X16) will be presented, and it will be shown that the proposed SSE method with L subspace datasets outperforms the subspace datasets L/2 and L×2. Therefore, in most cases, the model formulation, experimental analysis, comparisons, and discussions used in this study are based on the L number of segmented datasets in the image subspace. In this segmentation process, homogeneity and linearity are considered during the segmentation process, but data points within each of the L datasets are considered to be nonlinear, nonstationary, and heterogeneous. The relationship between the original and segmented datasets can be stated as follows:

$$N = \sum_{i=1}^{L} \mathbf{M}_i \tag{3.21}$$

where a sparse or segmented dimension $= (R + rM) \times (C + cM)$. Here, $M = ceil(N/L)$; $R = 1, 2, ..., M$; $C = 1, 2, ..., M$; $r = 0, 1, 2, ..., (L-1)$; and $c =$

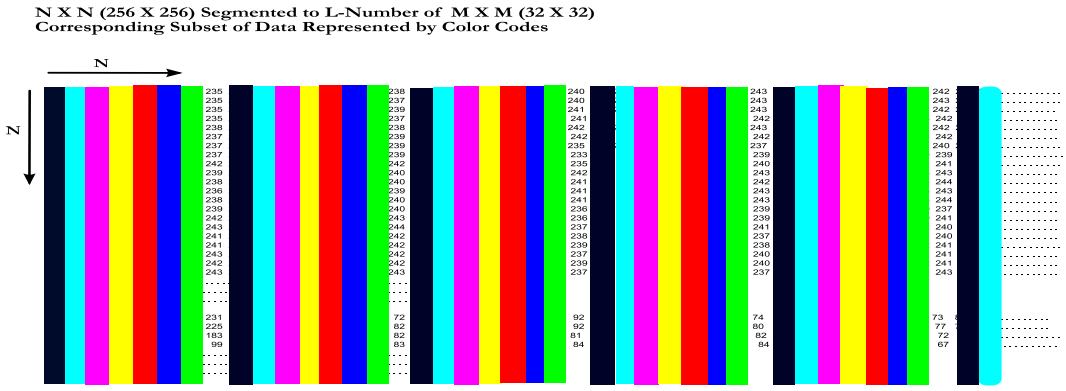
$0, 1, 2, ..., (L-1)$. r and c increase by 1 for every complete cycle of R and C, respectively, and the $'$ceil$'$ operation rounds up the value (N/L) to the nearest integer greater than or equal to (N/L). Hence, the estimation of the dataset reduces from $N \times N$ to L number of linearly independent datasets of dimension $M \times M$.

Consider an 8-bit 2D image, which has an $N \times N$ array of 8-bit intensity values. If the image is considered to be a vector of dimension N^2, then an image of size 8-bit (N=256) would need a vector of dimension $65,536$. In contrast, the proposed subspace approach would need a point in $M \times M$ (i.e. $32 \times 32 = 1024$) dimensional vector subspace. This is an iterative process which continues L (L=8) times using the same vector subspace. Therefore, using the subspace method, an ensemble of images and maps for a collection of points created in the image space leads to huge dimensional (and computational) savings. The SSE algorithm is being designed to implement the segmented datasets in the image subspace. This method estimates the principal feature vectors of the datasets and distributes them in the image subspace in order to mitigate the underlying noise level. Afterwards, the segmented (and filtered) image datasets concatenate in order to reconstruct the desired image. The subspace transformation process is shown in Fig. 3.2, where the corresponding subset of data (column vectors) is represented by color codes.

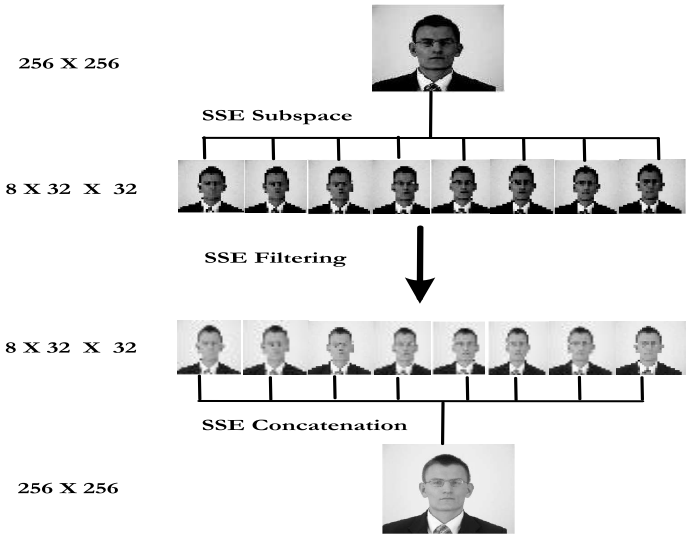
3.3.2 Model Formulation

The main objective of this section is to design a filter that given an estimate $\hat{\mathbf{y}}(t)$ at time t of the desired biometric feature vectors $\mathbf{d}(t)$, using the observed data sample $\mathbf{x}(t)$. In this case, constraints are added to the weight vector $\mathbf{w}$ to mitigate the noise in MSE sense [95]. The complete operational block diagram of the Sequential Subspace Estimator (SSE) is shown in Fig. 3.3. According to the figure, the estimated processor output $\hat{\mathbf{y}}(t)$ can be stated as:

$$\hat{\mathbf{y}}(t) = \mathbf{w}^T \mathbf{x}(t). \tag{3.22}$$



(a) Data Segmentation



(b) Subspace, Filtering, and Concatenation

Figure 3.2: SSE Subspace -Transformation Process

and the Mean Squared Error (MSE):

$$\begin{aligned}
\mathbf{e}(t) &= \mathbf{d}(t) - \hat{\mathbf{y}}(t) = \mathbf{d}(t) - \mathbf{w}^T(t)\mathbf{x}(t) \\
MSE = \mathbb{E}[\mathbf{e}^2(t)] &= \mathbb{E}[(\mathbf{d}(t) - \mathbf{w}^T(t)\mathbf{x}(t))^2] \\
&= \mathbb{E}[((\mathbf{d}(t) - \mathbf{w}^T(t)\mathbf{x}(t))(\mathbf{d}(t) - \mathbf{w}^T(t)\mathbf{x}(t))^T] \\
&= \mathbb{E}[\mathbf{d}^2(t) - \mathbf{w}^T(t)\mathbf{x}(t)\mathbf{d}(t) - \mathbf{d}(t)\mathbf{x}^T(t)\mathbf{w}(t) \\
&\quad + \mathbf{w}^T(t)\mathbf{x}(t)\mathbf{x}^T(t)\mathbf{w}(t)] \\
&= \mathbb{E}[\mathbf{d}^2(t)] - 2\mathbf{w}^T(t)\mathbb{E}[\mathbf{x}(t)\mathbf{d}(t)] \\
&\quad + \mathbf{w}^T(t)\mathbb{E}[\mathbf{x}(t)\mathbf{x}^T(t)]\mathbf{w}(t) \\
&= \Delta_d^2 - 2\mathbf{w}^T(t)\mathbf{P}_{xd} + \mathbf{w}^T(t)Q(t)\mathbf{w}(t) \qquad (3.23)
\end{aligned}$$

where

$$\begin{aligned}
Q(t) &= \text{noise covariance matrix,} \\
\Delta_d^2 &= \text{Variance of the desired dataset,} \\
\mathbf{P}_{xd} &= \text{Cross correlation between } \mathbf{x}(t) \textit{ and } \mathbf{d}(t) \\
&= \mathbb{E}[\mathbf{x}(t)d(t)] \\
&= \mathbb{E}[\mathbf{x}(t)\mathbf{x}^T(t)]\mathbf{w}_c(t)
\end{aligned}$$

Therefore, using the same analogy stated in section 3.2, the optimization problem can be formulated as:

$$\begin{aligned}
\min \; MSE = \Delta_d^2 + \mathbf{w}^T(t)Q(t)\mathbf{w}(t) - 2\mathbf{w}^T(t)\mathbf{P}_{xd} \\
\text{subject to: } \mathbf{w}^T\mathbf{w} = 1 \qquad (3.24)
\end{aligned}$$

Eq. (3.24) is the expected outcome or objective function of the proposed SSE.

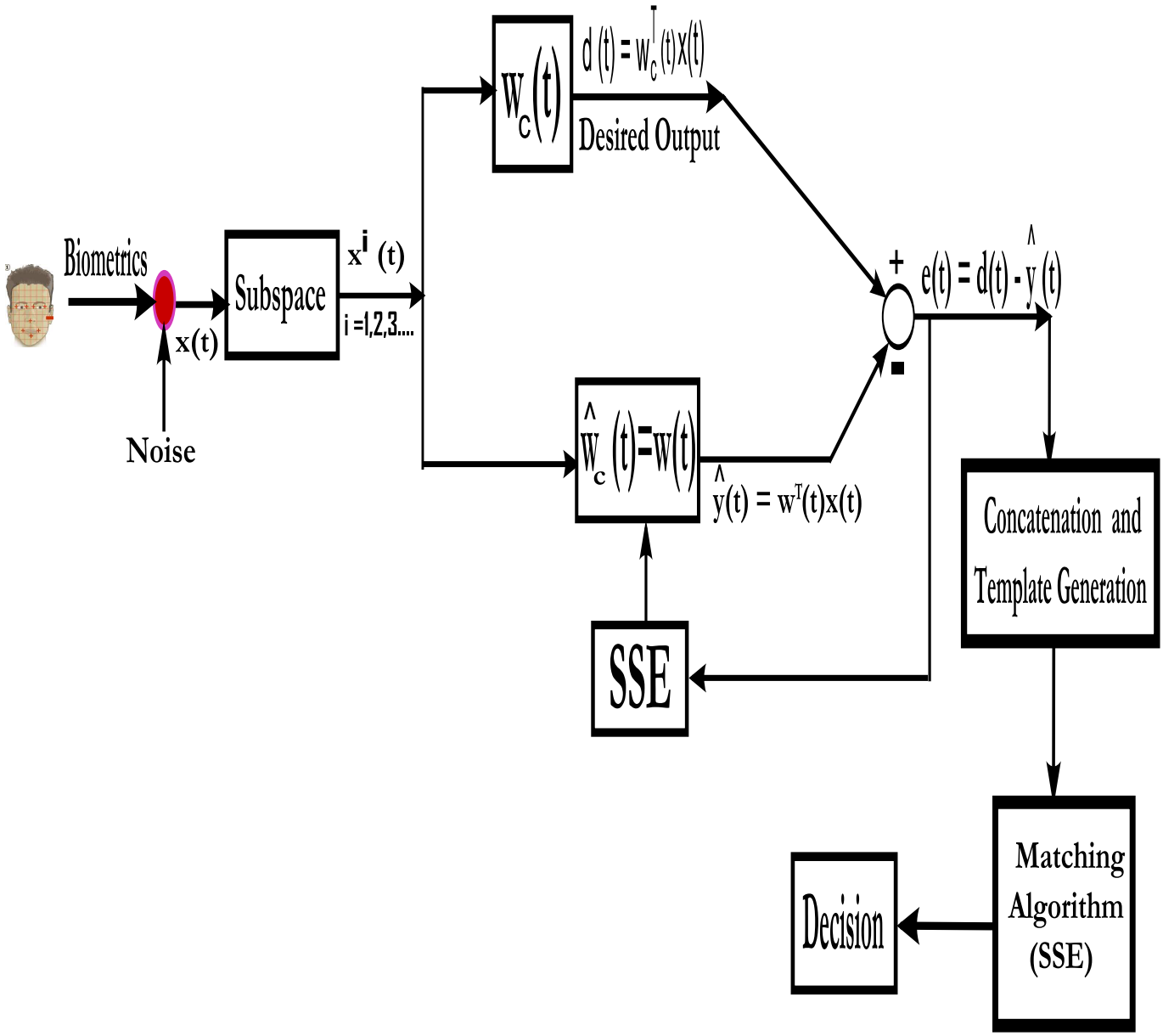


Figure 3.3: Sequential Subspace Estimator (SSE)

3.3.3 Working Principle

In the SSE authentication method, facial area and size and relative positions of eyes and lips have been extracted as biometric features. These features were selected because they are more visible, easy to extract, less changeable over time, and have the ability to authenticate an individual with greater accuracy in comparison to other features [68],[77]. The proposed SSE method is performed in three cycles. In its first cycle of operation, the main objective is to mitigate the noise and computational complexity associated with the large volume of biometric datasets. The steps involved in this SSE cycle are given below and in Fig. 3.4:

3.3.3.1 Extract Quality Facial Image

- Capture image
- Implement subspace method in order to segment the image in the image subspace (see Section 3.3.1)
- Perform SSE filtering method to mitigate the noise level
- Concatenate segmented images
- Train the system (See Section 3.3.6)
- Implement SSE method to detect the face
- Extract quality facial image
- Process extracted image for feature detection and extraction method (for next cycle)

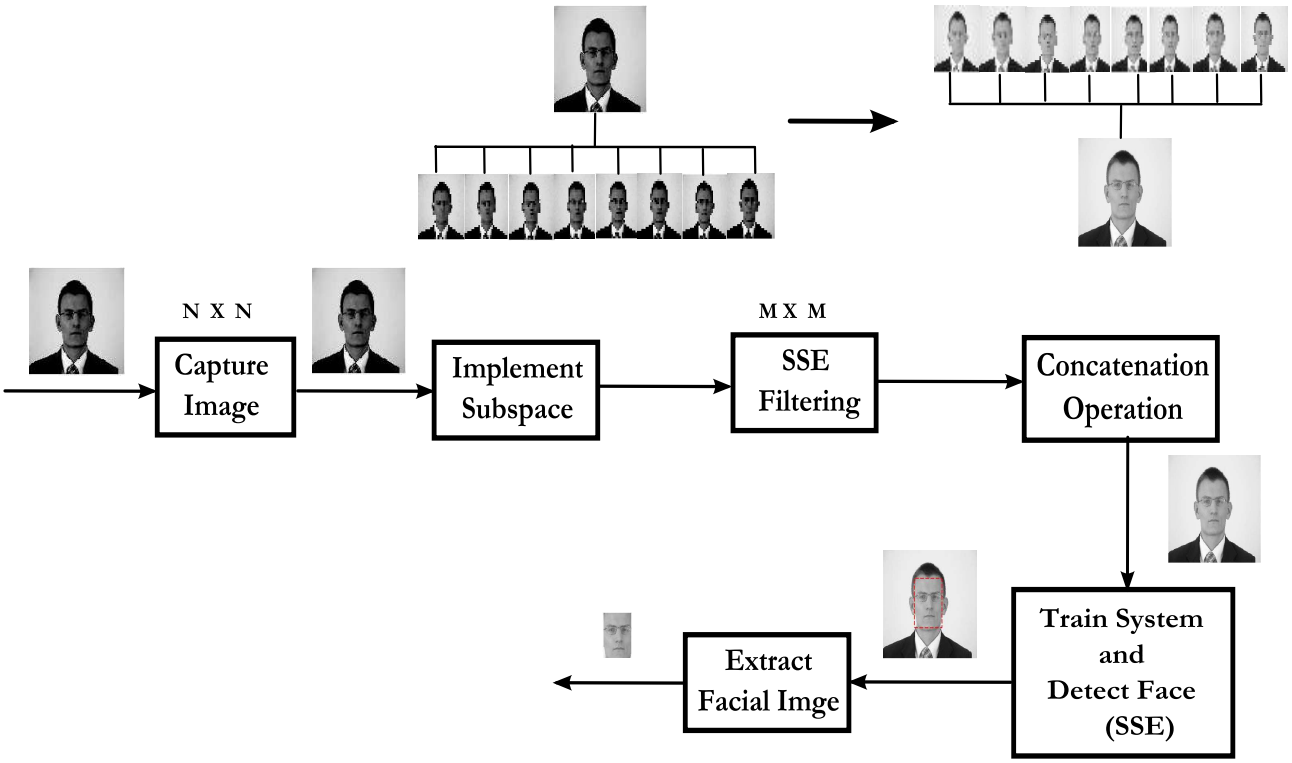


Figure 3.4: Extract Quality Facial Image

3.3.3.2 Detect and Create Biometric Template

In the second cycle, the main objective is to detect and extract the participating biometric features from the extracted facial image. The steps that are involved are given below and in Fig. 3.5:

- Train the system (See Section 3.3.6)
- Implement SSE to detect facial boundary, eyes, and lips
- Extract features
- Estimate facial area, size of eyes, and lips (See Fig. 3.5 and Appendix -C for Sample Data)
- Measure middle point between the two eyes as reference point
- Measure relative positions of eyes and lips from this reference point
- Use these extracted features as test biometric features (template)

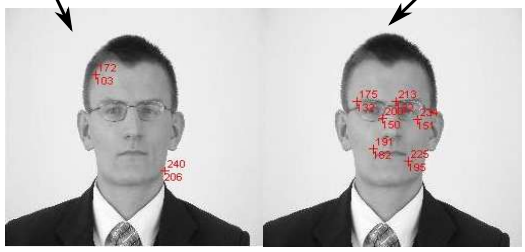
The method of training the system has been discussed in Section 3.3.6.

3.3.3.3 Biometric Template Matching

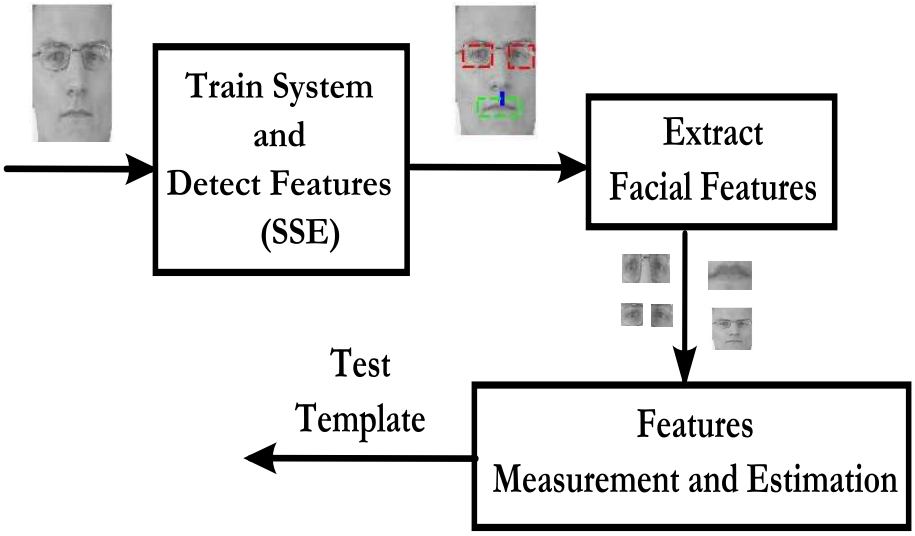
The proposed method is made independent of biometric traits; however the algorithm is being tested on facial images from the public nonlinear and heterogeneous "Put Face Database" [75] and less hetero-nonlinear "Indian Face Database" [76]. All image sizes have been considered (customized) to be 256×256 (8-bit). Afterwards, image is segmented in image subspace by a factor equal to the bit size. Therefore, 8 segmented datasets, each of size 32×32, are being constructed in the image subspace. The SSE algorithm is being developed to be implemented into each of the segmented datasets to mitigate the noise under consideration; thus there would be 8 iterative processes

	Left Top	Right Bottom
x	172	240
y	103	206

	Left Eye Top	Left Eye Bottom	Right Eye Top	Right Eye Bottom	Top Leaf	Bottom Leaf
x	176	200	213	234	191	225
y	131	150	132	151	182	195



(a) Feature Detection (Location)



(b) Feature Extrcation

Figure 3.5: Create Biometric Template

using the same vector space. The concatenate operation is performed on the filtered datasets in order to reconstruct the original image, hence the biometric template. The final step of the SSE authentication method is the verification process, where the test biometric template is compared with the template stored in the database system. In this comparison (matching process), the Euclidean distances of the stored biometric template (i.e. facial area, and size and relative positions of the eyes and lips) are compared with the biometric template generated from the received live image. This matching process can be seen in Fig. 3.6. The steps involved in the matching process are stated below:

- Use the test template as an input to the system
- Compare the test template with the stored template in the database system
- Compare with the threshold values
- Make the authentication decision

3.3.4 Sequential Subspace Estimator

The proposed method is executed under the assumption that the associated noise in the received facial image is nonlinear, nonstationary, and heterogeneous. In this approach, the system performs a sequential recursive filtering process in the image subspace to cancel out the nonlinear and heterogeneous noise. Afterwards, it extracts and estimates the size of the facial area, as well as the relative positions and size of the eyes and lips, in order to encode and create the biometric templates. This template is then stored in the biometrics database to be compared with other encoded biometrics. Using Eq. (3.8), the data received at the output of the processor can be stated as:

$$\mathbf{y}(t) = \mathbf{w}^T(t)\mathbf{x}(t) = \mathbf{w}^T(t)\mathbf{s}(t) + \mathbf{w}^T(t)\mathbf{n}(t). \tag{3.25}$$

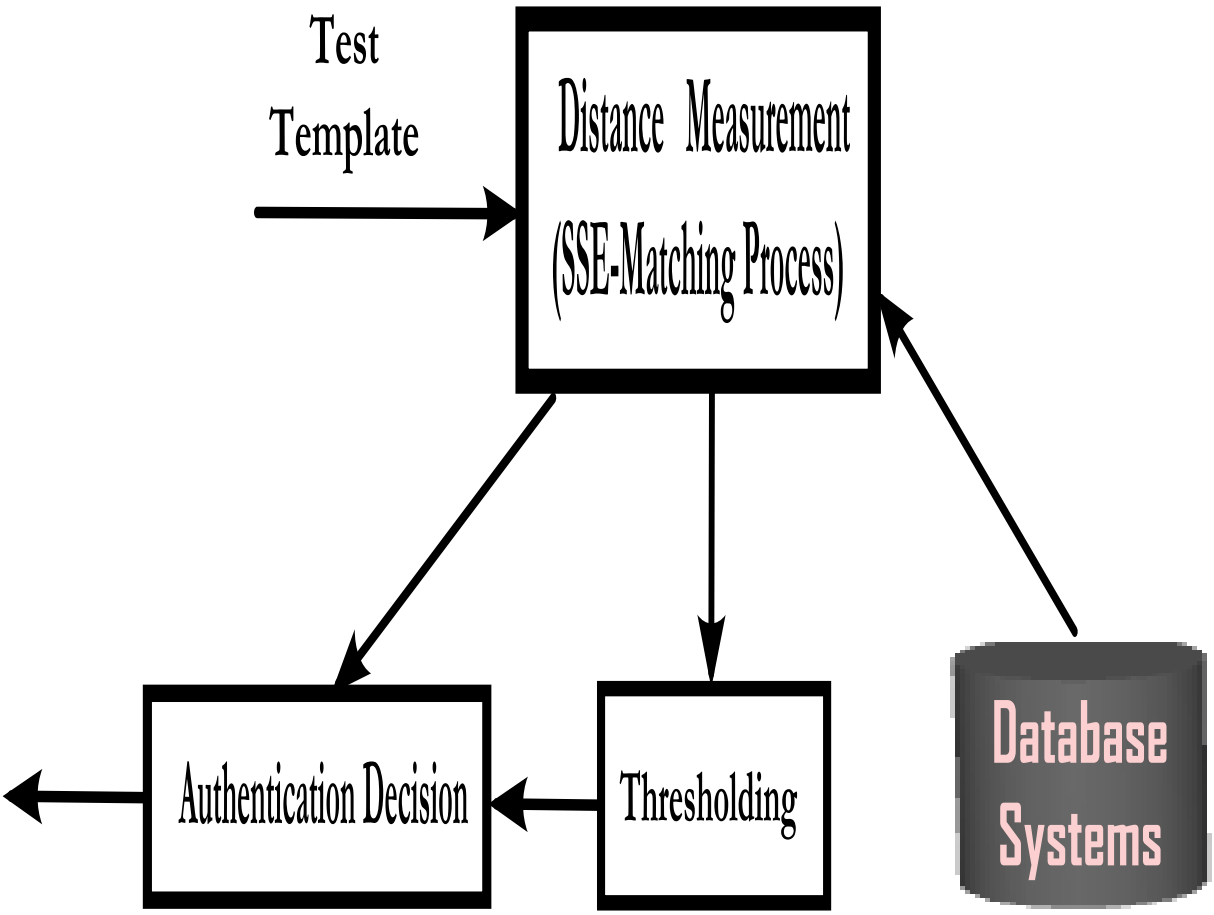


Figure 3.6: Template Matching

The main objective is to determine the minimum value of the Mean Squared Error (MSE), i.e. Minimum Mean Squared Error (MMSE). Once this value is obtained, the desired features from the underlying noise environment can be encoded to maximize the mutual information $I(\hat{\mathbf{y}}; \mathbf{d})$.

The proposed SSE optimization problem can be restated as follows:

$$\begin{aligned} \min \ MSE &= \Delta_d^2 + \mathbf{w}^T(t)Q(t)\mathbf{w}(t) - 2\mathbf{w}^T(t)\mathbf{P}_{xd} \\ \text{subject to: } & \mathbf{w}_j^T\mathbf{w}_j = 1, \text{ and } j = 1, 2, ..., M. \end{aligned} \tag{3.26}$$

The conditional mean is an optimal MMSE estimator and is computationally efficient; since it is recursive, it can process the features as they arrive. For linear and homogeneous systems, the Kalman Filter (KF) estimate of the conditional mean and the MMSE is optimal. Unfortunately, KF is an inadequate solution for the nonlinear and heterogeneous environment and EKF is conditionally inefficient. The proposed method is the promising alternative to overcome these challenges.

Now, consider an unknown dynamic system with state vectors $\mathbf{w}_c$ (subscript c implies constraint to vectors) where the system is driven by random noise. If the system can be modeled as a filter, then the proposed state equation can be written as [95-103]:

$$\begin{aligned} \mathbf{w}_c^i(t+1) &= F(t)\mathbf{w}_c^i(t) + \upsilon(t) \\ R &= \Psi_p^2 I \end{aligned} \tag{3.27}$$

where $F(t+1|t)$ is the state transition matrix, which is a function of time and relates the state vector from t to $t+1$, and $\upsilon(t)$ is processed noise. The covariance matrix of the processed noise is represented by R [95],[96]; where I may assume as an identity matrix, t is the time index, and the superscript $'i'$ $(i = 1, 2, ..., L)$ represents the number of linearly independent datasets of dimension $M \times M$ in the

image subspace. For convenience, the $'i'$ may be ignored for the rest of the cases.

If the operating environment is considered to be linear, stationary, and homogeneous, then the state vectors $\mathbf{w}_c$ would be fixed or a function of any arbitrary constant. In this case, the state transition matrix $F(t+1|t)$ is considered to be an identity matrix. However, for a nonlinear, nonstationary, and heterogeneous noise environment, a more complex method for $F(t+1|t)$ needs to be developed so that the model can track the changes in response to environmental fluxes.

Now, the measurement equation can be represented by [95],[98]:

$$\begin{aligned} \mathbf{d}(t) &= \mathbf{x}(t)^T \mathbf{w}_c(t) + \rho(t) \\ &= H[t, \mathbf{w}_c(t)] + \rho(t) \end{aligned} \tag{3.28}$$

where $\rho(t)$ is measurement (observation) noise, considered to be linear, stationary, and homogeneous with zero mean, and covariance is given by:

$$\mathbb{E}[\alpha(a)\alpha(b)] = \Delta_m^2(t)\Delta_{ab} \tag{3.29}$$

In the proposed method, the associated noise in the extracted dataset is considered to be nonlinear, nonstationary, and heterogeneous. Therefore, the proposed measurement from Eq. (3.28) under these assumptions can be restated as:

$$\mathbf{d}_{non}(t) = h[t, \mathbf{w}_c(t), \rho(t)] \tag{3.30}$$

where $h[.]$ is the Jacobian evaluation of $H[.]$.

Eqs. (3.27) and (3.30) are the state and measurement equations respectively, designed for the proposed SSE. These equations are being used to model the SSE method in the image subspace based on the proposed constraints given in Eq. (3.26).

Now, the estimate $\hat{\mathbf{y}}(t)$ of the desired dataset $\mathbf{d}(t)$ can be stated as [95],[99]:

$$\hat{\mathbf{y}}(t) = h[t, \hat{\mathbf{w}}_c(t)]. \tag{3.31}$$

The MSE between the desired features and the estimated output can be defined by using Eq. (3.26) as follows:

$$\begin{aligned} \mathbf{e}(t) &= \mathbf{d}(t) - \hat{\mathbf{y}}(t) && (3.32) \\ \min_{\|\hat{\mathbf{w}}_c^j\|=1} MSE &= \mathbb{E}[|e(t)|^2] \\ &= \Delta_d^2 + \hat{\mathbf{w}}_c^T(t) Q(t) \hat{\mathbf{w}}_c(t) \\ &\quad -2\hat{\mathbf{w}}_c^T(t)\mathbf{P}_{xd}. && (3.33) \end{aligned}$$

An initial estimate of the weight vector starts with the relation stated in Eq. (3.3) and uses the estimated covariance matrix calculated with Eq. (3.1) from sample dataset. Thus, using SSE, $\hat{\mathbf{w}}_c$ would be converged to the optimal value in MSE sense.

The innovation or the measurement residue may now be stated as [95],[96],[98]:

$$\nu(t) = \mathbf{d}(t) - \hat{\mathbf{y}}(t|t-1). \tag{3.34}$$

Hence, the updated state becomes:

$$\hat{\mathbf{w}}_c(t+1|t+1) = \hat{\mathbf{w}}_c(t+1|t) + \mathbf{k}(t+1)\nu(t+1) \tag{3.35}$$

where $\mathbf{k}$(t) is the filter gain. Now, $\mathbf{k}$(t) can be written in terms of the first order (Jacobian) measurement matrix [95]:

$$\mathbf{k}(t+1) = P(t+1|t)[\frac{\partial h(t, \hat{\mathbf{w}}_c(t))}{\partial \mathbf{w}_c(t)}]\mathbf{M}^{-1}(t+1) \tag{3.36}$$

and the estimated (predicted) conditional covariance matrix [95-98]:

$$P(t+1|t) = F(t)P(t|t)F^T(t) + R(t). \tag{3.37}$$

Measurement Innovation covariance:

$$\begin{aligned} \mathbf{M}(t+1) &= \Delta_m^2(t+1) + [\frac{\partial h(t, \hat{\mathbf{w}}_c(t))}{\partial \mathbf{w}_c(t)}]^T \\ &\quad .P(t+1|t)[\frac{\partial h(t, \hat{\mathbf{w}}_c(t))}{\partial \mathbf{w}_c(t)}]. \end{aligned} \tag{3.38}$$

The covariance update [95],[96]:

$$P(t+1|t+1) = P(t+1|t) - \mathbf{k}(t+1)M(t+1)\mathbf{k}(t+1)^T. \tag{3.39}$$

Using the Matrix Inversion Lemma [95], it can be written as:

$$\begin{aligned} P(t+1|t+1)^{-1} &= [(P(t+1|t))]^{-1} + \frac{\partial h(t, \hat{\mathbf{w}}_c(t))}{\partial \mathbf{w}_c(t)} \\ &\quad [\Delta_m^2]^{-1}[\frac{\partial h(t, \hat{\mathbf{w}}_c(t))}{\partial \mathbf{w}_c(t)}]^T. \end{aligned} \tag{3.40}$$

If the first term $[(P(t+1|t))]^{-1}$ is neglected due to the large initial value condition, then the above equation may be restated as [95],[99,[100]]:

$$P(t+1|t+1)^{-1} = \frac{\partial h(t, \hat{\mathbf{w}}_c(t))}{\partial \mathbf{w}_c(t)}[\Delta_m^2]^{-1}[\frac{\partial h(t, \hat{\mathbf{w}}_c(t))}{\partial \mathbf{w}_c(t)}]^T. \tag{3.41}$$

This is a recursive process beginning with Eq. (3.27) that stops once the stop criteria are met. The algorithmic diagram of the SSE model can be seen in Fig. 3.7 and its associated computational complexities have also been shown (i.e. marked by arrow) in the diagram.

The differences shown in Eq. (3.34) represent the differences between the desired

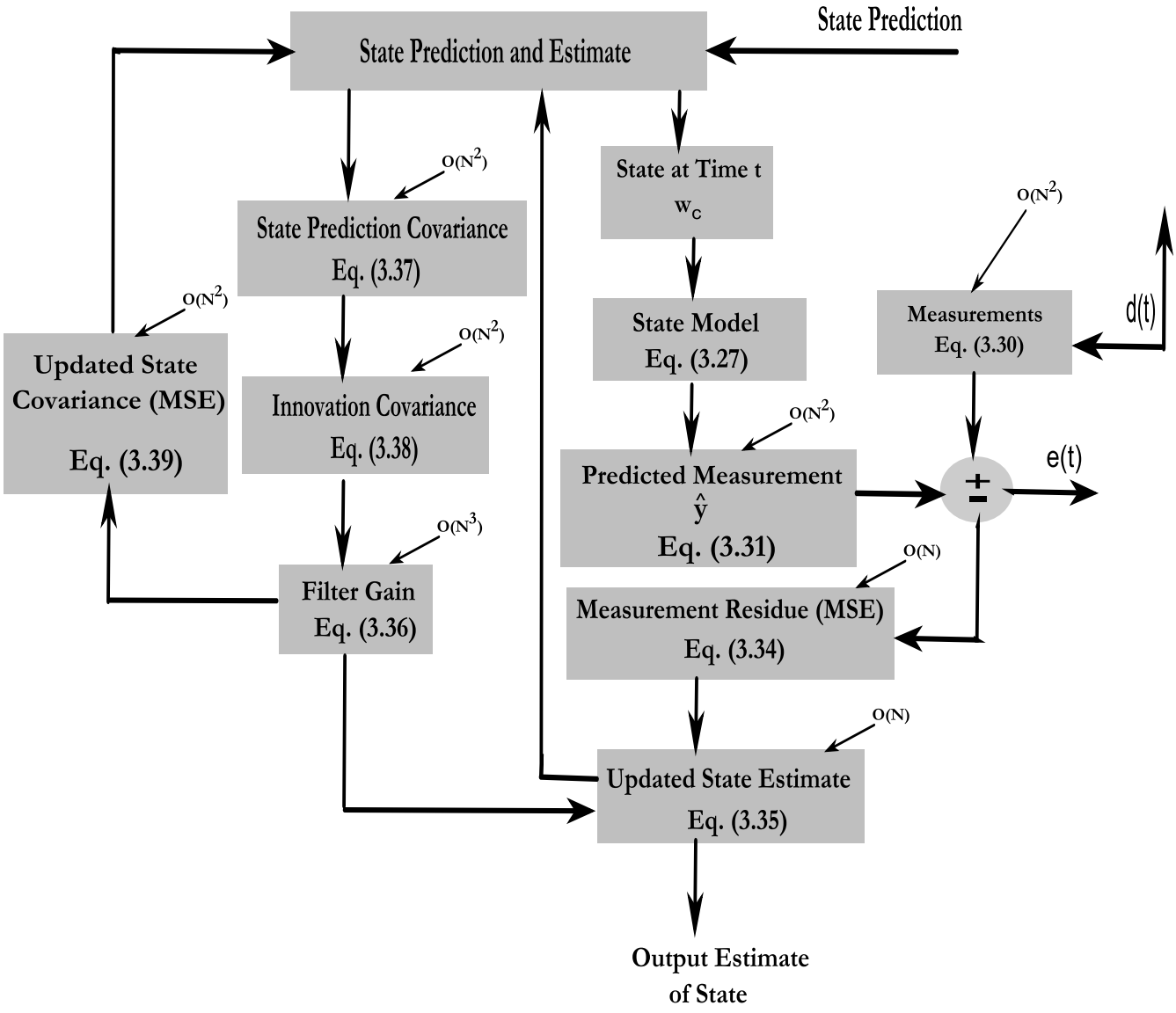


Figure 3.7: SSE Algorithm - One Cycle of Operation

output and the actual output, estimated using the weight vector and the asymptotic covariance matrix. If the desired output $\mathbf{d}(t)$ can be interpreted as an approximation of the actual desired dataset using the constraint, then the actual data sample $\mathbf{a}(t)$ and the approximated desired data sample $\mathbf{d}(t)$ with an approximation error $\beta(t)$ can be related as follows:

$$\mathbf{a}(t) = \mathbf{d}(t) + \beta(t). \tag{3.42}$$

If $\mathbf{a}(t)$ and $\beta(t)$ are assumed to be linear, homogeneous, and uncorrelated, then

$$\Delta^2(t) = MMSE + \mathbb{E}[\beta^2]. \tag{3.43}$$

In the proposed SSE method, the measurement $\mathbf{d}(t)$ in Eq. (3.28) is generated using the realistic approximation (i.e. training dataset) of the desired dataset. So, $\Delta^2(t)$ could be approximated based on the MMSE achieved by an observed dataset, the approximation of the constraint weight vector $\mathbf{w}_c(t)$, and the filtering model as stated above.

3.3.5 Selection of Parameters

The state transition matrix $F(t+1|t)$ and covariance R of Eq. (3.27) has a more complex form in a nonlinear, nonstationary, and heterogeneous system. For that reason, the parameters of the state equation must be chosen in such a way that the system model can track and adapt changes caused by the diversity of the environment [73],[91],[95]. Under these assumptions, the state transition matrix is not an identity matrix [i.e. $F(t+1|t) \neq I$], which may make the state equation unstable; the stability of the filter may be assured by the observability condition. The state covariance matrix R is the total uncertainty from adapting the linear and stationary environment assumption represented by the identity state transition matrix in equations (3.27) and

(3.37). The effect associated with this deviation due to a nonlinear and nonstationary environment $[\upsilon(t) \neq 0 \; and \; F(t+1|t) \neq I]$ prevents the proposed Sequential Subspace Estimator from minimizing the objective function in Eq. (3.33) to values that drive the estimation and detection accuracy to an optimal level. Furthermore, the estimate of the optimal weight vector $\hat{\mathbf{w}}_c$ is also able to follow variations in the weight vector due to a nonlinear, nonstationary, and heterogeneous noise environment.

In this experiment, the range of parameters selected for the observation noise, state transition matrix, and the covariances are based on the estimation models discussed in [48],[70],[74],[93],[95],[96],[98]. The PCA is an orthogonal transformation method based on the estimation of the zero mean, eigenvalues and corresponding eigenvectors for constructing the principal components of the feature vectors from the extracted features. Parameters were selected for the PCA method based on the method outlined in [93] and Section 1.2.1. In the PCA-Bayesian and MLE methods, the parameters for the noise covariance matrix were modeled based on the method given in [48],[74]. Parameters for the PCA-Wiener have been selected based on the method stated in [95] and [96]. Finally, the parameters used for the proposed SSE and Extended Kalman Filter have been selected based on [70],[95],[96],[98]. In both cases, three parameters for the transition matrix (0.5, 0.75, and 1) and three parameters for the process noise (10^{-4}, 10^{-3}, and 10^{-2}) have been chosen. Afterward, in using these parameters, a looping operation has been performed and has taken the average from the outcome of this operation. The data obtained from this experimental is included in $Appendix-C$. The list of parameters used in these experiments is given in Table 3.1:

3.3.6 Training Using MLP-SSE

A Multilayer Perception (MLP) is a feed forward neural network model with one or more hidden layers between the input and output. In theory, a neural network is an arbitrary mapping method that maps one vector space to another vector space using

Table 3.1: *List of Parameters Used for The Experiment*

Methods	**Transition Matrix**	**Process Noise**	**Observation Noise**
Proposed SSE	0.5, 0.75, and 1	10^{-4}, 10^{-3}, and 10^{-2}	0.1
Extended Kalman Filter	0.5, 0.75, and 1	10^{-4}, 10^{-3}, and 10^{-2}	0.1
PCA	Not Applicable	Not Applicable	Not Applicable
PCA-Wiener	Not Applicable	10^{-2}	0.1
PCA-MLE	Not Applicable	10^{-2}	0.1

some a priori unknown information hidden in the data. The process of capturing unknown data by adjusting the weight coefficients under certain constraints is known as the training of the neural network. This multilayer neural network training can be considered state estimation problems and is based on prediction and correction [70],[71],[73]. Therefore, a supervised training framework using the proposed SSE algorithm can be used to train this network. In this case, output values are compared with the target to compute the value of the error function as stated by Eq. (3.33) in Section 3.3.5. This error then feeds back through the network. Finally, based on this information, the proposed SSE algorithm can be used to adjust weight vectors and reduce the value of MSE. The summary of the SSE algorithm for training the MLP is presented as follows:

- Initialize of parameters, as has been done in the SSE filter method.
- Input the vectors (matrix) data in the MLP network.
- Compare the values (output from the network, Eq. 3.31) with the desired one (Eq. 3.30) and compute the correction factor given in Eq. (3.32).

- Estimate the gain using Eq. (3.36).
- Correction factor is then fed back to the network.
- Update estimate of the state using Eq. (3.35).
- Update the covariance using Eq. (3.39).
- MLP with weight vectors using Eq. (3.35) operates on the input to produce the actual output, and the predicted $\hat{y}(t)$ operates on the current desired response to produce the estimate of the weight vectors $\hat{w}(t)$.
- Check with the threshold values (pre-assigned) to see if it fulfills the conditions.
- Stop the process if it fulfills the stop criteria, otherwise continue the next iteration.

3.3.7 Computational Complexity

Computational complexity is an important issue for the proposed Sequential Subspace Estimator (SSE) model. Starting from Eq. (3.30), the SSE's computational complexity for Jacobian evaluation is $\mathbf{O}(N^2)$. The complexity of Eq. (3.31), for estimating the desired dataset, is $\mathbf{O}(N^2)$. The computational bottleneck for computing the inverse of the updates covariance at each cycle is $\mathbf{O}(N^3)$. The complexity for updating the weight vector in Eq. (3.35) is $\mathbf{O}(N^2)$, the gain in Eq. (3.36) is $\mathbf{O}(N^3)$, and the predicted covariance in Eq. (3.37) is $\mathbf{O}(N^2)$. The computational cost for innovation covariance stated in Eq. (3.38) is $\mathbf{O}(N^2)$; the covariance update in Eq. (3.39) is $\mathbf{O}(N^2)$ and in Eq. (3.41) is $\mathbf{O}(N^3)$.

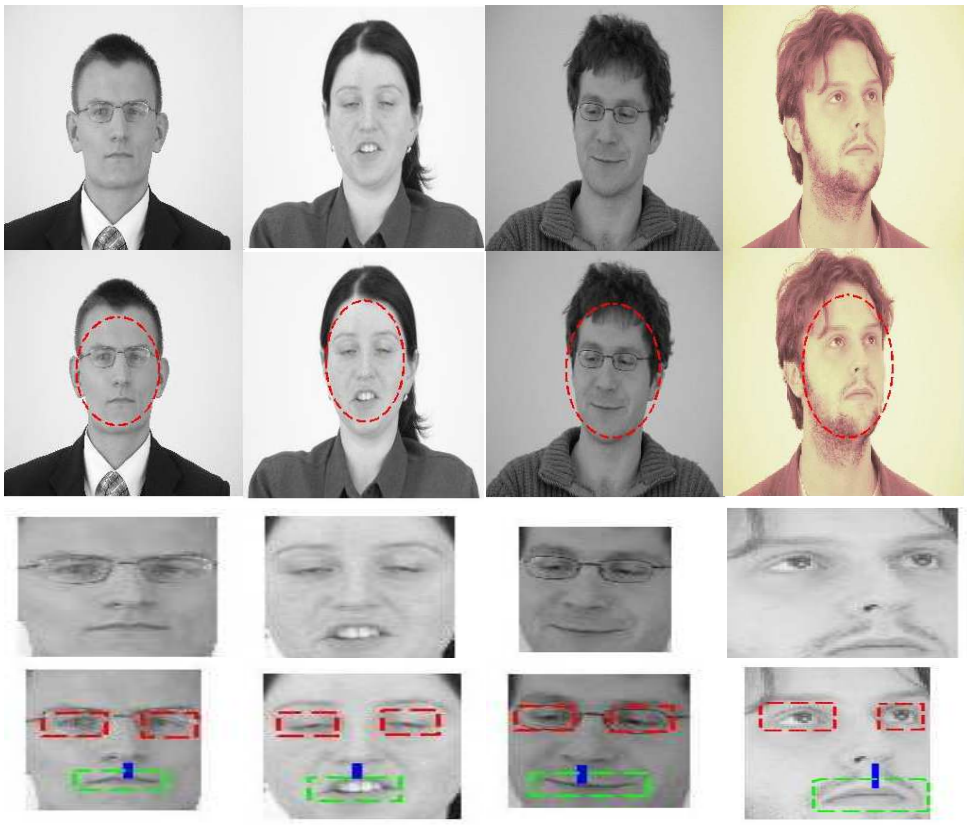


Figure 3.8: A Sample from Test Data (Put Face Database)

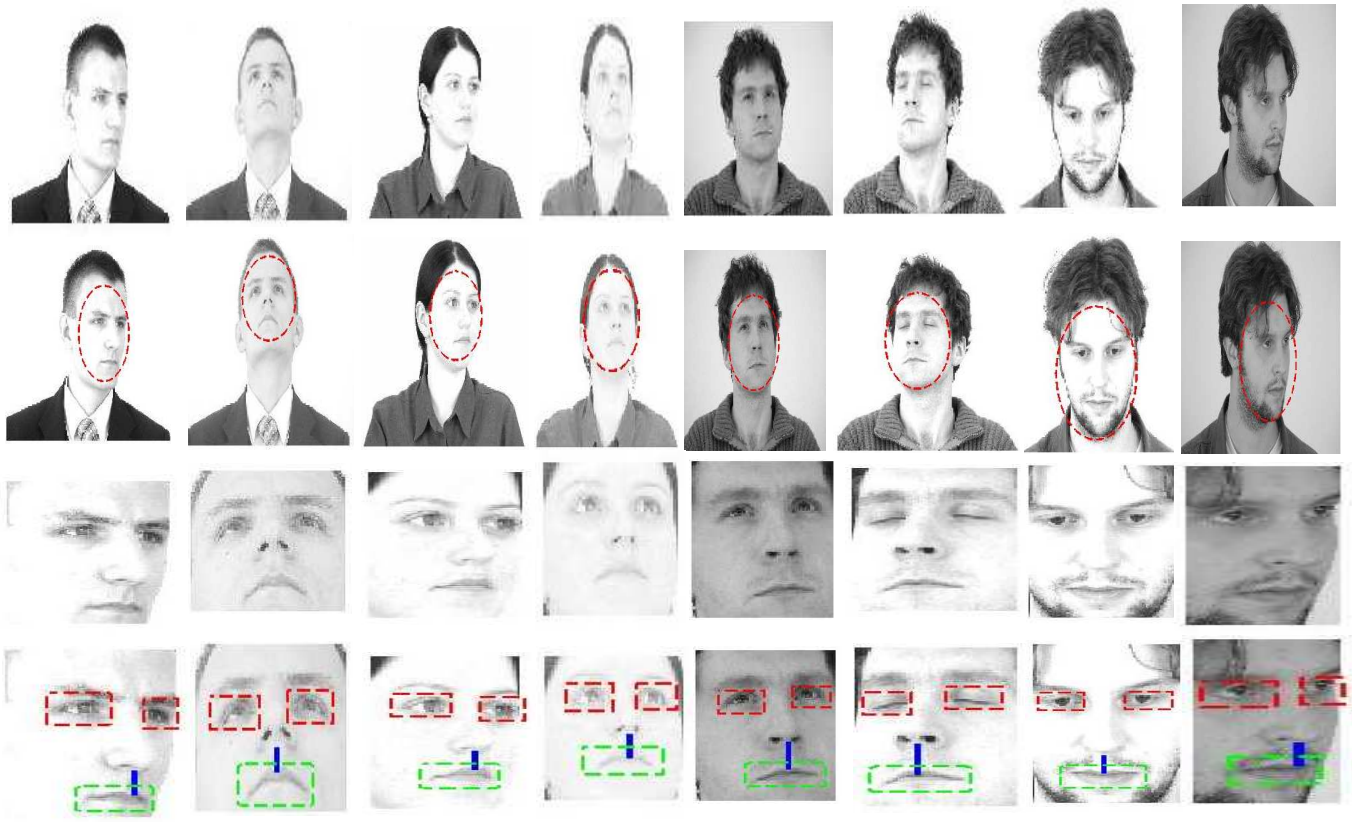


Figure 3.9: A Sample from Training (Put Face Database)

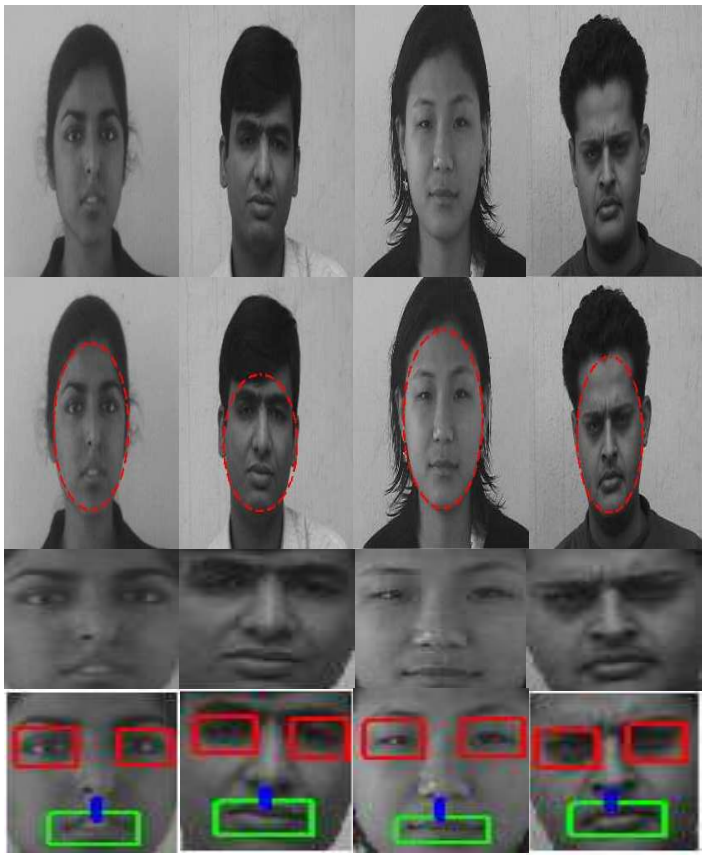
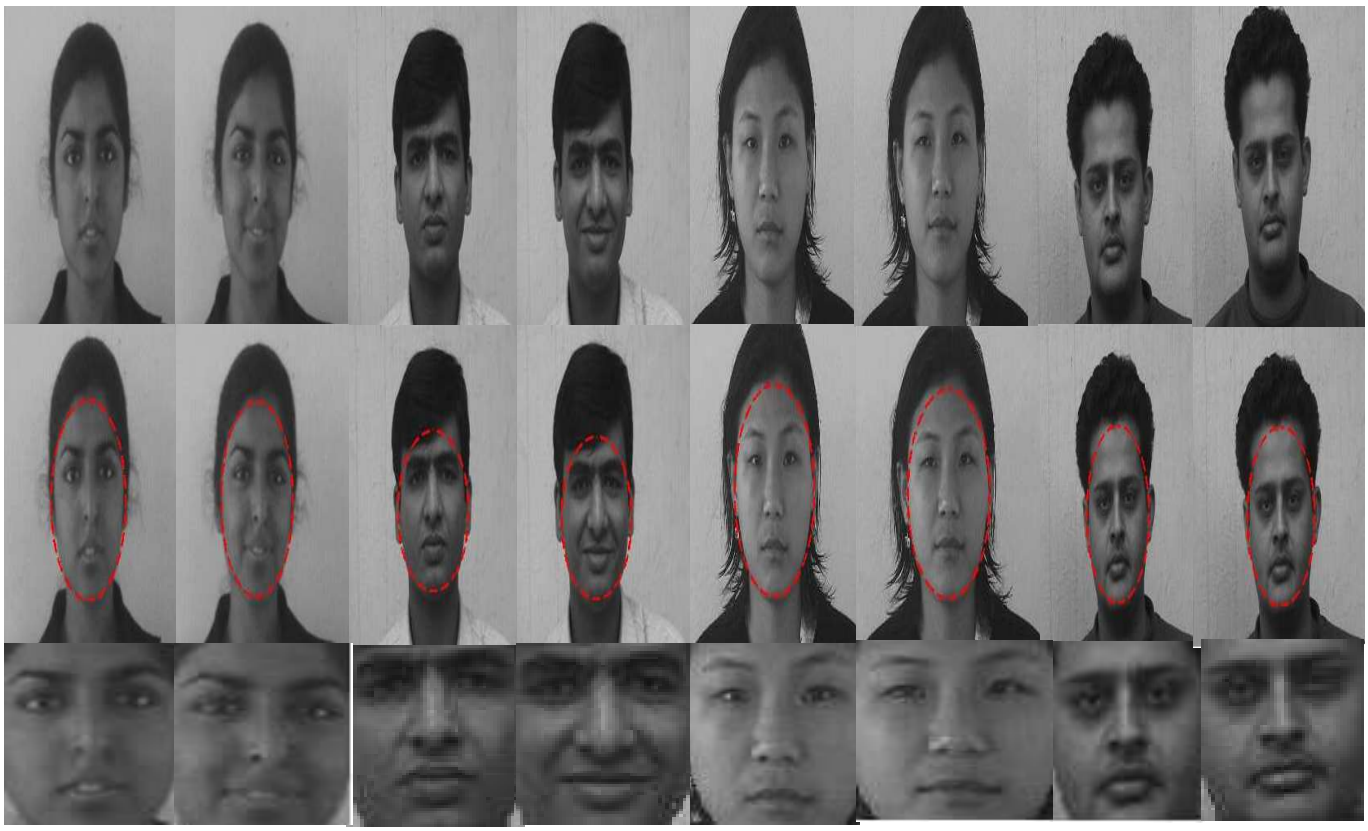


Figure 3.10: A Sample from Test Data (Indian Face Database)



a. First Row -Original Image, b. Second Row - Computation of Facial Boundaries , c. Third Row - Extracted Face

Figure 3.11: A Sample from Training Data (Indian Face Database)

3.4 Experimental Results and Analysis

The proposed subspace sequential state estimation method is considered to be a general method for a biometric authentication system. It was tested on two public databases: the "Put Face Database" (nonlinear and heterogeneous) and the "Indian Face Database" (less hetero-nonlinear). In the experiment, we used the "Put Face Database" to create three sets of image databases: $dB1$, $dB2$, and $dB3$; with 20, 40, and 60 subjects, respectively. As well, we used the "Indian Face Database" to create two more sets of image databases, $dB4$ and $dB5$, with 10 and 20 subjects respectively. The parameters used in this experiment are discussed in Section 3.3.5 and listed in Table 3.1. The data obtained from this experiment is included in $Appendix - C$.

Each of the $dB1$, $dB2$, and $dB3$ databases contains 10 images of each subject. Therefore, there are 200, 400, and 600 images in databases $dB1$, $dB2$, and $dB3$, respectively. In this process, 7 out of 10 face images from each subject were used to train the system. The rest of the three subjects$'$ images were used for testing purposes. Images of different orientations and facial expressions were taken under different lighting conditions, as a function of time. Furthermore, the original size of each image in the database (3-D) is $1536 \times 2048 \times 3$, but all the images are considered to be 8-bit 2-D images of size 256×256.

Furthermore, each of the $dB4$ and $dB5$ databases contains 5 images of each subject; thus there are 50 and 100 images in databases $dB4$ and $dB5$, respectively. In this process, 3 out of 5 face images from each subject were used to train the system. The rest of the two subjects$'$ images were used for testing purposes. Images were taken from the same frontal position, using the same lighting conditions and background (i.e. less nonlinear and less heterogeneous). Furthermore, the original size of each image in the database was 640×480, but all of the images were considered to be 8-bit 2-D images of size 256×256.

The conversion to 256 × 256 image size was done by taking every 6th or 3rd (i.e. 1536/256=6 or 640/256=3) row and 8th or 2nd (i.e., 2048/256=8 or 480/256=2) column datapoints from the original datasets. This conversion process has already been discussed in Section 3.3.1. The size of the images from the two databases are presented in Table 3.7, and the maximum size of the training dataset was approximately 19MB. In both cases, Microsoft Access in conjunction with MatLab database design architecture was used to implement the system. Two sample datasets (test and training) from the "Put Face Database" are shown in Fig. 3.8 and Fig. 3.9, respectively; and those from the "Indian Face Database" are shown in Fig. 3.10 and Fig. 3.11, respectively. Since the proposed biometric authentication method has two parts–identification and verification–the performance evaluation of the proposed method was conducted based on these two modes.

3.4.1 Identification

The experiment for the identification process was conducted using databases $dB1$, $dB2$, $dB3$, $dB4$, and $dB5$, based on the ability of the system to correctly classify an identification request. In this process, the received image was compared with all of the stored images in the database. During the comparison cycle, the Euclidean distances of the two feature vectors (biometric templates) were measured, and the smallest Euclidean distance was labeled as the closest identity of the subject. There were 200, 400, 600, 50, and 100 samples in databases $dB1$, $dB2$, $dB3$, $dB4$, and $dB5$, respectively; therefore there were 200, 400, 600, 50, and 100 identification attempts.

The identification process can be stated as follows:

$$\min_k \quad = \quad \|\Phi - \Phi_k\| \tag{3.44}$$

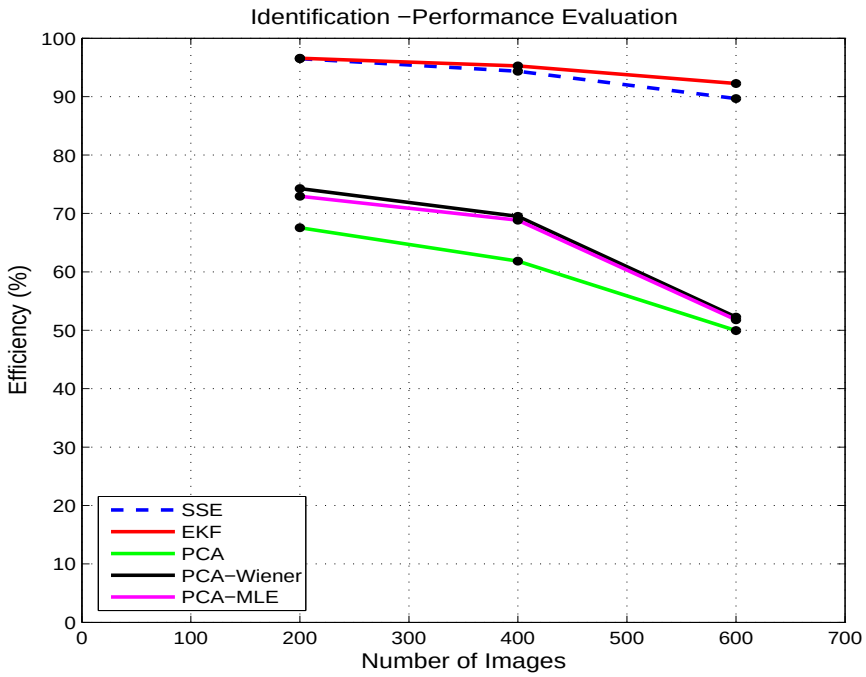
where Φ is the biometric template of the received live image, and Φ_k represents

the stored biometric templates (images or feature vectors) in the database system. Here, $k = 1, 2, ...p$; where p is the total number of stored subject images or templates in the database system.

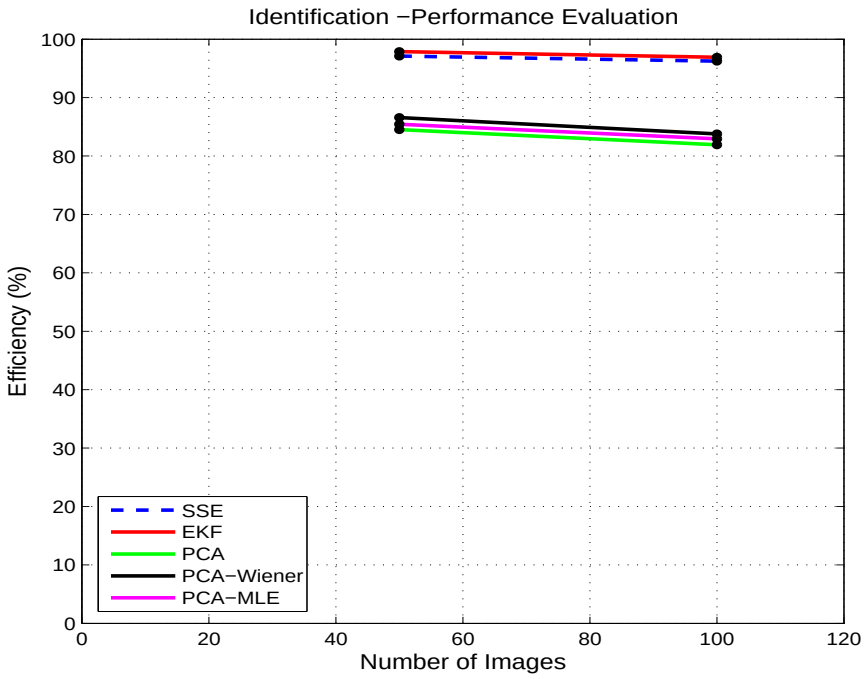
The performance of the identification process was evaluated using CRR as stated in Section 1.1.4. The experimental results rendered a percentage of CRR for each of the databases, and their averages were recorded. Comparisons of the proposed SSE method with the state-of-the-art algorithms EKF, PCA, PCA-MLE, and PCA-Wiener were also recorded and shown in Table 3.2, Table 3.3, and Fig. 3.12. A comparison of the proposed SSE method using L/2 (64×64), L (32×32), and 2XL (16×16) datasets in the image subspace has also been presented in Table 3.11. The parameters used in this experiment are discussed in Section 3.3.5 and listed in Table 3.1. The data obtained from this experiment is included in $Appendix - C$.

Table 3.2: *Performance Evaluation in (%) - CRR Comparison (Put Face Database)*

Methods	$dB1$	$dB2$	$dB3$	*Average*
Proposed SSE	96.49	94.35	89.67	93.50
EKF	96.57	95.25	92.25	94.69
PCA	67.55	61.83	49.95	59.78
PCA-Wiener	74.25	69.50	52.25	65.33
PCA-MLE	72.95	68.85	51.80	64.53



(a) PUT Face Database



(b) Indian Face Database (With Less Hetero-Nonlinear Dataset)

Figure 3.12: Identification - Performance Comparison

Table 3.3: *Performance Evaluation in (%) - CRR Comparison (Indian Face Database)*

Methods	$dB4$	$dB5$	*Average*
Proposed SSE	97.12	96.25	96.68
EKF	97.88	96.91	97.35
PCA	84.53	81.93	83.21
PCA-Wiener	86.57	83.77	85.17
PCA-MLE	85.43	82.95	84.19

3.4.2 Verification

In the verification process, the received feature vectors that comprise the biometric template only need to be compared with the biometric template of the claimed individual. The verification of a genuine person was conducted by comparing the face image of each person with their other face images. Imposter processing was conducted by comparing the face image of one person with the face images of other persons. During the comparison cycle, the Euclidean distance was computed and compared with the threshold value to determine the legitimacy of the claimed individual. There were 60, 120, 180, 20, and 40 testing samples for databases $dB1$, $dB2$, $dB3$, $dB4$, and $dB5$, respectively; therefore there were 60, 120, 180, 20, and 40 genuine matches. The verification process can be stated as follows:

$$True \quad = \quad \|\Phi - \Phi_k\| < \tau \tag{3.45}$$

where τ is the threshold value.

The performance of the verification was evaluated using the Equal Error Rate

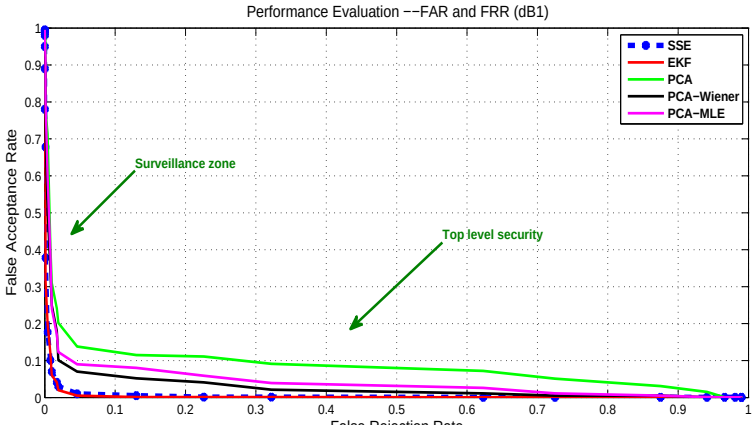
(EER) stated in Section 1.1.4. The lower the point of EER, the higher the verification performance. The percentages of FAR and FRR and the corresponding EER points were determined and the experimental results recorded. The experimental results, based on the proposed SSE method for each of the five databases, are presented in Tables 3.4-3.6 and Table 3.10. The graphical outcomes of these results are also presented in Figs. 3.13-3.16 and Figs. 3.18-3.20. The parameters used in this experiment are discussed in Section 3.3.5 and listed in Table 3.1. The data obtained from this experiment is included in $Appendix - C$.

Table 3.4: *Performance Evaluation in (%) - FAR and FRR Comparison (Put Face Database)*

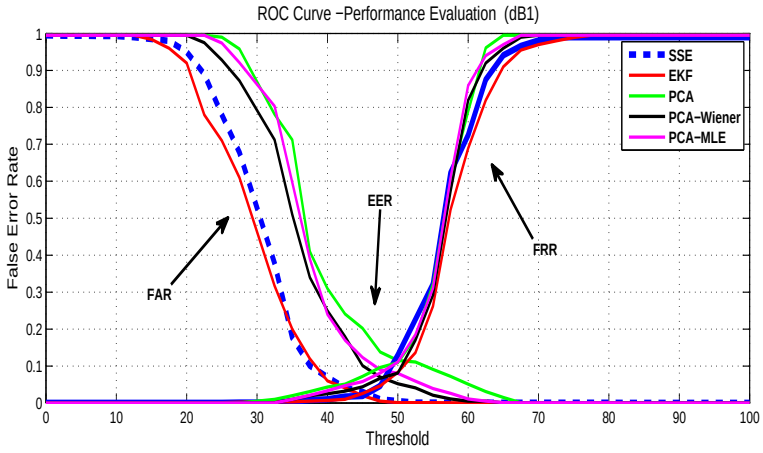
Methods	$dB1$		$dB2$		$dB3$	
	FAR	FRR	FAR	FRR	FAR	FRR
Proposed SSE	1.25	2.09	1.96	6.24	4.86	9.87
EKF	1.18	4.17	1.78	6.12	3.70	8.96
PCA	11.86	9.70	17.87	9.55	21.09	38.86
PCA-Wiener	7.81	8.54	10.06	13.67	18.74	38.79
PCA-MLE	8.93	9.21	14.18	17.25	20.08	38.75

3.4.3 Comparisons

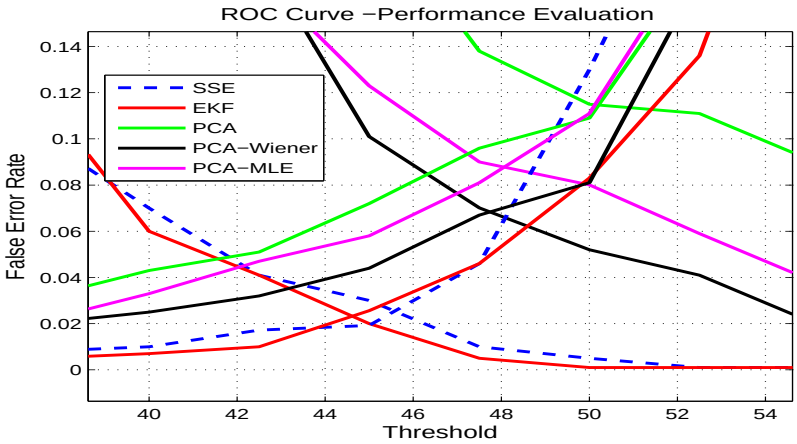
In this experiment, two important aspects of the biometric authentication method have been addressed: the extraction of quality features from a nonlinear, nonstationary, and heterogeneous environment leading to authentication accuracy, and computational complexity (execution time). These two elements are considered to be the



(a) FAR and FRR -dB1

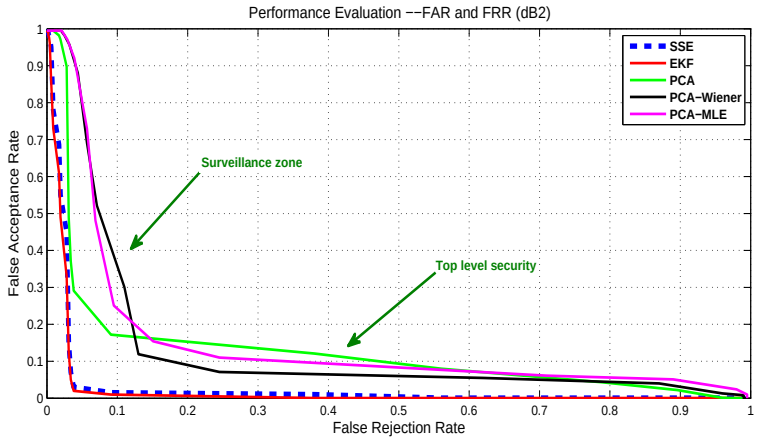


(b) ROC -dB1

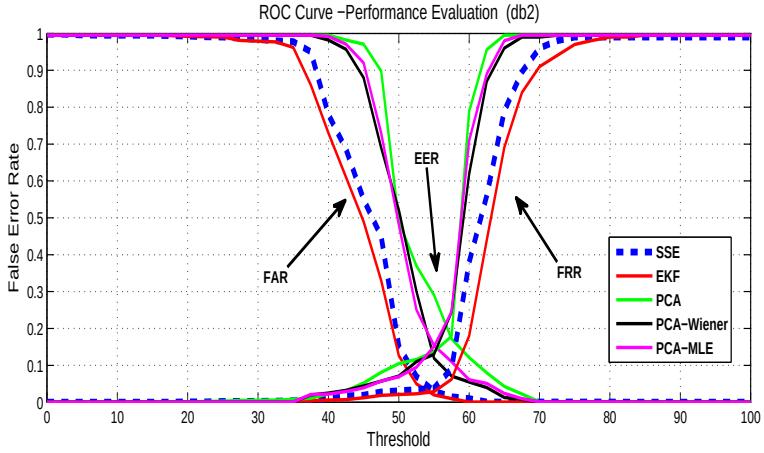


(c) ROC -Zoom (dB1)

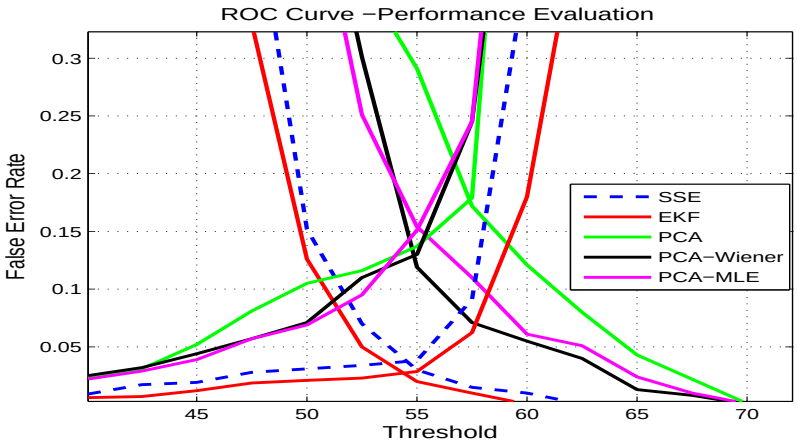
Figure 3.13: Verification - Performance Evaluation



(a) FAR and FRR -dB2

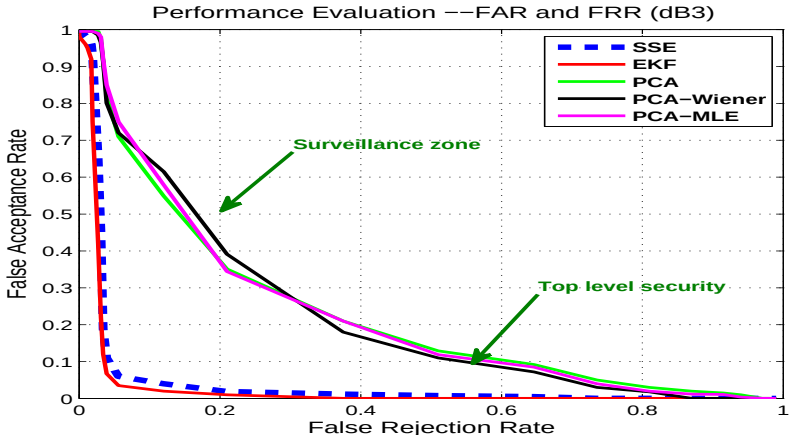


(b) ROC -dB2

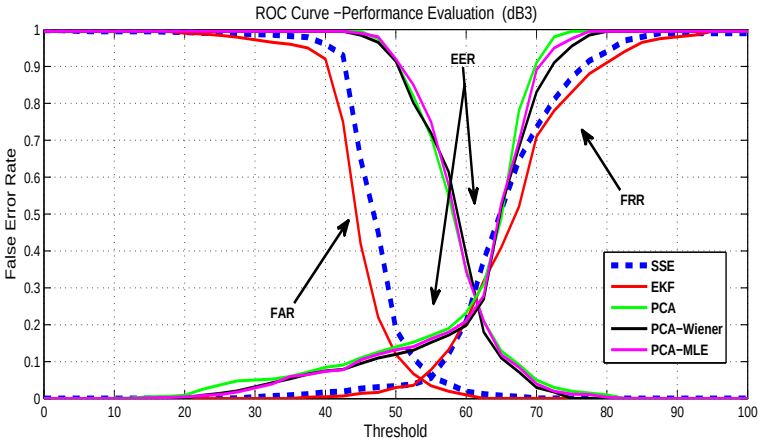


(c) ROC -Zoom (dB2)

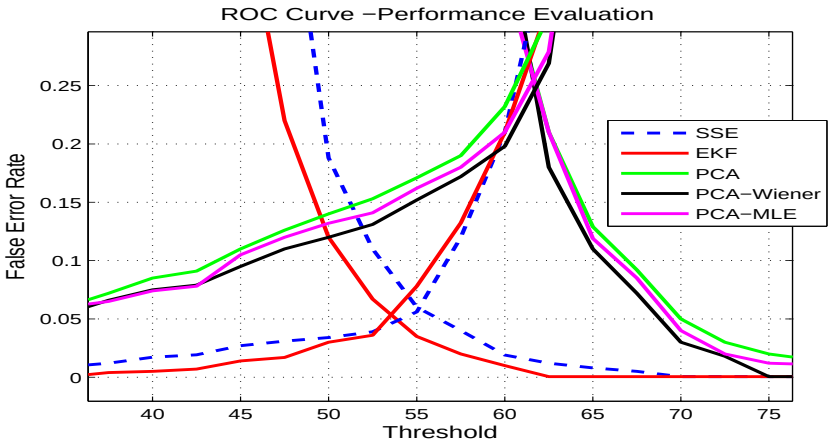
Figure 3.14: Verification - Performance Evaluation



(a) FAR and FRR-dB3

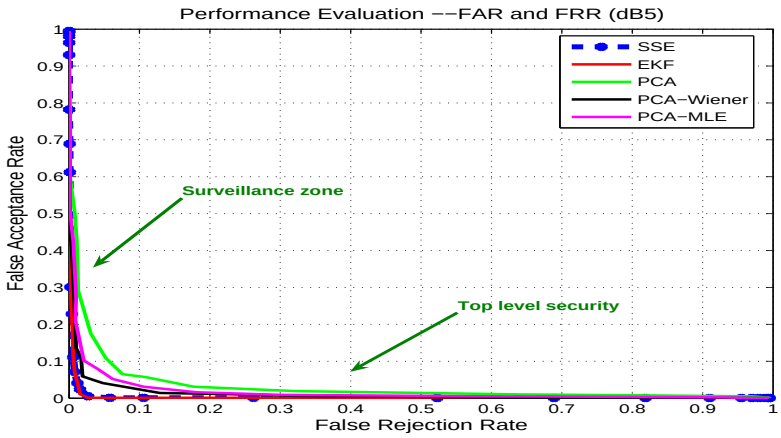


(b) ROC -dB3

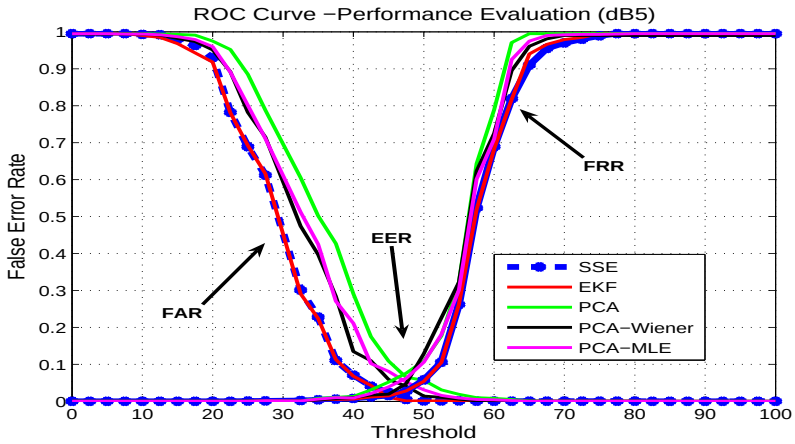


(c) ROC -Zoom (dB3)

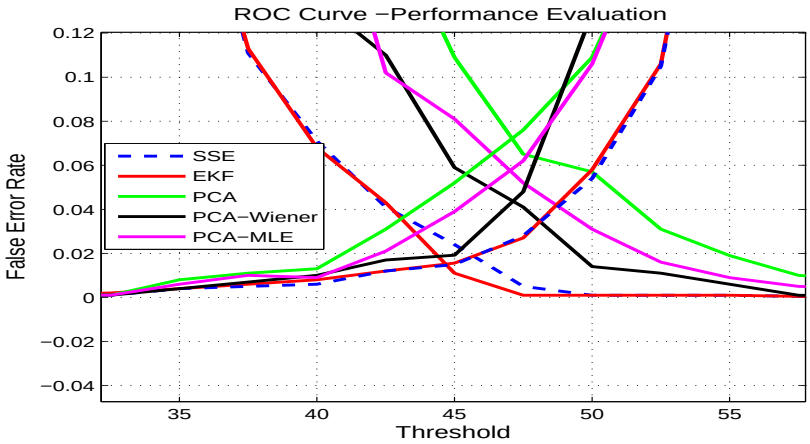
Figure 3.15: Verification - Performance Evaluation



(a) FAR and FRR -dB5



(b) ROC -dB5



(c) ROC -Zoom (dB5)

Figure 3.16: Verification - Performance Evaluation (With Less Hetero-Nonlinear Dataset)

Table 3.5: *Performance Evaluation in (%) - EER Comparison (Put Face Database)*

Methods	$dB1$	$dB2$	$dB3$	*Average*
Proposed SSE	1.87	3.32	6.11	3.76
EKF	1.81	3.15	5.14	3.37
PCA	10.82	17.75	27.85	18.80
PCA-Wiener	7.22	12.86	24.79	14.96
PCA-MLE	8.79	14.65	25.71	16.38

measurements for the acceptability of biometric authentication system implementation. The execution time to complete a total authentication transaction plays the most vital role in biometric systems within an acceptable authentication accuracy range (based on the required security level, preferably within 90%). This is because biometrics always deals with a large scale database in which huge numbers of transactions are performed. Each transaction involves data manipulation, searching, retrieval, and data transferring operations within the large system. A lower execution time is highly desirable; otherwise, the execution time can cause the system to be inappropriate for real time applications, even with a higher authentication accuracy. The data obtained from this experiment is included in $Appendix-C$. The parameters used in this experiment are discussed in Section 3.3.5 and listed in Table 3.1.

First, the performance of the authentication process for the proposed SSE method has been evaluated using EER and CRR rates, and compared with four state-of-the-art methods: PCA, PCA-Wiener, PCA-MLE, and EKF. It is apparent from the experimental results that the SSE method outperformed its counterparts, the PCA, PCA-Wiener, and PCA-MLE algorithms, and was very close to the EKF algorithm.

Table 3.6: *Performance Evaluation in (%) - FAR, FRR and EER Comparison (Indian Face Database -dB5)*

Methods	FAR	FRR	EER
Proposed SSE	1.24	1.56	1.76
EKF	1.25	1.49	1.73
PCA	6.86	8.75	8.15
PCA-Wiener	4.56	5.32	4.80
PCA-MLE	5.30	6.45	5.65

Table 3.7: *Databases Used for This Experiment*

Databases	Original Image Size (Pixels)	Modified
Put Face	2048x1536 (gray)	256x256 (gray)
Indian Face	640x480 (gray)	256x256 (gray)

Secondly, we evaluated and compared the execution time of the SSE method with PCA, PCA-Wiener, PCA-MLE, and EKF. We recorded the execution times of the identification and verification processes for each of the methods in Tables 3.8 and 3.9, respectively. The simulation results are presented in Fig. 3.17. It is apparent from the experimental results that the execution time of the proposed SSE method is 2.0 times lower than the EKF method and is very close to the PCA, PCA-Wiener, and PCA-MLE algorithms. Therefore, the performance and efficiency (execution time) of the SSE method is outstanding compared to its counterparts PCA, PCA-Wiener, and PCA-LME with a slightly higher execution time, as well as its counterpart EKF with very adjustable EER and CRR rates.

Table 3.8: *Average Execution Time in Seconds -Identification*

Authentication	$dB1$	$dB2$	$dB3$	$dB4$	$dB5$
Proposed SSE	44.30	70.16	81.24	18.75	23.68
EKF	89.07	156.45	194.78	59.21	72.34
PCA	42.59	68.27	79.19	18.63	23.49
PCA-Wiener	43.58	69.31	80.20	18.68	23.56
PCA-MLE	43.66	69.42	80.33	18.65	23.54

Furthermore, the performance of the authentication process of the SSE method using three segmented datasets in the image subspace SSE-64×64 (i.e. L/2), SSE-32×32 (i.e. L), and SSE-16×16 (i.e. L×2) (discussed in Section 3.3.1) have been presented in Figs 3.18-3.20. We also recorded the data of EER and CRR in Table 3.10 and Table 3.11, respectively. It is evident from the experimental results that the performance of the SSE method using SSE-32×32 is outstanding in comparison to the SSE method using 16×16, and is close to the SSE method using 64×64 datasets in the image subspace. We also evaluated and compared the execution time of the SSE method in the image subspace using the three segmented datasets discussed above. The simulation results are presented in Fig. 3.21, and experimental data is recorded in Table 3.12 and Table 3.13. It is apparent from the experimental results that the execution time of SSE using SSE-32×32 subspace datasets is outstanding compared to SSE-64×64, and is very close to SSE-16×16.

In this experiment, facial images from two different sets of public databases, the "Put Face Database" with highly nonlinear and heterogeneous noise and the "Indian Face Database" with less nonlinear and less heterogeneous noise, have been used.

Table 3.9: *Average Execution Time in Seconds -Verification*

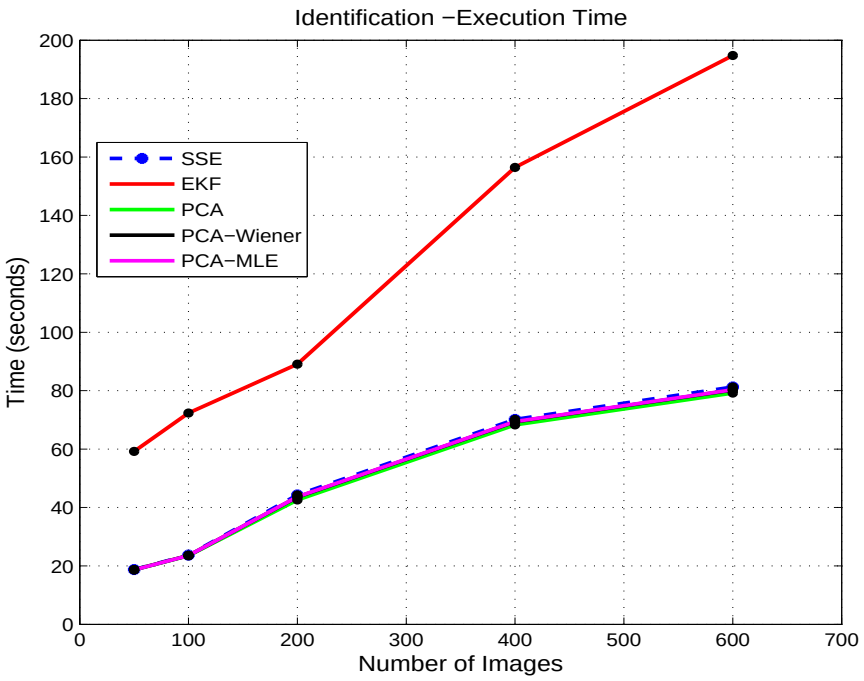
Authentication	$dB1$	$dB2$	$dB3$	$dB4$	$dB5$
Proposed SSE	7.07	8.45	9.38	3.25	4.10
EKF	15.67	17.91	21.53	7.95	10.13
PCA	6.79	7.92	8.81	3.08	3.88
PCA-Wiener	6.92	8.22	9.06	3.17	4.01
PCA-MLE	6.94	8.23	9.10	3.16	3.99

The main objective when using two different sets of databases is to show that the proposed method is not only the optimal solution for the nonlinear, nonstationary, and heterogeneous environment, but is also the optimal solution for the nearly linear and nearly homogeneous environment. In this experiment, it has also been shown that the proposed SSE method is the promising alternative to the widely used optimal PCA method for the linear and homogeneous system.

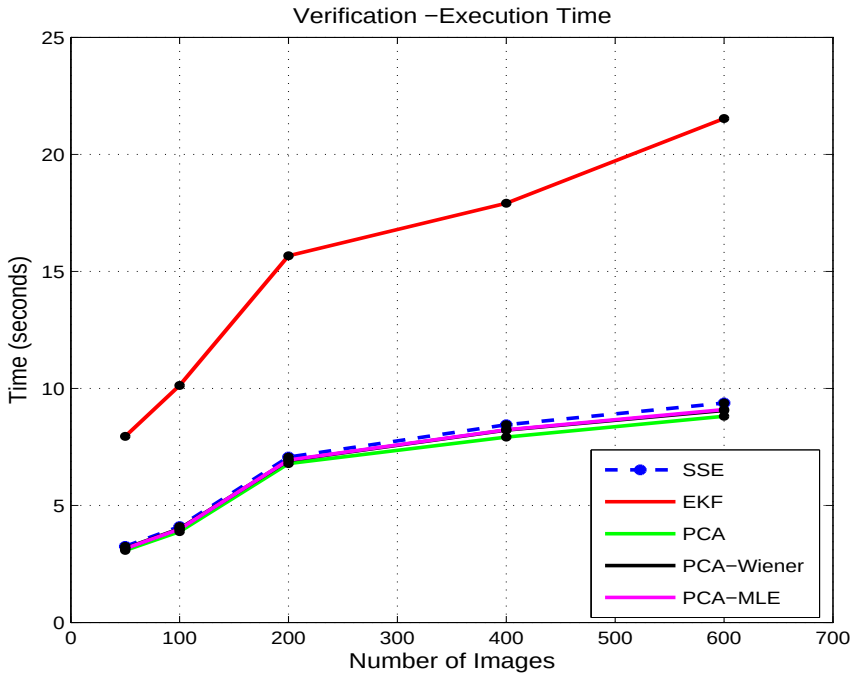
In summary, according to the experimental outcome and comparisons presented above and considering both the authentication performance and efficiency (execution time), the SSE subspace using 32×32 segmented datasets (i.e. SSE-32 × 32) in the image subspace is the optimal solution to ensure the quality of the biometric features while maintaining the outstanding performance and efficiency of the biometric authentication method.

3.4.4 Discussions

The experiment of the proposed system was conducted based on the combined effects of nonlinear, nonstationary, and heterogeneous noise on the extracted biometrics from

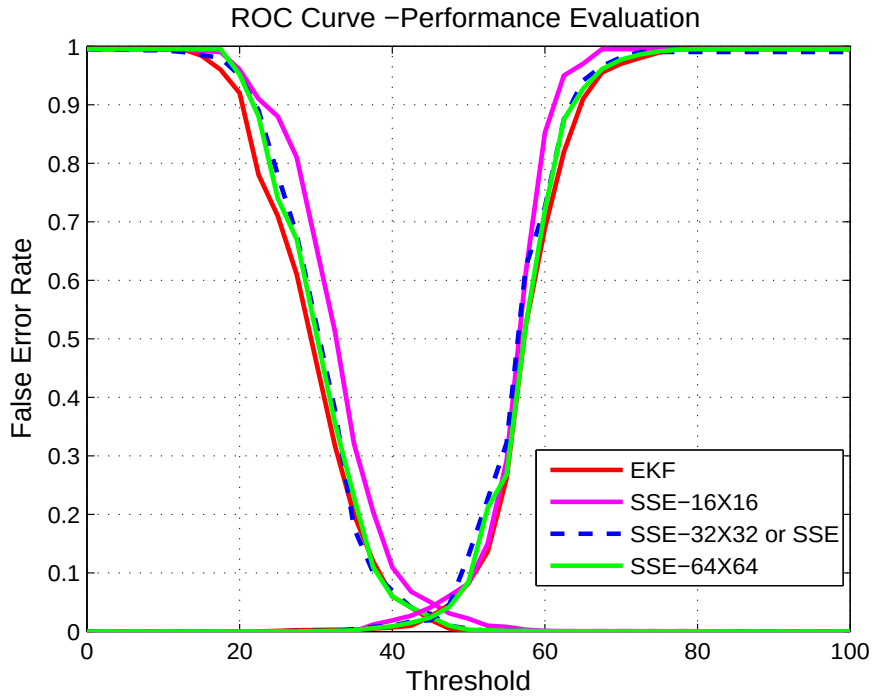


(a) Identification

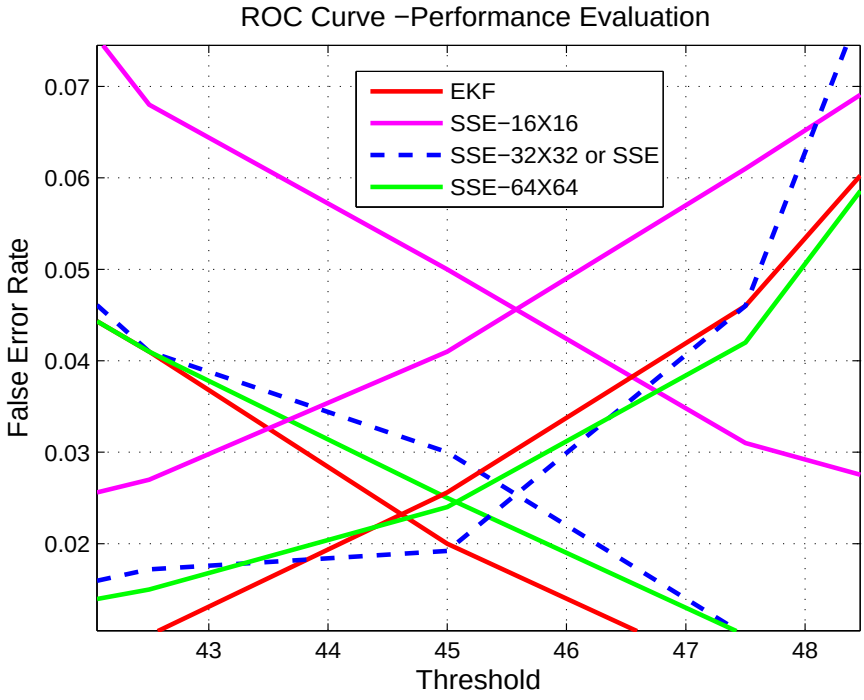


(b) Verification

Figure 3.17: Efficiency Evaluation -Execution Time

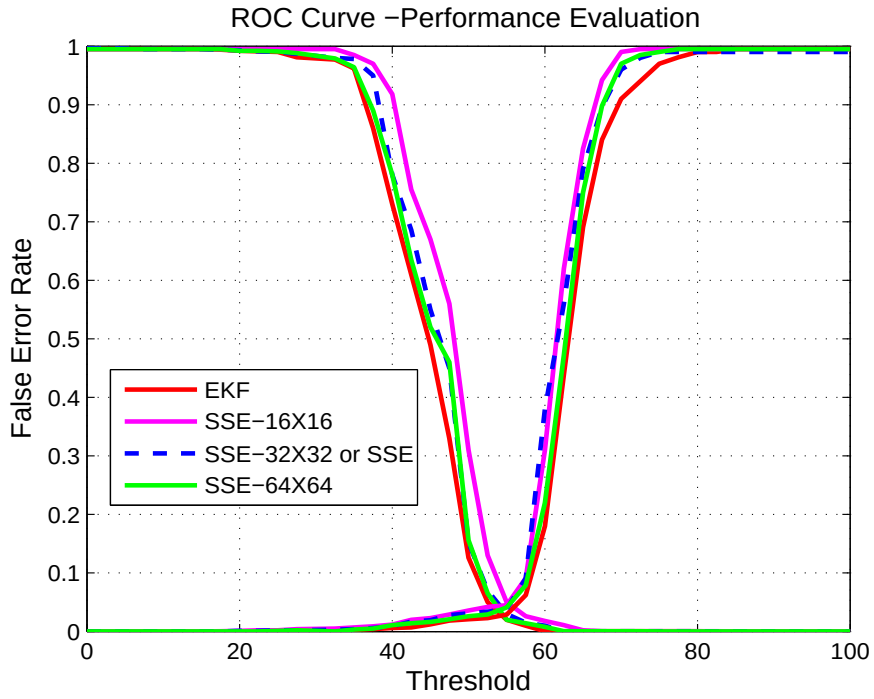


(a) ROC -dB1

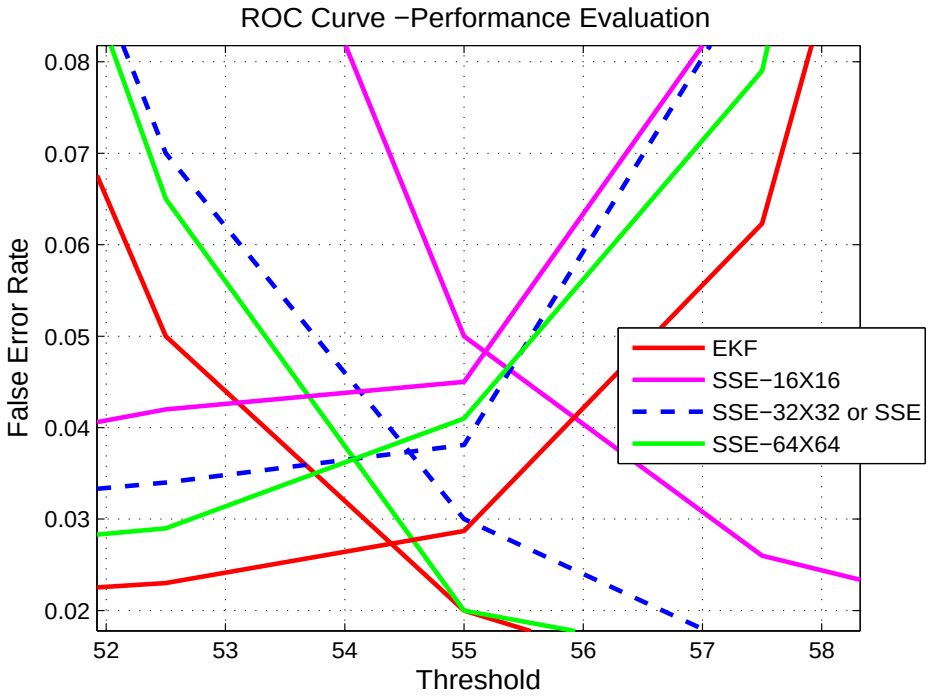


(b) ROC (Zoom) -dB1

Figure 3.18: Performance Evaluation -Verification

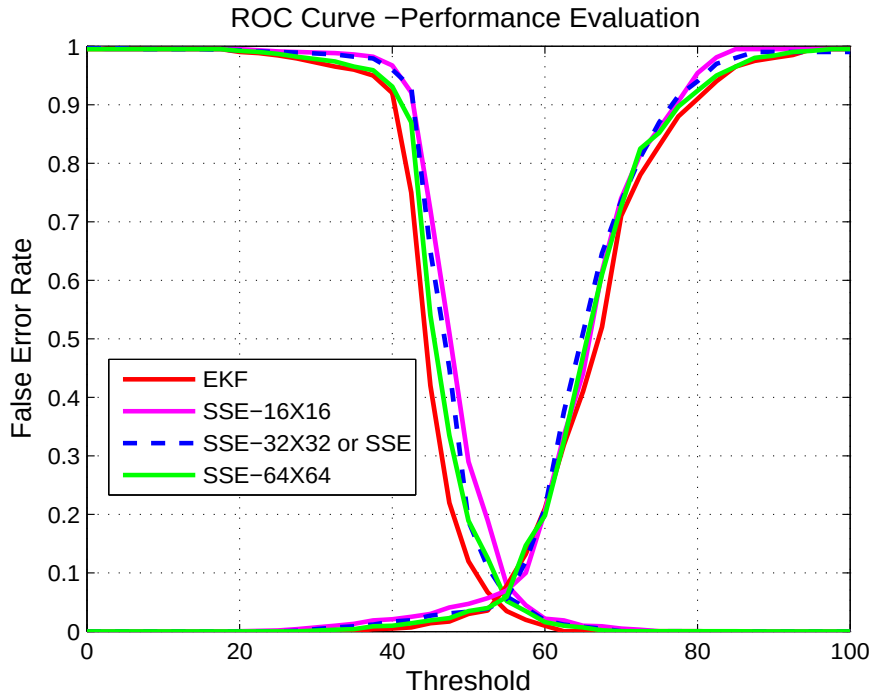


(a) ROC -dB2

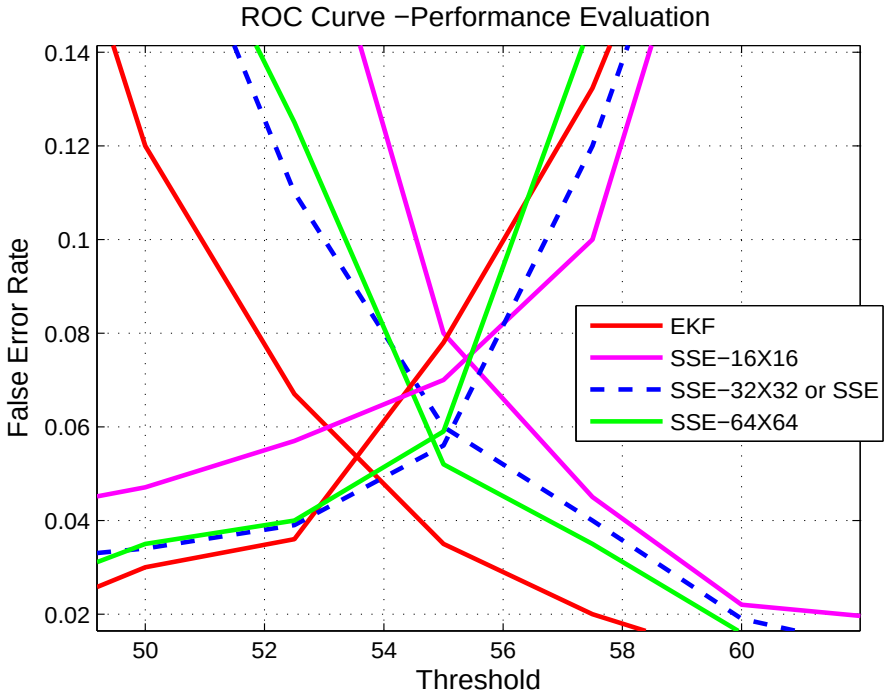


(b) ROC (Zoom) -dB2

Figure 3.19: Performance Evaluation -Verification

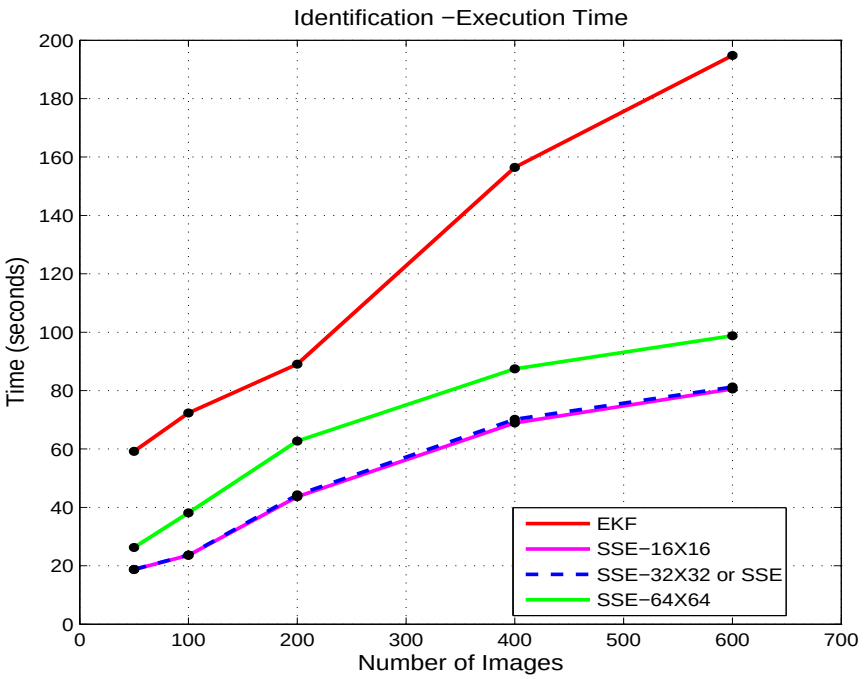


(a) ROC -dB3

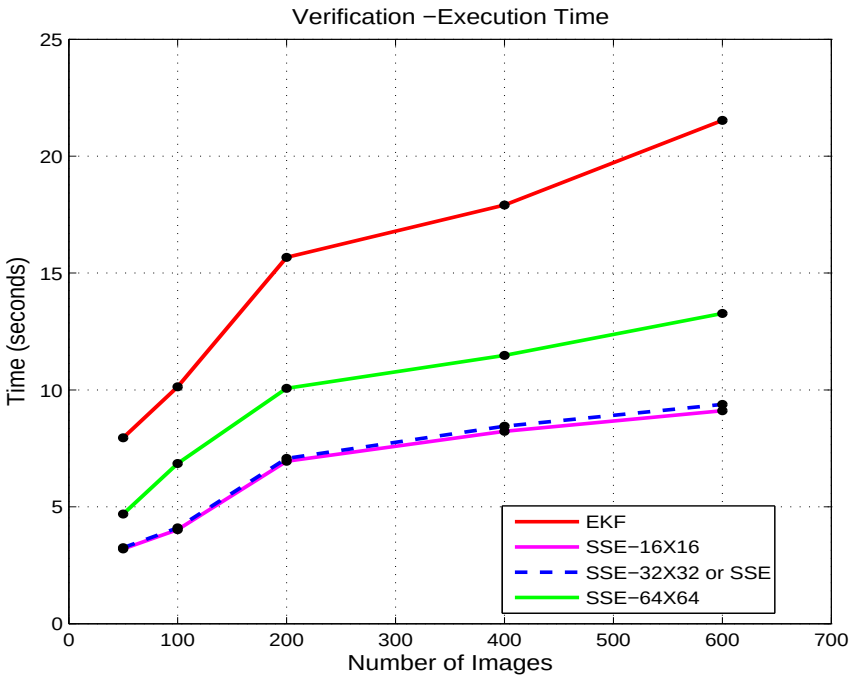


(b) ROC (Zoom) -dB3

Figure 3.20: Performance Evaluation -Verification



(a) Identification



(b) Verification

Figure 3.21: Efficiency Evaluation -Execution Time

Table 3.10: *Performance Evaluation in (%) - EER Comparison*

Methods	$dB1$	$dB2$	$dB3$	*Average*
EKF	1.81	3.15	5.14	3.37
SSE -16x16	3.16	4.39	7.85	5.13
SSE -32x32 or SSE	1.87	3.32	6.11	3.76
SSE -64x64	1.85	3.24	5.79	3.62

Table 3.11: *Performance Evaluation in (%) - CRR Comparison*

Methods	$dB1$	$dB2$	$dB3$	*Average*
EKF	96.57	95.25	92.25	94.69
SSE -16x16	91.25	88.59	83.61	87.82
SSE -32x32 or SSE	96.49	94.35	89.67	93.50
SSE -64x64	96.52	94.81	90.38	93.89

the public database "Put Face Database". According to the simulation outcomes shown in Fig. 3.12(a) and Figs. 3.13-3.15, the proposed sequential subspace approach achieves the best authentication accuracy. The parameters used for this experiment are discussed in Section 3.3.5 and listed in Table 3.1. The data obtained from this experiment is included in $Appendix - C$.

In the experiment, three different databases $dB1$, $dB2$, and $dB3$ containing 20, 40, and 60 subjects, each with 10 images, were used. The identification performance was analyzed based on the CRR. The efficiency versus databases (no. of samples) graph is shown in Fig. 3.12(a). The average execution time of the identification process for

Table 3.12: *Average Execution Time in Seconds -Identification*

Authentication	$dB1$	$dB2$	$dB3$	$dB4$	$dB5$
EKF	89.07	156.45	194.78	59.21	72.34
SSE -16x16	43.89	69.48	80.55	18.70	23.61
SSE -32x32 or SSE	44.30	70.16	81.24	18.75	23.68
SSE -64x64	62.53	87.45	98.78	26.27	38.14

Table 3.13: *Average Execution Time in Seconds -Verification*

Authentication	$dB1$	$dB2$	$dB3$	$dB4$	$dB5$
EKF	15.67	17.91	21.53	7.95	10.13
SSE -16x16	6.98	8.31	9.15	3.22	4.05
SSE -32x32 or SSE	7.07	8.45	9.38	3.25	4.10
SSE -64x64	10.15	11.42	13.27	4.69	6.85

$dB3$ using MatLab 2008 and Microsoft Access on a i5-2.4GHz CPU with 8 GB RAM was 81.24 sec, which is almost 2.5 times lower than the EKF. The average execution times for each database and method are presented in Table 3.8, Table 3.9, Table 3.12, and Table 3.13. The results displayed in Table 3.2 and Fig. 3.12(a) show that the proposed subspace method (identification) outperforms its counterparts PCA, PCA-Wiener, and PCA-MLE estimator, and is very close to the EKF.

As well, experimental results of the verification process were recorded and presented in Table 3.4, Table 3.5, Table 3.10, Figs. 13-15, and Figs. 18-20. The receiver operating curves (ROC) of the proposed method, based on the three databases $dB1$,

$dB2$, and $dB3$, are presented in Figs. 3.13-3.15 and Figs. 18-20. These ROC curves measure the performance of the verification system, and are plotted as a function of threshold values. FAR and FRR presented in the ROC curve characterize the verification accuracy, and the point EER represents the performance of the verification system. The average execution time for the verification process using $dB3$ was 9.38 sec, which is almost 2.5 times lower than the EKF. More importantly, the performance of the proposed method was analyzed and compared with four state-of-the-art algorithms, namely: EKF, PCA, PCA-Wiener, and PCA-MLE. Experimental results show that the proposed SSE method outperforms the PCA, PCA-Wiener, and PCA-MLE algorithms, and is very close to the EKF algorithm with a promising EER of 1.87% and an average EER of 3.76%.

Furthermore, the experiment of the proposed model was also conducted using less hetero-nonlinear images from the public database "Indian Face Database". In the experiment, the two different databases $dB4$ and $dB5$, containing 10 and 20 subjects with 5 images each, were used. According to the simulation outcomes shown in Fig. 12(b) and Fig. 3.16, the proposed sequential subspace approach achieves the best authentication (verification and identification) accuracy. The experimental results of the identification and verification were recorded and presented in Table 3.3 and Table 3.6, respectively. It is also apparent from the outcomes of the experiment that the proposed SSE method outperforms its counterparts, the PCA, PCA-Wiener, and PCA-MLE methods, and is very close to EKF. However, significant improvement in the performance of the PCA, PCA-Wiener, and PCA-MLE algorithms was observed.

In this study, three subspace datasets–16×16, 32×32, and 64×64–have also been used to evaluate, analyze, and compare the performance and efficiency of the SSE proposed method. However, other forms of segmented datasets can also be used in this experimental evaluation and analysis. The experimental outcomes for the authentication and efficiency (execution time) have been presented in Figs. 3.18-3.21,

and their data has also been recorded in Tables 3.10-3.13. Considering the results of both the authentication performance and the execution time, it is apparent from the experimental results that the proposed SSE method using 32×32 segmented datasets has shown outstanding performance and efficiency in comparison to the segmented datasets 16×16 and 64×64.

The execution times of the identification and verification for each method have been estimated and recorded in Table 3.8, Table 3.9, Table 3.12, and Table 3.13. Simulation results of these execution times have also been presented in Fig. 3.17 and Fig. 3.21. It is apparent that the efficiency of the proposed method is outstanding in comparison to EKF and is very close to the PCA, PCA-Wiener, and PCA-MLE methods.

The slight deviation in performance of the proposed SSE from EKF and the slight deviation of efficiency (execution time) from PCA, PCA-Wiener and PCA-MLE are due to the use of the subspace technique. In the proposed SSE method, the features segmentation, estimation, and reconstruction processes have been performed in the image subspace. According to the results, these deviations are negligible for small sized databases and are within the acceptable range for large databases. In this experiment, we also found that the performance of the proposed SSE method is outstanding compared to the optimal PCA algorithm in a linear and homogeneous environment (i.e. "Indian Face Database"). The subspace technique allows the system to simplify the dimensional complexity, and it was found that the efficiency (i.e. lower execution time) of the proposed method was almost 2.5 times higher than the EKF method.

3.5 Conclusions

The properties of biometrics are always dynamic in nature. There are many situations where the quantities and properties of useful information in the extracted biometric features are not fixed during processing. This dynamic data structure also leads to the fact that the characteristics of the extracted features are highly influenced by the surrounding environment and are a function of time. The efficiency and accuracy of biometric authentication systems are also dependent on the quality of the extracted features, their consistency, and their mutual relationship. In this situation, linear, stationary, and homogeneous assumptions are insufficient to produce good results. Typically, LDA, MLE, Bayesian, LMS, and Wiener are inadequate methods to cater to the nonlinear, nonstationary, and heterogeneous noise environment. The integration of PCA with these methods allows the biometric authentication system to overcome the challenges associated with nonlinear and heterogeneous noise. Another promising alternative, the sequential estimator, also has the capability of adapting to the diverse nature of noise; however it is computationally inefficient, as it needs to perform extensive matrix operations.

In this chapter, a new recursive sequential subspace method is being developed. The proposed method addresses the challenges of the extracted biometrics due to nonlinear, nonstationary, and heterogeneous noise (i.e. noise covariance matrix). It also overcomes the computational burden associated with sequential estimation. This is a recursive method, so the extracted data and its associated noise update in every iteration using the biometric features (dataset) from the immediate past state. SSE design is based on the minimization of noise and maximization of information content in the received data, in MSE sense. Thus, the method would be able to make a close approximation of the desired data model, which would otherwise be contaminated by nonlinear, nonstationary, and heterogeneous noise. After mitigation

of the noise level, the dataset is normalized in the image subspace; then the normalized datasets concatenate to reconstruct the biometric template. This method is being tested on facial images from two public databases: the hetero-nonlinear "Put Face Database" and the less hetero-nonlinear "Indian Face Database". In this study, the experiment of the proposed method has also been performed in the image subspace using three segmented datasets. Considering both the performance (authentication) and the efficiency (execution time), it is apparent that the SSE-32 $\times$ 32 method demonstrates superiority in comparison to the SSE-16 $\times$ 16 and SSE-64 $\times$ 64 methods.

Finally, the performance and efficiency of the identification process is analyzed and compared using the percentage of the Correct Recognition Rate (CRR). The performance and efficiency of the verification process is also analyzed and compared using the percentage of the Equal Error Rate (EER). More importantly, the performance and efficiency of the proposed model is compared to the four state-of-the-art algorithms, namely: EKF, PCA, PCA-MLE, and PCA-Wiener. It is found that the performance and efficiency of the proposed method outperforms its counterparts.

Chapter 4

MultiBiometrics Encryption and its Management System

4.1 Introduction

Biometrics is a rapidly growing branch of information technology that automatically authenticates an individual based on two basic properties of human biometric features: distinctiveness and permanence. The effectiveness and strength of the biometric authentication and cryptography (or encryption) systems are dependent on the extent to which they can hold these two properties. As a result, fingerprint, face, iris, hand geometry, and gait have been used as primary biometric traits, since soft or auxiliary biometric characteristics including age, weight, height, and race lack distinctiveness and permanence [104-113].

A limited number of biometric traits possess sensitive human information that is also unique and cannot be revoked or reissued once compromised. Furthermore, the features extracted from the biometric traits are stored in the database during enrollment in order to compare (match) and authenticate the legitimacy of the subject of interest. Typically, this comparison performs in the unencrypted domain, since

the authentication accuracy can be largely influenced by a small variation in the feature properties if it takes place in the encrypted domain. More importantly, after biometric data acquisition, the method of biometric data manipulation and representation techniques is almost the same as any other traditional data management system. Therefore, concerns about the security and privacy of biometric features (templates), and their data management architecture are of paramount importance in the exploration of biometric systems. Ideally, the security and privacy of the template is accomplished based on mathematical algorithms which must be difficult to decrypt by the unintended recipients. In addition, a template protection algorithm should be irreversible, robust, and revokable [112-114].

In this chapter, a novel MultiBiometrics encryption algorithm is proposed that protects the stored and dynamic biometric templates against security, privacy, and unlinkability attacks. Unlike current biometric encryption, the proposed method uses cryptographic keys in conjunction with extracted MultiBiometrics to create cryptographic bonds, called "*BioCryptoBond*". Importantly, to further enhance the security and privacy protection during the comparison process and to improve authentication accuracy, a multilayered Biometrics Data Management System (BDMS) is also proposed. The theoretical foundation of the proposed method along with the model evaluation and experimental results have also been presented in this chapter. The performance of the method is being analyzed based on the FAR, FRR, EER, and CRR.

In the method proposed in this chapter, the cryptographic system is designed to deal with two categories of people: user and subject. In this case, user and subject biometric templates are considered to be stored in the local and central databases, respectively. Multiple 32-bit digital cryptographic keys are generated and securely bond with the MultiBiometrics (i.e. face and fingerprint) features, creating cryptographic data blocks known as *BioCryptoBond*s. Neither the biometric features nor

the secret keys can be retrieved from these *BioCryptoBond*s without a successful user authentication in the presence of the subject. In this case, the facial area; facial biometrics such as the size and the relative positions of the eyes and lips; and fingerprint biometrics features such as ridge patterns, minutiae points, and code points, are considered for biometric template generation. The motivation for the proposed MultiBiometrics encryption method is the protection of stored and dynamic biometric information from security, privacy, and unlinkability attacks, using multilayered encryption and its management system. The method will also address the diversity, revocability, and performance of the system. In this cryptographic model, successful user authentication in the presence of the subject will be required in order to access subject databases.

The remainder of the chapter is organized as follows. Section 4.2 studies the features extraction process and its associated challenges. The detailed analysis and algorithmic formulation of the proposed biometric encryption, enrollment, and authentication systems are presented in Section 4.3. Section 4.4 presents the Biometrics Data Management System (BDMS). Section 4.5 studies the performance evaluation of the proposed method. Experimental results and discussions are given in Section 4.6. Finally, the conclusions are presented in Section 4.7.

4.2 Filter Design

Biometrics, especially fingerprint and facial features, are always contaminated by noise; including misalignments, position orientation, illumination, and environmental noise. Thus, there are some dissimilarities between the received biometric features and the desired one [5],[115]. In this section, a mathematical formulation of the proposed filtering or estimation method for minimizing these dissimilarities has been

discussed. The main objective is to extract quality biometric features for the biometric enrollment and authentication process. More importantly, this method would optimize to produce consistent output from biometric features, tolerate position orientation and illumination effects on facial biometric features as well as misalignment effects on fingerprint features, and produce a lower Equal Error Rate (EER).

Now, consider that the facial or fingerprint images (dataset) have been received as vectors of matrix –$\mathbf{x}$. Each row and column of the received dataset –$\mathbf{x}$ represents an observation and a particular type of datum, respectively. If the received dataset is contaminated by noise, then the received images can be written as:

$$\mathbf{x} = \mathbf{s} + \mathbf{n} \tag{4.1}$$

where $\mathbf{n}$ is the noise matrix, and $\mathbf{s}$ is the noise-free or desired dataset.

Principal components can be derived from the $\mathbf{x}$ dataset, and these derived components can be written as [93]:

$$\mathbf{z} = \mathbf{w}^T\mathbf{x}$$

Therefore using Eq. (4.1):

$$\mathbf{z} = \mathbf{w}^T\mathbf{s} + \mathbf{w}^T\mathbf{n} \tag{4.2}$$

where $\mathbf{w}$ represents weight vectors which map to each row vector of x, z is considered to be inherited (data) with maximum possible variance from the x dataset, and each of the weight vectors $\mathbf{w}$ is constrained to be a unit vector [91],[93].

So, the main objective is to minimize the noise $\mathbf{n}$ and estimate the image of interest. In addition, the features of interest are extracted in order to create and compare biometric templates. The Sequential Subspace Estimator (SSE) has been used to minimize the dissimilarities between the received images and the desired one

[91],[93],[100]. Furthermore, the SSE method has also been used to extract and compare the biometric templates in order to authenticate the legitimacy of an individual. In this case, noise associated with the extracted features is considered to be non-stationary, nonlinear, and heterogeneous due to misalignments, position orientation, illumination, background, and environmental noise. The detailed analysis, algorithmic formulation, and operational principle of the Sequential State Estimator method have already been discussed in Chapter 3.

4.3 MultiBiometrics Encryption and Enrollment

The biometric templates created from the images received at the output of the filter studied in Section 4.2 are the desired templates. These templates will be stored (enrollment) in the databases for the authentication process. The security and confidentiality of the stored and dynamic biometric features are dependent on the protection of the filtered biometrics against security, privacy, and unlinkability attacks. Therefore, the objective of the proposed encryption method is to develop a secure, robust, and reliable encryption algorithm to protect these templates.

Now consider that $h(t)$ represents the filtered biometric templates used in the biometric enrollment and authentication process in the time domain. So, the objective of the encryption method presented in this chapter is to protect the template $-h(t)$ against security, privacy, and unlinkability attacks. In contrast to current biometric encryption systems, the proposed method generates a 32-bit digital secret key and creates a cryptographic data block, *BioCryptoBond*. The secret key, and facial or (and) fingerprint biometric features (i.e. h(t)), are monotonically bonded in order to create this MultiBiometrics cryptographic bond. The goal is to protect the stored or dynamic biometric features and key in such a way that neither the biometric features nor the secret key can be retrieved without a successful authentication process. The

method of creating a MultiBiometrics template using the fusion of facial and fingerprint features is stated below. Afterwards, the detailed analysis and formulation of the Encryption and enrollment method are discussed.

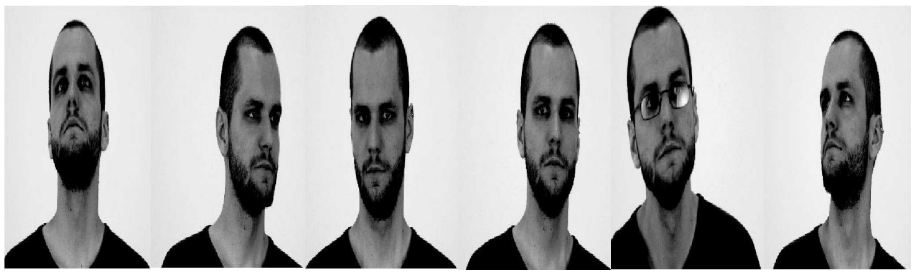
4.3.1 MultiBiometrics Template

In this experiment, fingerprint and facial biometrics have been used to create Multi-Biometric templates. The facial images from the public "Put Face Database" and "Indian Face Database" have been extracted and fused with fingerprint images taken from the public "CASIA Fingerprint Version 5" database. These three databases contain images of different individuals. There is no relationship between individuals in the fingerprint database and those in the facial database; individuals in one database are not in the other. Therefore, for the formation of each MultiBiometrics template, a set of fingerprint images from a particular individual in the fingerprint database has been assigned to a particular individual from the facial database. A set of facial images of an individual and the corresponding assigned set of fingerprint images are shown in Fig. 4.1.

A detailed analysis, complete algorithmic formulation, implementation of the proposed cryptographic bond *BioCryptoBond*, and the enrollment method have been studied in the following subsections.

4.3.2 BioCryptoBond

The cryptographic architecture of this method is being designed to deal with two categories of people: the authorized user and the subject (target). The user cryptographic bond, $BioCryptoBond_u$, is being created based on user fingerprint biometrics (i.e. minutiae points, code point, and orientation angle (Fig. 4.3)) in conjunction with the digital secret key. Conversely, three subject cryptographic bonds–$BioCryptoBond_F$,



(a) PUT Face Database

(b) CASIA Fingerprint Version 5.o

Figure 4.1: A Set of MultiBiometrics Template

$BioCryptoBond_{FP}$, and $BioCryptoBond_{FF}$–are being created using facial, fingerprint, and the fusion of facial and fingerprint biometrics, respectively. The three subject cryptographic bonds are being created here with the objective of providing multilayered security protection for the subject's biometric features. The detailed analysis, implementation, and execution of this multilayered security protection system is presented in Chapter 5. A detailed system diagram and processing method for generating user and subject *BioCryptoBond* bonds based on facial, fingerprint, and the fusion of facial and fingerprint (i.e. MultiBiometrics) biometrics is presented in Fig. 4.2.

Furthermore, in the proposed method, tensor and orthogonal operations are implemented on biometric features and digital secret keys at different stages. The algorithmic architecture and formulation for creating four cryptographic bonds have been stated below.

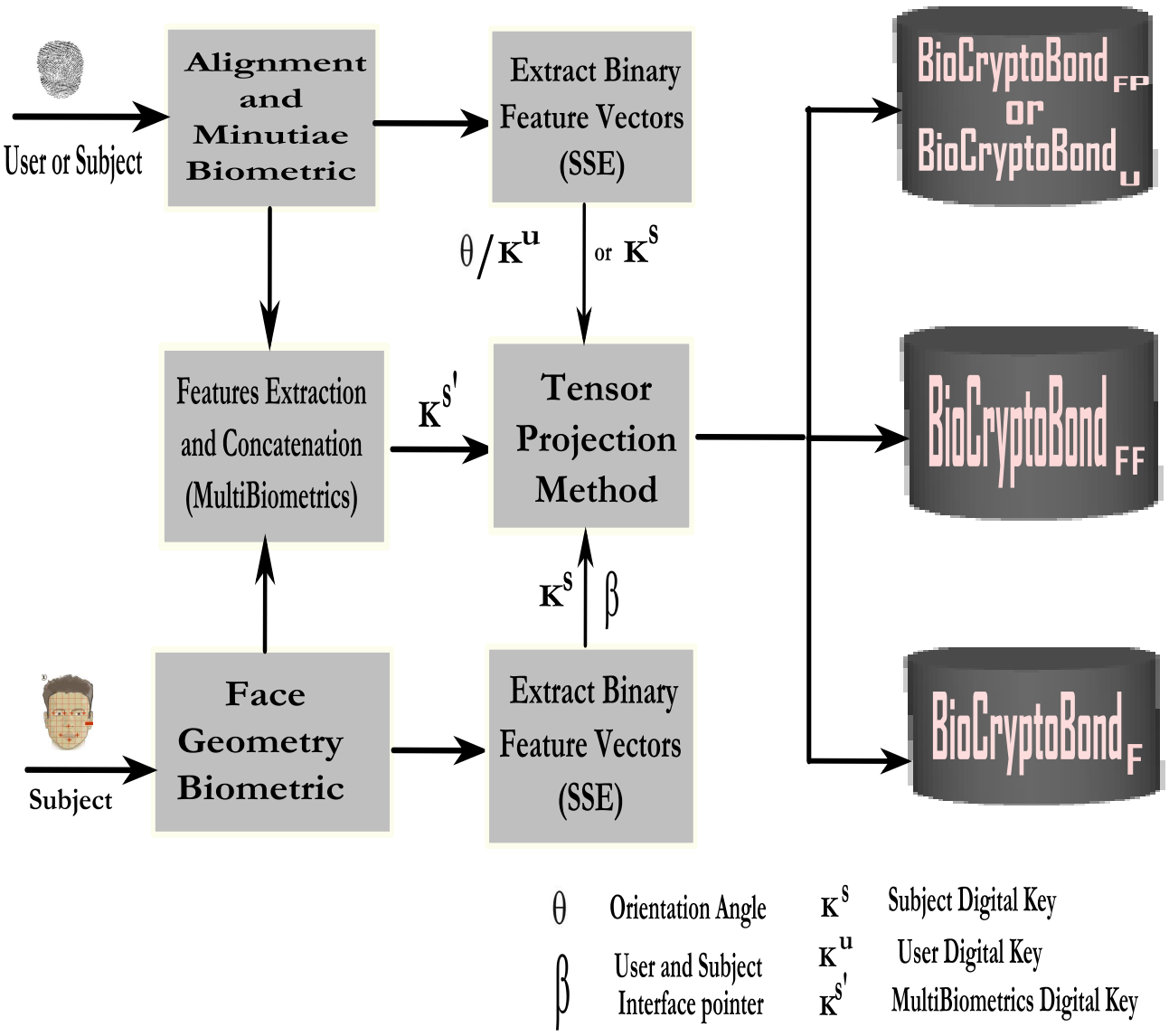


Figure 4.2: System Architecture -BioCryptoBond

4.3.2.1 $BioCryptoBond_u$

The steps involved in creating the user cryptographic bond $BioCryptoBond_u$, are stated below:

(i) Extract and compute orientation angle (θ) (Fig. 4.3) from received user fingerprint features [7],[8],[108],[110], [115].

(ii) The tensor operation is performed on the user filtered fingerprint biometric template $h(t)$ (minutiae points) as a function of orientation angle.

(iii) Output from the tensor operation is converted into an orthogonal matrix Π.

(iv) A digital random key K^u for the user is generated (Fig. 4.2) and fused with an orthogonal matrix of vectors Π, creating the user cryptographic bond, $BioCryptoBond_u$. This cryptographic bond binding process can be formulated as follows:

$$\begin{aligned} \mathbb{T} &= \theta \times \digamma(s) \\ \Pi &= \mathbb{T}_{or} \\ BioCryptoBond_u &= \Pi \times K^u \end{aligned} \tag{4.3}$$

where $\mathbb{T}$ is the output from the tensor operation; the subscript $_{or}$ is the orthogonal operator; and $\digamma(s)$ is the fourier transform of $h(t)$.

4.3.2.2 $BioCryptoBond_{FP}$

The steps that are involved in creating the subject cryptographic bond $BioCryptoBond_{FP}$ using $h(t)$ fingerprint features (minutiae points (Figs. 4.1 and 4.2)) are stated below.

(i) Randomly generated key K^s is transformed into the orthogonal matrix Π_{fp}.

(ii) Matrix Π_{fp} is fused with the filtered fingerprint output $h(t)$, creating the cryptographic bond $BioCryptoBond_{FP}$.

This bond binding process can be formulated as follows:

$$\begin{aligned} \Pi_{fp} &= K_{or}^{s} \\ BioCryptoBond_{FP} &= \Pi_{fp} \times \digamma(s) \end{aligned} \tag{4.4}$$

4.3.2.3 $BioCryptoBond_F$

The steps that are involved in creating the subject cryptographic bond $BioCryptoBond_F$ using subject facial biometrics (i.e. facial area, size and relative positions of eyes and lips (Figs. 4.2 and 4.4)) are stated below:

(i) An arbitrary interface pointer β is received. This interface pointer is generated by the system upon successful user authentication.

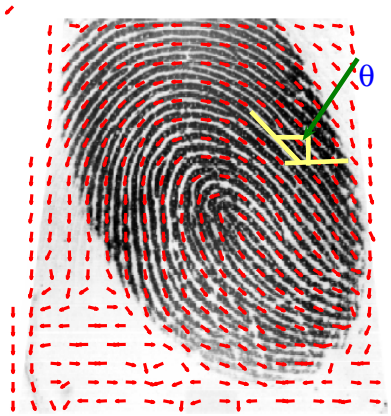
(ii) Tensor operation is performed as a function of β on received filtered facial biometrics $h(t)$.

(iii) Output of tensor operation is converted into the orthogonal matrix Π_f.

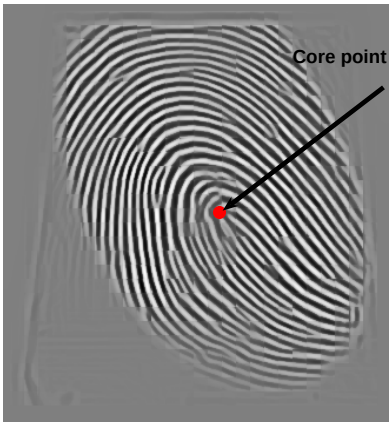
(iv) Matrix Π_f is fused with the same randomly generated digital key K^s used to create the subject's $BioCryptoBond_F$ bond. This bond binding process can be formulated as follows:

$$\begin{aligned} \mathbb{T} &= \beta \times \digamma(s) \\ \Pi_f &= \mathbb{T}_{or} \\ BioCryptoBond_F &= \Pi_f \times K^s \end{aligned} \tag{4.5}$$

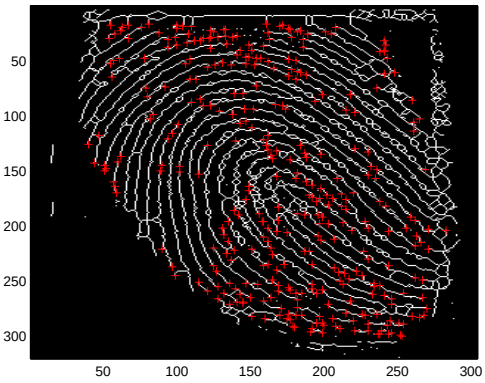
(a) Original Image



(b) Ridge Orientation

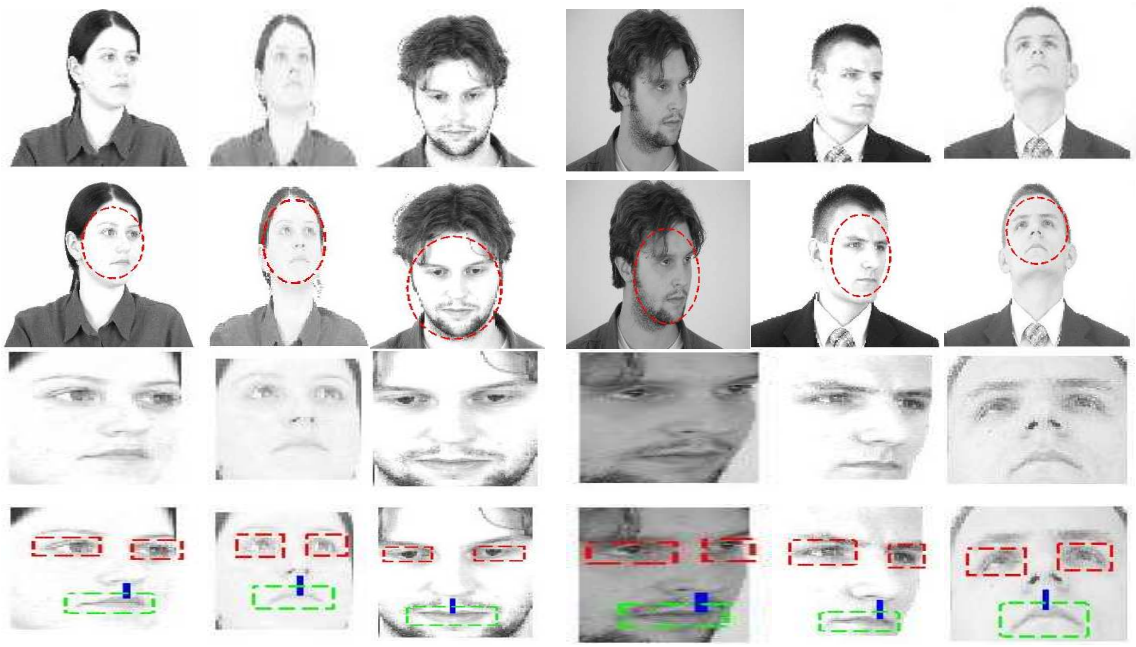


(c) Core Point



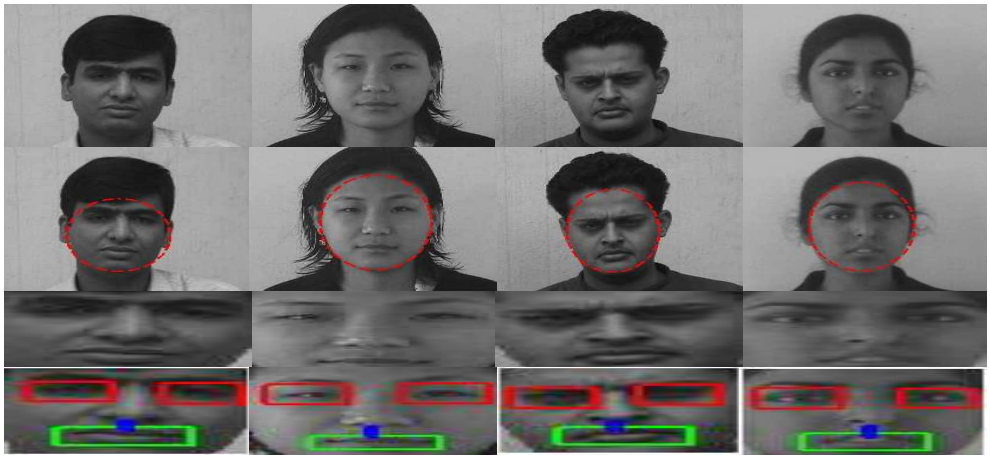
(d) Minutiae Points

Figure 4.3: Fingerprint Biometrics –Features Extraction



(a) Put Face Database

i) First Row -Original Image
ii) Second Row - Computation of Facial Boundaries
iii) Third Row - Extracted Face
iv) Fourth Row - Extracted Features



(b) Indian Face Database

Figure 4.4: Facial Biometrics -Feature Extractions

4.3.2.4 $BioCryptoBond_{FF}$

The steps that are involved in creating the subject cryptographic bond $BioCryptoBond_{FF}$ using MultiBiometrics (the fusion of facial and fingerprint biometrics) are stated below:

(i) Subject filtered fingerprint and facial biometrics are concatenated (or fused), and a MultiBiometrics template is created.

(ii) Concatenated matrix or MultiBiometrics is converted to orthogonal matrix Π_{ff}.

(iii) Orthogonal matrix is fused with a randomly generated digital secret key $K^{s'}$ (Fig. 4.2), and a $BioCryptoBond_{FF}$ bond is created.

This bond binding process can be formulated as follows:

$$\begin{aligned} c(t) &= c[h_1(t) + h_2(t)] \\ \mathbb{C}(s) &= \mathcal{F}(c(t)) \\ \Pi_{ff} &= \mathbb{C}_{or}(s) \\ BioCryptoBond_{FF} &= \Pi_{ff} \times K^{s'} \end{aligned} \tag{4.6}$$

where $h_1(t)$ and $h_2(t)$ represent filtered outputs for fingerprint and facial biometrics, respectively; $c(t)$ represents the concatenate operation; $\mathbb{C}(s)$ represents the fourier transformation of the concatenate operation.

4.3.3 Enrollment

The next stage of the proposed biometric cryptographic method is the enrollment process. The common steps involved during the user and subject enrollment process are stated below:

(i) Digital secret key is fused with $BioCryptoBond$.

(*ii*) Outcome is hashed with primary biometric features and generates 16-bit reference pointer [see $Appendix - B$].

The enrollment process can be formulated as follows:

$$\mathbb{R} \;=\; \mathbb{H}[(BioCryptoBond \;\times \mathbb{S}_k)(\mathbb{I}_p)] \tag{4.7}$$

where $\mathbb{H}$, $\mathbb{R}$, and $\mathbb{I}_p$ are the hash function, reference pointer transformation, and primary biometric features, respectively. $\mathbb{S}_k$ represents the digital key.

4.3.3.1 User

The system architecture of the user enrollment process is depicted in Fig. 4.5 and the steps involved in the user enrollment process are stated below:

(i) User template is processed and verified with the stored template in *User Database* (dB_u) using reference pointers given in Eq. (4.7).

(ii) Upon activation of the positive verification signal (if user not enrolled), reference pointers along with the biometric template and description of the user are stored in respective user databases $Encryption_u$ and *User Database* (dB_u), as shown in Fig. 4.5.

4.3.3.2 Subject or Target

The subject enrollment process includes additional steps, which are executed after generating the reference pointers stated in Eq. (4.7). The main objective of these additional steps is to provide multilayered security protection for subject biometric templates. The system architecture of the subject enrollment process is presented in Fig. 4.6, and additional steps are stated below:

(i) Outputs of reference pointers are hashed and fused with a 32-bit composite foreign key to create a link function termed a Hot-Key function (Φ_{hk}). This function

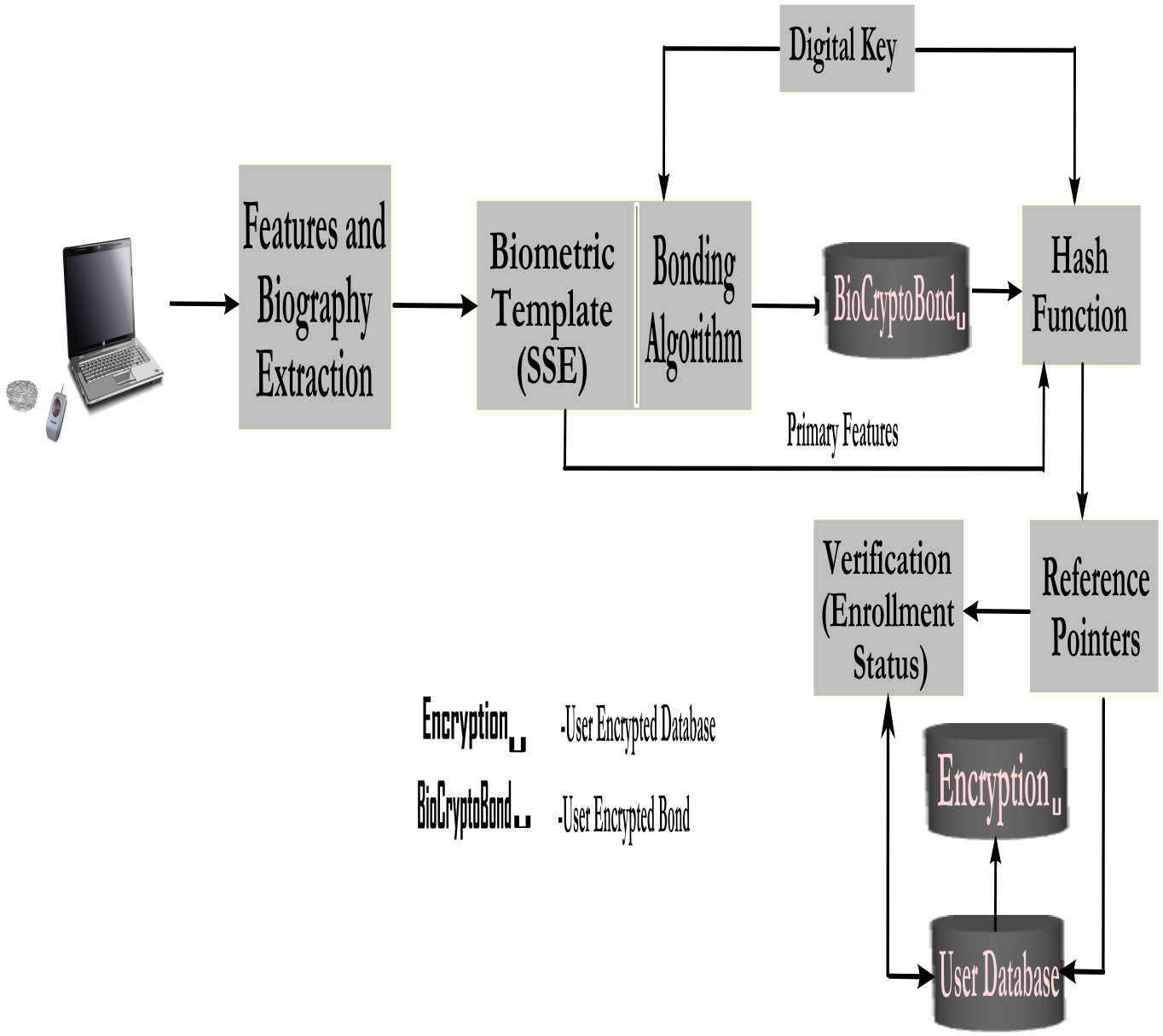


Figure 4.5: User Enrollment Process

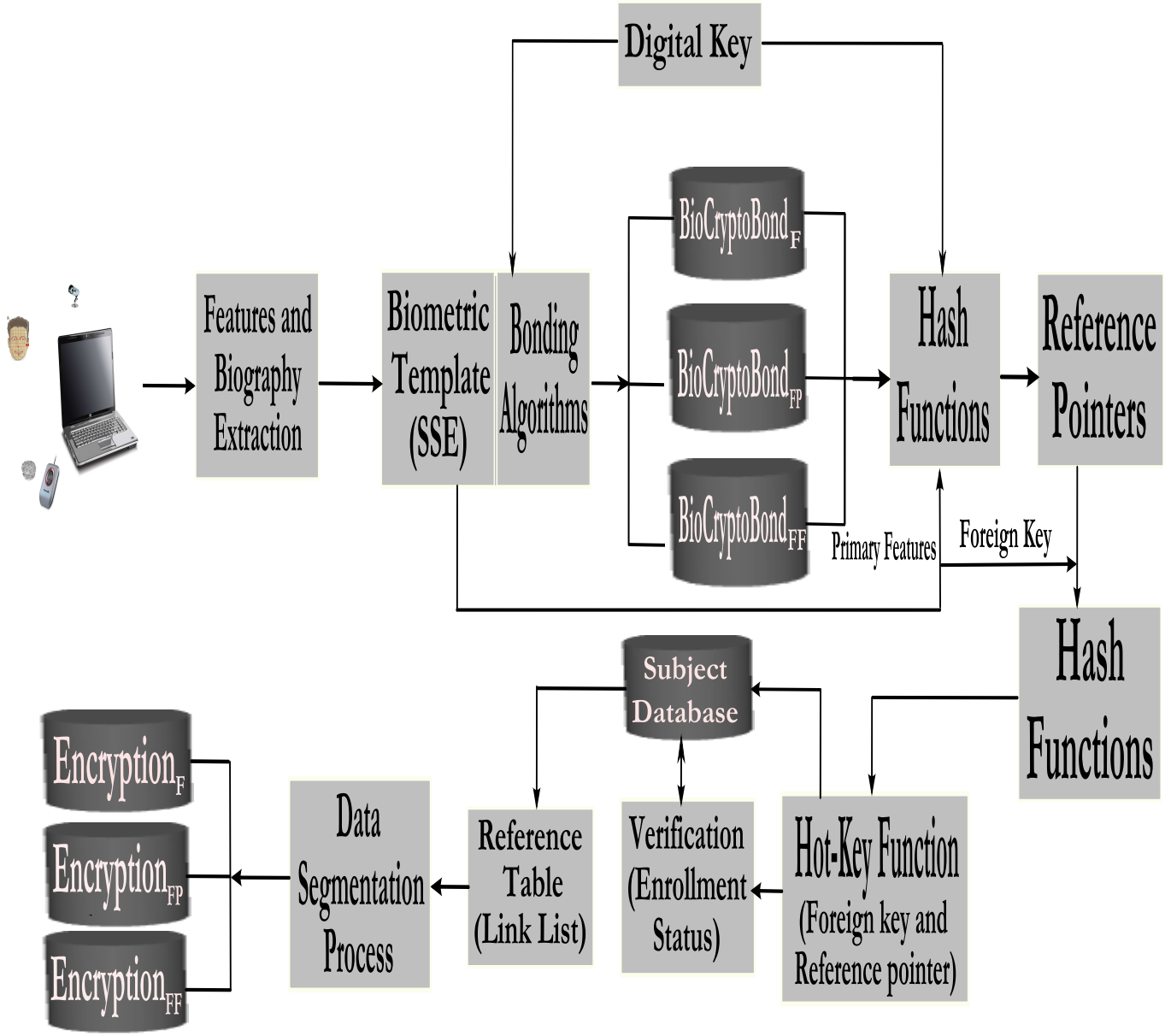


Figure 4.6: Subject Enrollment Process

is required to develop a map for the proposed biometrics information infrastructure [see Section 4.4 and $Appendix - B$].

(ii) Biometric template is verified with the stored template at *Subject Database* (dB_s) using the Hot-Key function (Fig. 4.6 and Fig. 4.8).

(iii) Upon activation of a positive verification signal (if subject not enrolled), a reference table is created (link list); the intra data segmentation technique has been developed as shown in Fig. 4.6 and Figs. 4.9.

The segmentation process can be formulated as follows:

$$\begin{aligned} \Phi_{hk} &= \mathbb{H}[\mathbb{F} \times \mathbb{R}^s] \\ \Upsilon &= \mathbb{R}^s \times \Phi_{hk} \times \digamma(s) \end{aligned} \tag{4.8}$$

where $\mathbb{F}$ and $\mathbb{R}^s$ are the foreign key and reference pointer, respectively, and Υ represents segmented data.

(iv) Hot-Key function in conjunction with the reference table and data segmentation process develops a Biometric Data Management System (BDMS) [Section 4.4].

(v) Finally, the biometric template and description of subject are stored (enrolled) in respective subject databases $Encryption_F$, $Encryption_{FP}$, $Encryption_{FF}$, and dB_s as shown in Figs. 4.5 and 4.8.

4.3.4 Authentication

In the case of the user authentication process, fingerprint biometric features received from the authorized user are combined with the cryptographic bond, $BioCryptoBond_u$, and the digital secret key is released. In this stage, authentication is performed to ensure the legitimacy of the user and to release the user secret key K^u. The user authentication process is shown in Fig. 4.7.

During the user authentication cycle, the same algorithmic operation stated in

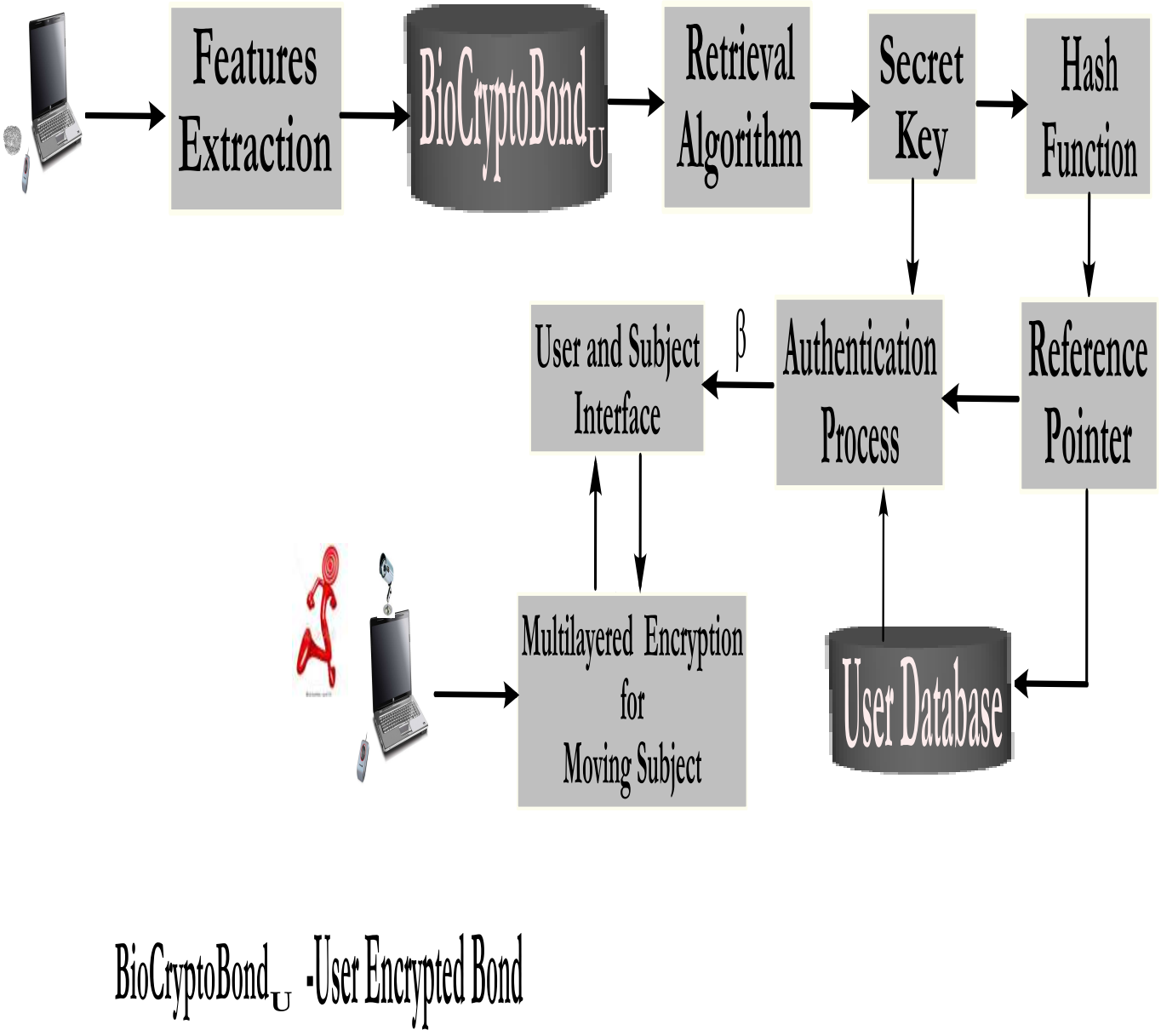


Figure 4.7: User Authentication Process

Eq. (4.3) is performed on the live user fingerprint features, generating the matrix Π. Afterwards, Π is combined with the previously stored $BioCryptoBond_u$ to release the key K^u. This process can be stated as follows:

$$\begin{aligned} \mathbb{T} &= \theta \times \digamma(s) \\ \Pi &= \mathbb{T}_{or} \\ K^u &= \Pi \times BioCryptoBond_u \end{aligned} \tag{4.9}$$

Once the secret key is activated and released, it is hashed with the user biometric features and generates the reference pointers required to complete the final level of authenticity of the user. This reference pointer along with the secret key then allows the user to access the system. This process can be formulated as follows:

$$\begin{aligned} \mathbb{R}^u &= \mathbb{H}[K^u \times \mathbb{I}_p] \\ \text{Required Info} &= \mathbb{R}^u\ [dB_u] \end{aligned} \tag{4.10}$$

where $\mathbb{R}^u$ is the user reference pointer.

Finally, a triggering signal is processed to initialize an interface between user and subject, if the user authenticity is found positive. This interface allows the user to prepare a system platform for receiving subject biometric features as an input. Furthermore, the system also releases an interface pointer β, which is required to ensure that the system is ready to enroll, authenticate, and release subject information in the presence of the legitimate user and the subject of interest. The analysis, implementation, and execution process of the subject authentication system and its features protection method are presented in Chapter 5.

4.4 Biometrics Data Management System

The main objective of the Biometrics Data management System is to enhance the protection of the stored and dynamic biometric features against security, privacy, and unlinkability attacks. In this case, a multilayered and MultiBiometrics data management system has been proposed to protect the users and the subjects' biometric features. The cryptographic bonding architecture and its process have already been presented in previous subsections. The hash function, Hot-Key, and segmentation processes are integral parts of this management system, and are presented in the following subsections.

4.4.1 Hot-Key Function

The Hot-Key function is the compound function key generated from a combination of the reference pointer and foreign key [see $Appendix - B$]. The foreign key ($\mathbb{F}$) given in Section 2.3.7 is a 32-bit digital key generated from the primary indexed biometric features.

The first step of this process is to create a reference pointer for the users (or subject) from the system generated $32 - bit$ digital key hashed with the primary features of the user (or subject) biometrics. This reference pointer is used to store the encrypted user biometrics features (enrollment) in the user databases, as shown in Fig. 4.5. In this case, the user biographical information is stored in the user database dB_u (user database) and the encrypted biometric features are stored in the $Encryption_u$ database. This reference pointer is used to establish a relationship between user databases.

In the case of a subject database, the reference key is generated in the same way as the user. Afterwards, this reference key is hashed with the indexed foreign key generated from the subject biometric features as shown in Fig. 4.6. The output of this

hash function is called the Hot-Key (Φ_{hk}) function, and its main objective is to create an extra-layer (multilayered) of security for the stored and dynamic biometric features of the subject. Furthermore, the subject's biographical information and biometric features are stored in the subject databases (dB_s (subject database), $Encryption_F$, $Encryption_{FP}$, and $Encryption_{FF}$) and the generated reference pointers (i.e. key or function) are used to create a link between the subject databases through the reference table and data segmentation process. The system architecture of this methodology is presented in Fig. 4.8. The theoretical aspects of the hash key, foreign key, and Hot-Key functions are stated in $Appendix - B$.

4.4.2 Segmentation Process

The main purpose of the segmentation (stated in Section 2.3.7) process is to cluster (or group) the subject biometric features and biographical information based on the address pointers created as shown in Fig. 4.8. This clustering process is done using the index biometric features of face, fingerprint, and MultiBiometrics (fusion of face and fingerprint). In this process, a hash key function in conjunction with the composite key and reference pointer are implemented to construct the Hot-Key algorithm. In addition, the data segmentation technique along with the Hot-Key algorithm are employed in order to develop a secure Biometrics Data Management System ($BDMS$). A reference table is created which is basically a link list (or address pointer) to keep the reference addresses and to locate the records stored in the subject databases. Furthermore, the relationship between subject databases is also maintained by the reference table (along with the segmentation process) as stated in Fig. 4.6. The system architecture of this segmentation process is also presented in Fig. 4.9 [see $Appendix - B$].

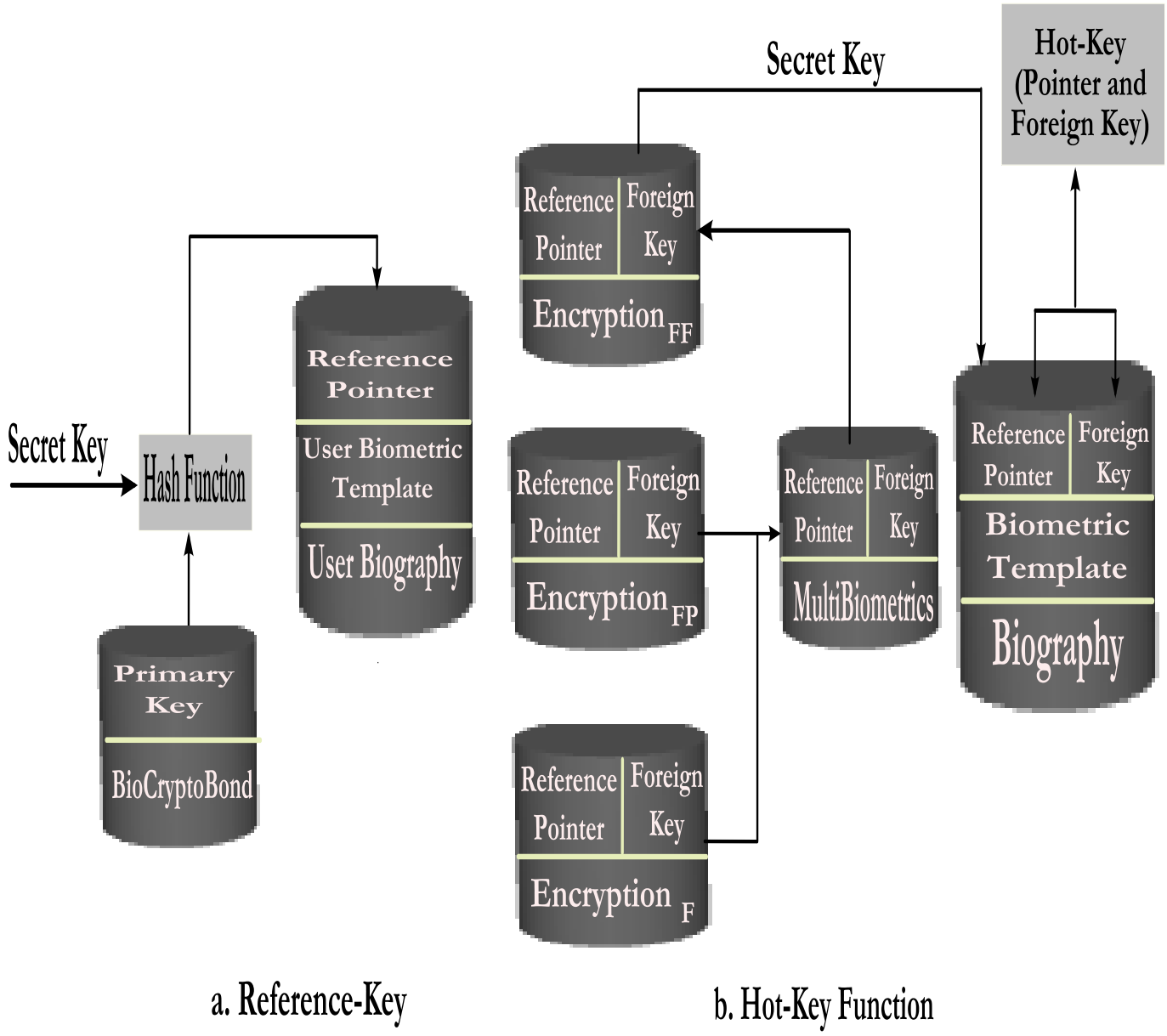


Figure 4.8: Key Generation Process

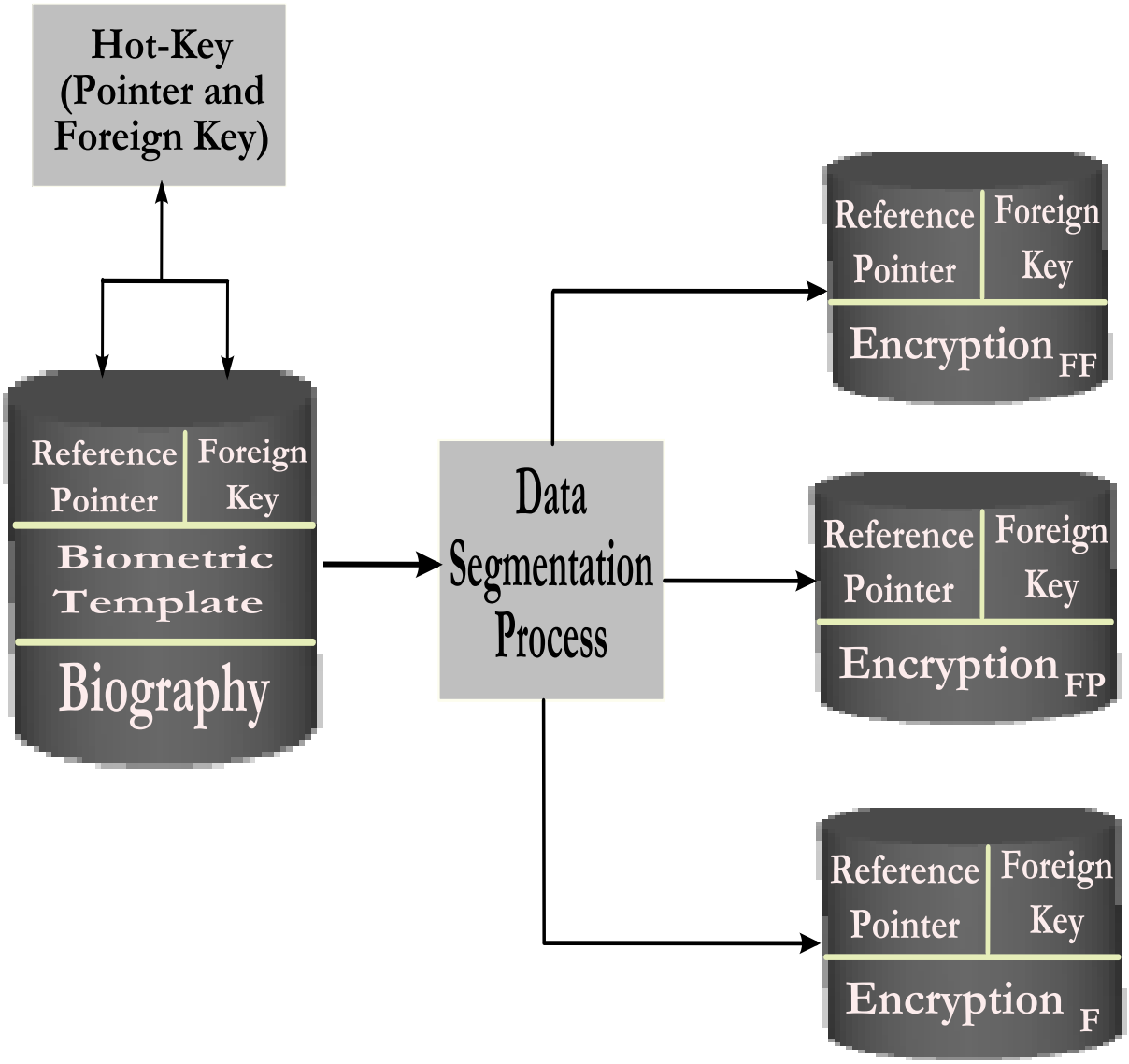


Figure 4.9: Segmentation Process

4.5 Evaluation

For example, if the same filter output $\digamma(s)$ is generated by an authorized user and an imposter, then the two authentication processes can be shown using Eqs.(4.3), (4.9) and (4.10):

Authorized user

$$\begin{aligned} \digamma_a(s) == \digamma_r(s) \text{ and } \theta_a \approx \theta_r \\ \Gamma_r = \mathbb{T}[\theta_{rr} \times \digamma_r] = \Gamma_a \\ \Pi_r = [\Gamma_r]_{or} \approx \Pi_a \\ K^u = \Pi_r \times BioCryptoBond_u \\ \mathbb{R}^u = \mathbb{H}[K^u] = \text{Authentication Successful} \end{aligned}$$

Imposter

$$\begin{aligned} \digamma_a(s) == \digamma_r(s) \text{ and } \theta_a \neq \theta_r \\ \Gamma_r = \mathbb{T}[\theta_{rr} \times \digamma_r] \neq \Gamma_a \\ \Pi_r = [\Gamma_r]_{or} \neq \Pi_a \\ K^u \neq \Pi_r \times BioCryptoBond_u = \text{Authentication Failed} \end{aligned}$$

where the subscripts a and r represent actual and received values, respectively; and other parameters carry the same meaning as given in Eqs.(4.3), (4.9) and (4.10).

The biometric database is protected by the multilayered encryption method. The biometric information is segmented, and reference pointers are used to establish a link between the segmented biometrics. In this method, it isn't possible to obtain the original biometrics from these reference pointers and vice versa. As well, it isn't possible

to know the individual's identity or construct (or guess) original biometric features of an individual from the segmented biometrics stored in the databases. Database is segmented and information is transformed, so complete authorized processing is required in order to access the biometrics and biographic information. Therefore, this system is invincible to unlinkable attacks, and imposters cannot retrieve data based on information found in other parts of the system.

Computational Complexity

Computational complexity starts from Eq. (4.1), which is required $O(N)$, and both Eq. (4.2) and Eq. (4.3), which are required $O(N^2)$. The computational complexities from Eq. (4.4) to Eq. (4.10) are $O(N^3)$.

4.6 Experimental Results and Analysis

In this experiment, two types of authentication processes have been performed: i) user authentication, and ii) authentication and retrieval of the subject's information. The experimental results and resultant analysis presented here are based on these two processes. The data obtained from this experiment is included in $Appendix - C$.

4.6.1 User Authentication

In this experiment, two user encrypted databases were created for 30 users, then 10 users with fingerprint biometrics from the public database ″CASIA Fingerprint Image Database Version 5.1". The encrypted database set containing 30 users has been used for authorized user fingerprints, and the encrypted database set containing 10 users has been used for imposter fingerprints. The main objective of this process is to authenticate the legitimacy of a user. An evaluation of the verification performance of the encryption method is also presented in this chapter. In this case, each of the 40

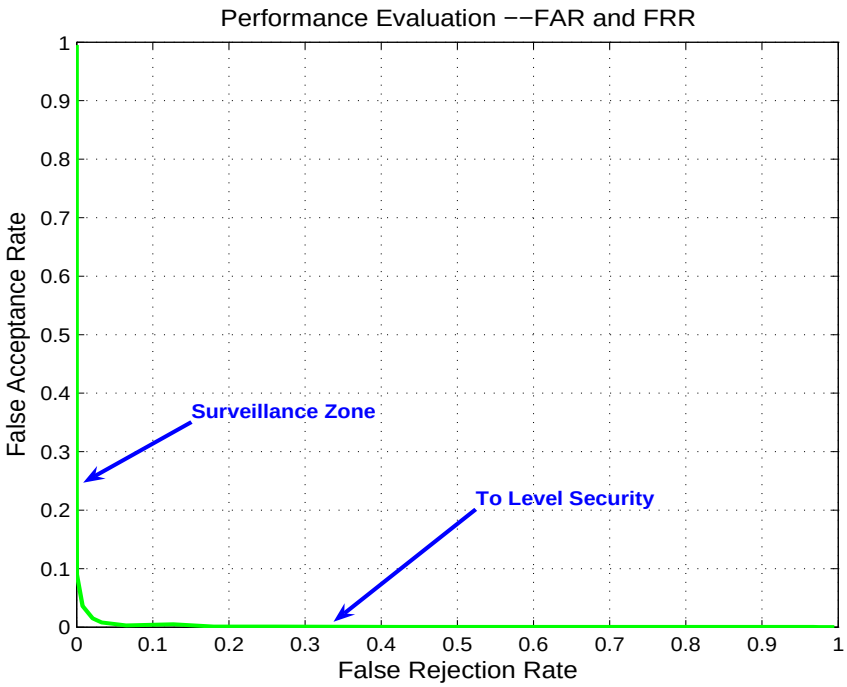
users has been tested against the encrypted users' biometrics stored in the databases. The performance of the verification process has been evaluated based on the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). The experimental results of this verification process have been recorded in Table 4.1, and the graphical outcome of the FAR, FRR, and ROC are presented in Fig. 4.10.

Table 4.1: *Performance Evaluation in (%) - FAR, FRR, and EER (User Fingerprint Biometrics)*

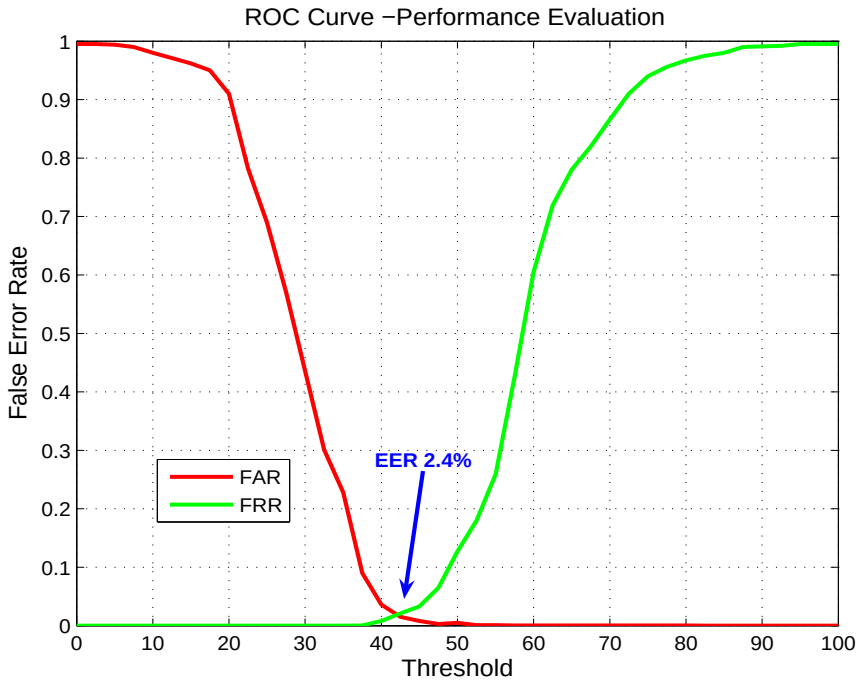
Database	FAR	FRR	EER
User -CASIA Fingerprint	1.20	3.50	2.40

4.6.2 Authentication and Retrieval of the Subject's Information

The performance of the proposed Biometric Encryption (BE) method has been evaluated based on the images of the public databases: "Put Face Database" [75], "Indian Face Database" [76], and "CASIA Fingerprint Image Database Version 5.1". The experimental results presented here are based on the authorized users' authentication processes using fingerprint biometric features in the presence of the respective subjects. In this experiment, two sets of encrypted user databases and four sets of encrypted subject databases have been created from the original image databases. The user databases were created for 20, then 10 users with fingerprint biometrics from the fingerprint images. In this case, the set containing 20 users has been used for imposter fingerprints and the set containing 10 users has been used for authorized user fingerprints. These encrypted user databases were created from the fingerprint images from the public database: "CASIA Fingerprint Image Database Version 5.1". Two of the four encrypted databases contain facial biometrics of 20 and 40 subjects, respectively. These databases were created from the facial images of the public



(a) FAR and FRR



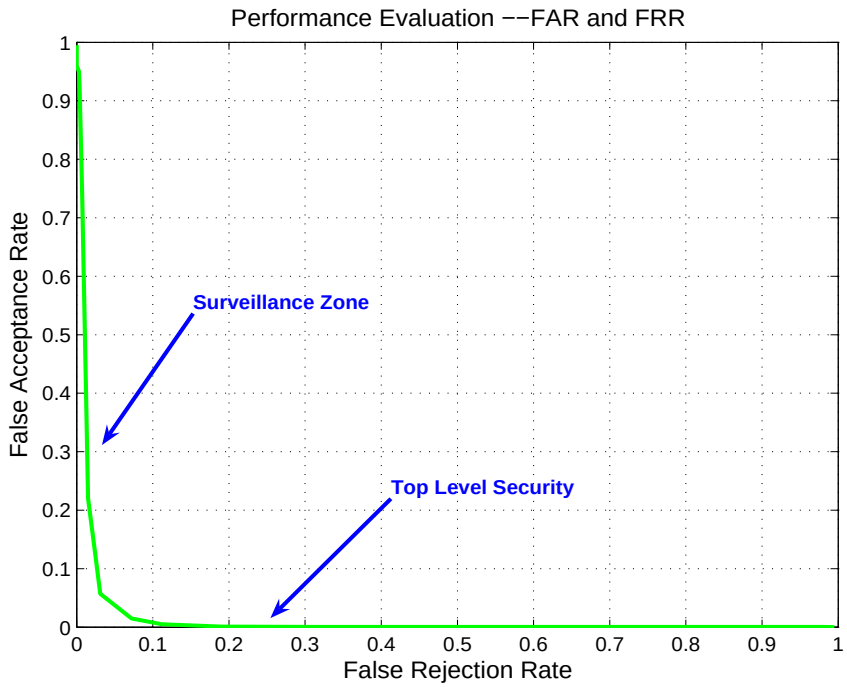
(b) ROC Curve

Figure 4.10: User Fingerprint Biometrics -Verification Process

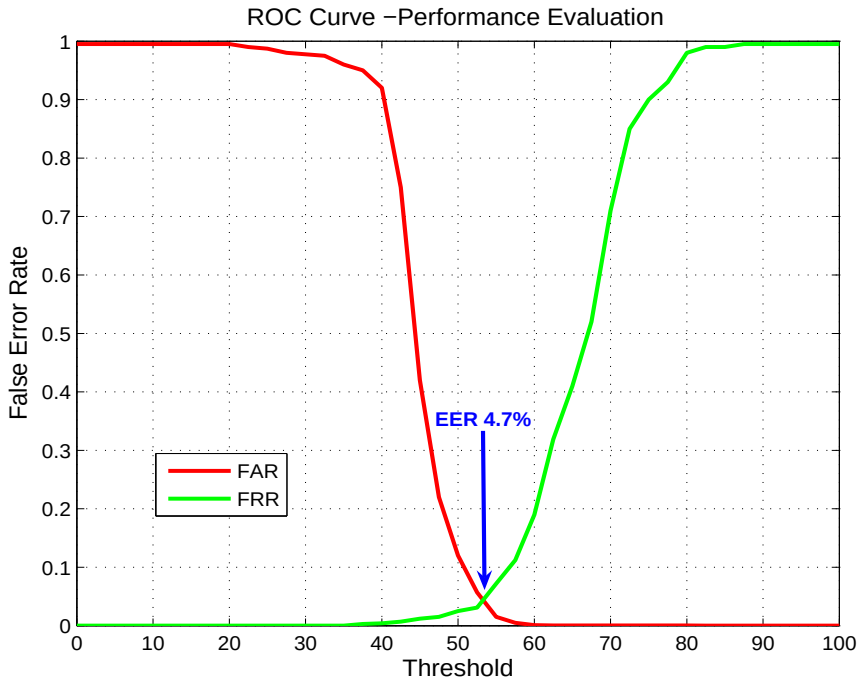
database: "Put Face Database". The other two sets contain facial biometrics of 10 and 20 subjects, respectively, created from the facial images of the public database: "Indian Face Database". Each subject's biometrics along with their biographies have been stored in their respective databases as stated in the above sections. In this experiment, the retrieval of the subject's information from their databases has been attempted by legitimate and illegitimate users, with and without the presence of the subject. The retrieval by each legitimate user has been conducted by comparing the encrypted fingerprint biometrics of each user with another fingerprint biometric of the same user, with and without the presence of the subject. Imposter processing has been conducted by comparing the encrypted fingerprint biometrics of one user with the encrypted biometrics of the other users. The percentages of Correct Recognition Rate (CRR), False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER) have been determined, and experimental results have been recorded. The experimental results of this authentication process have been recorded in Table 4.2 and Table 4.3. Simulation results from the legitimate (and illegitimate) user verification process to retrieve the subject biometrics in the presence (and without the presence) of the respective subjects are shown in Figs. $4.11 - 4.14$. As well, the performance of the identification process has been shown in Fig. 4.15, and this result has been recorded in Table 4.4 and Table 4.5.

Table 4.2: *Performance Evaluation in (%) - FAR, FRR, and EER (Put Face Database)*

No. of Subjects	FAR	FRR	EER
20 Subjects	1.45	8.50	4.70
40 Subjects	1.75	9.30	5.10

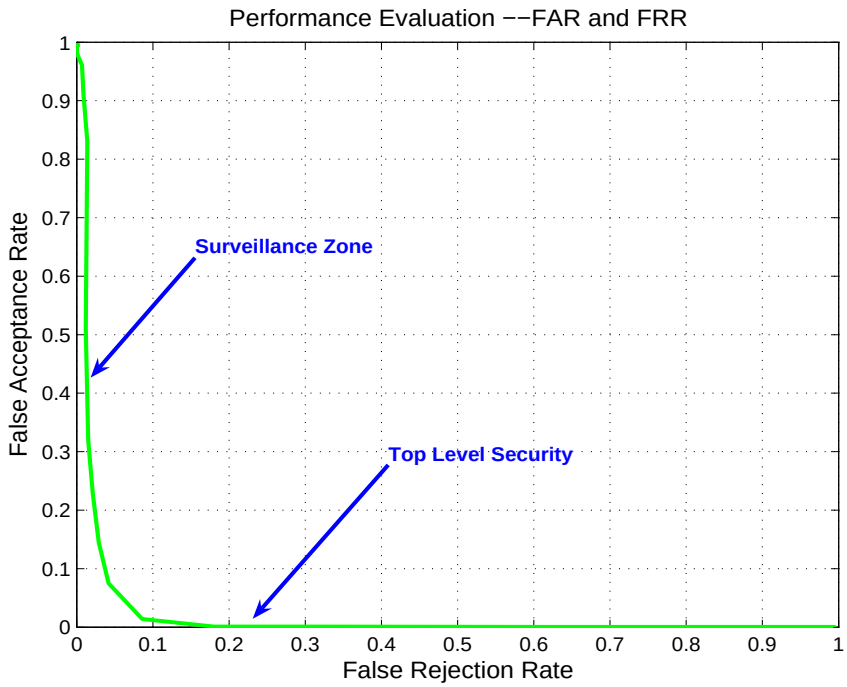


(a) FAR and FRR

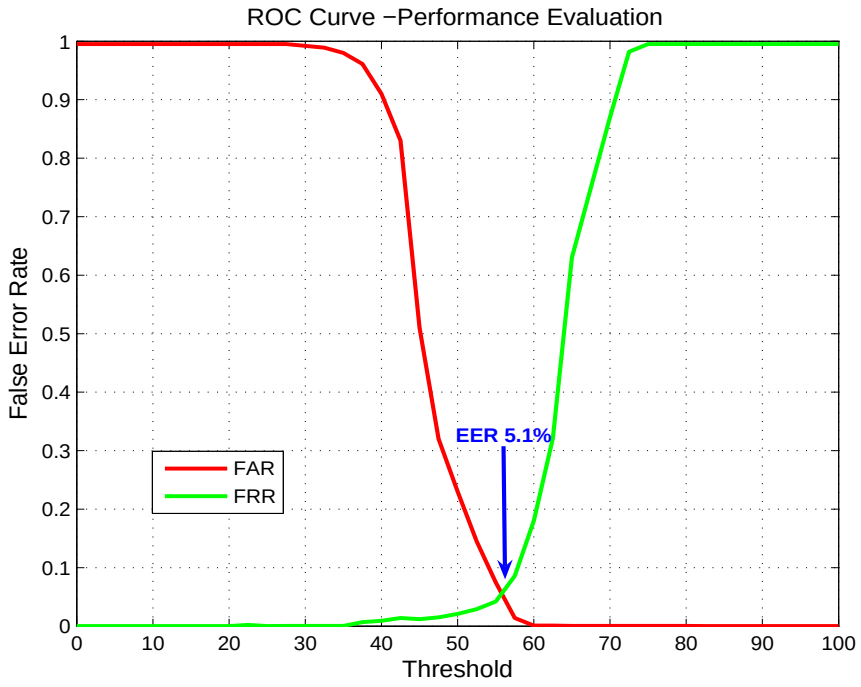


(b) ROC Curve

Figure 4.11: MultiBiometrics Encryption –Put Face Database(20 subjects)

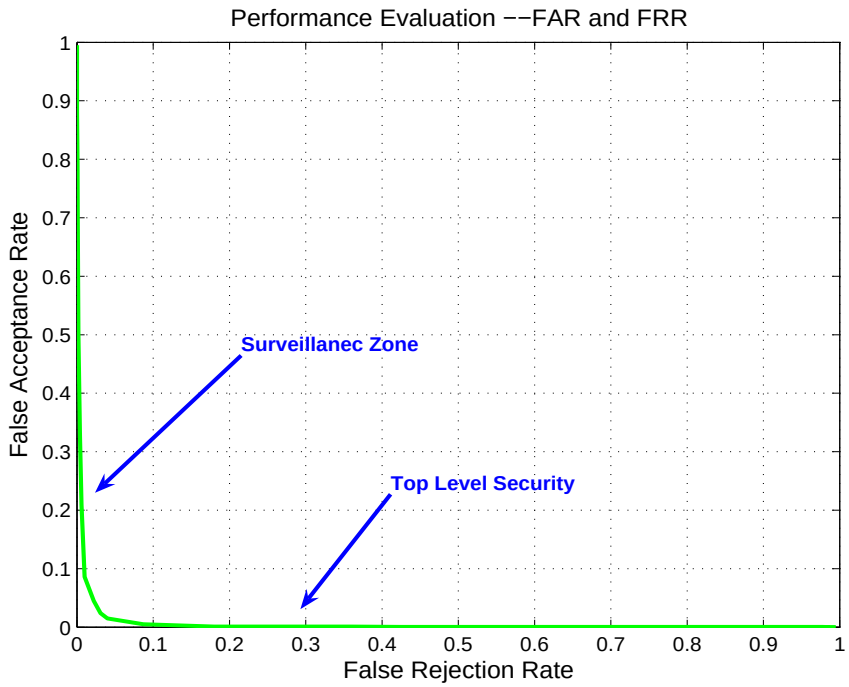


(a) FAR and FRR

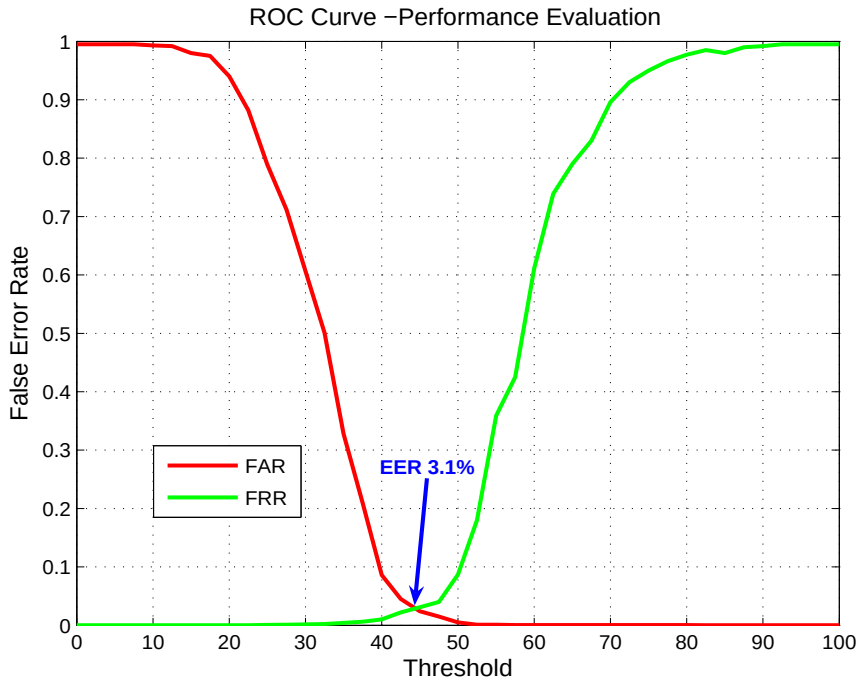


(b) ROC Curve

Figure 4.12: MultiBiometrics Encryption –Put Face Database(40 subjects)

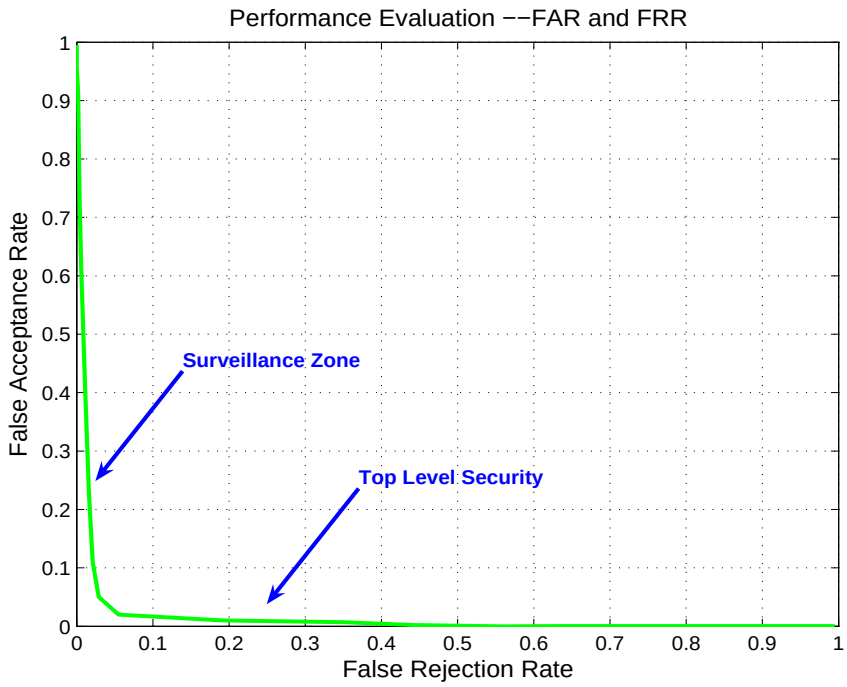


(a) FAR and FRR

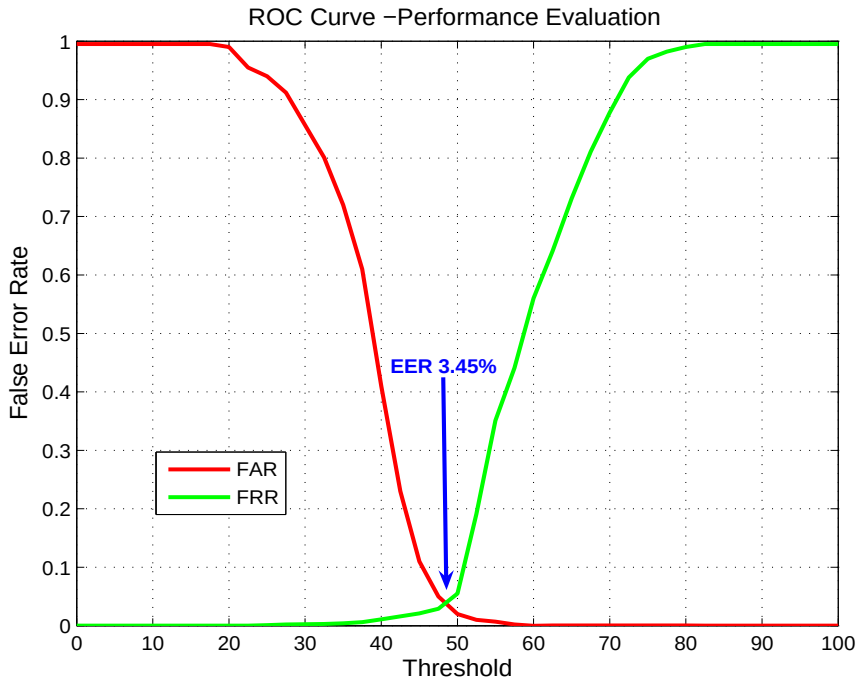


(b) ROC Curve

Figure 4.13: MultiBiometrics Encryption –Indian Face Database (10 subjects)

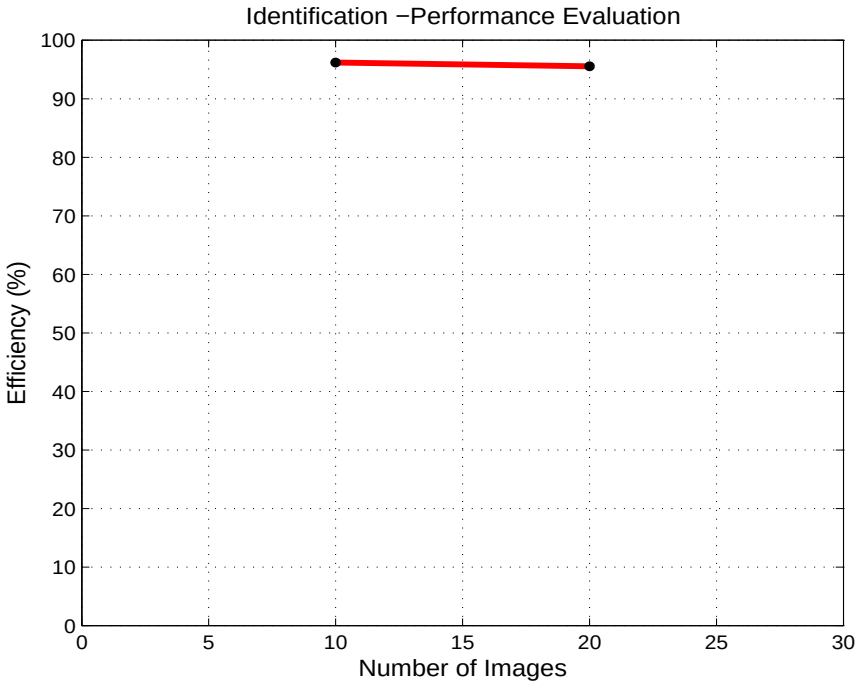


(a) FAR and FRR

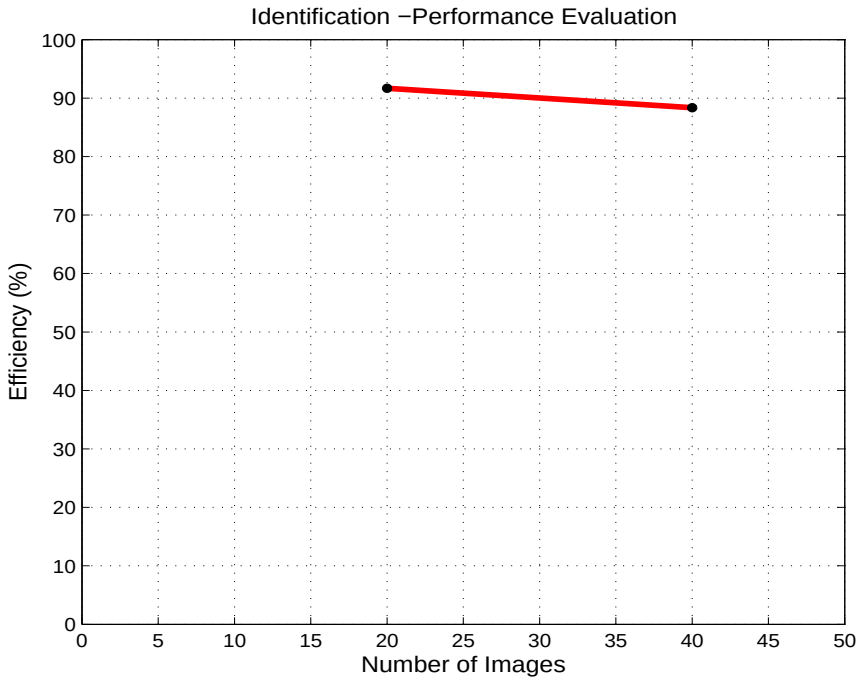


(b) ROC Curve

Figure 4.14: MultiBiometrics Encryption –Indian Face Database (20 subjects)



(a) CRR -Indian Face Database



(b) CRR -Put Face Database

Figure 4.15: MultiBiometrics Encryption -Identification Process

Table 4.3: *Performance Evaluation in (%) - FAR, FRR, and EER (Indian Face Database)*

No. of Subjects	FAR	FRR	EER
10 Subjects	1.50	4.60	3.10
20 Subjects	1.86	5.40	3.45

Table 4.4: *Performance Evaluation in (%) - CRR (Put Face Database)*

Database	**20-Subject**	**40-Subject**	**Average**
Put Face	91.68	88.35	90.02

4.6.3 Analysis and Discussions

The experiment for the encryption method presented in this chapter has been performed based on the encrypted user fingerprints and subject facial biometrics. The experimental results for this authentication process are recorded in Tables $4.1 - 4.5$, and simulation results for this experiment are shown in Figs. $4.10 - 4.15$.

First, the experiment for this method has been conducted for the encrypted user fingerprint biometric databases. Fingerprint images from the public fingerprint database "CASIA Fingerprint Image Database Version 5.1" were used to create two encrypted user databases with 30 and 10 users, respectively. The performance of the verification process for this encryption method with fingerprint biometrics has been analyzed and evaluated. In this case, there were 30 legitimate user records, and therefore there were 30 genuine matches. An EER of 2.4% has been achieved, and a FAR of 1.2% at the cost of FRR 3.5% has been achieved using this proposed method.

Afterwards, user encrypted biometrics databases with 10 and 20 users were created using fingerprint images of the public fingerprint database "CASIA Fingerprint

Table 4.5: *Performance Evaluation in (%) - CRR (Indian Face Database)*

Database	**10-Subject**	**20-Subject**	**Average**
Indian Face	96.20	95.55	95.87

Image Database Version 5.1". The encrypted database set with 10 users contained authorized users, and the set with 20 users contained imposters. As well, two subject encrypted facial database sets, each of 10 and 20 subjects, have been created using the public facial image database "Indian Face Database". Two more subject encrypted facial database sets, each of 20 and 40 subjects, have also been created using the public facial image database "Put Face Database". The Receiver Operating Curve (ROC) of the proposed method, based on the legitimate (and illegitimate) user authentication in order to retrieve the subject biometrics in the presence (and without the presence) of the subject, has been presented in Figs. $4.11 - 4.14$. This ROC curve measures the performance of the verification system, and has been plotted as a function of threshold values. FAR and FRR presented in the ROC curve characterize the verification accuracy, and the point EER represents the performance of the encryption method. Experimental results for the verification process have been recorded in Table 4.2 and Table 4.3. In this experiment, an EER of 3.1% and FAR of 1.5% at the cost of 4.6% FRR have been achieved. In addition, the performance of the identification process has also been analyzed using CRR. The results are recorded in Table 4.4 and Table 4.5. The simulation result is shown in Fig. 4.15. It was found that a CRR of 95.87% has been achieved using the proposed encryption method.

4.7 Conclusions

A biometrics system contains attributes that exclusively represent an individual's identity. These properties don't change and are difficult to lose or fake. Therefore, the main concern for the exploration of the biometric system is to protect the security and privacy of these biometric features. This cannot be neglected otherwise it can revert the overall process in the opposite direction, since the damage to this system is irreversible and may cost more than the system it is used for. In this chapter, a MultiBiometrics encryption and management system have been presented that protect biometric features against security, privacy, and unlinkability attacks. In this encryption method, secure cryptographic bonds have been created to protect not only the stored biometric features but also the dynamic biometrics, as the comparison during the authentication process is performed in the unencrypted domain. In addition, to further enhance the authentication accuracy and to protect the biometric features, a Biometrics Data Management System has been developed. The main objective of this data management system is to protect the biometrics from unlinkability attacks. In this method, the encrypted biometrics are segmented before being stored in the biometric databases. The relationship between the segmented biometrics and their databases is maintained by the reference pointers, which contain the addresses of the location where the biometric features will be stored. It isn't possible to retrieve the biometrics and the identity of an individual from these reference pointers. This is a clustered operation and every point of the operation has to be performed successfully to establish a link between all of the reference pointers necessary to retrieve the biometric and biographic features.

Furthermore, the proposed MultiBiometrics *BioCryptoBond* is secure and efficient, since a 1.5% FAR has been achieved at the cost of 4.6% FRR. According to the experimental results, the proposed method is also found to be robust with a promising

EER of 3.1%. As well, this method provides multilayered protection against security, privacy, and unlinkability attacks for the dynamic and stored biometric features in the databases. It can also be concluded that the encryption method presented in this chapter is heuristic, robust, and reliable in comparison to its counterparts. This is because, unlike other key binding encryption systems, the biometric data management architecture is implemented to enhance security protection and improve authentication accuracy. Without a successful authentication process, neither the secret key nor the biometric features can be retrieved independently from the cryptographic bond. In addition, even if the secret key or the transformed biometric features are intercepted at any point of operation by the imposter, the original biometric features are not obtainable. Finally, top level security has also been maintained for subject biometric templates, since the retrieval of the subject's biometric features would also require the physical presence of the subject along with (release of pointer β) a successful user authentication process.

Chapter 5

Implementation and Execution

5.1 Introduction

It is of paramount importance for government and private organizations including airport security, the Lottery and Gaming Corporation (or Casino self-exclusion program), Secret Service, civil aviation, border security, and military to establish a robust, reliable, and accountable surveillance zone for their field of view (FOV). Organizations are often required to track people in motion; for example, they may need to verify if a particular individual is the same person who had entered a room or crowd. As a result, biometrics is considered to be the most effective method of verification, since it offers undeniable physiological and behavioral attributes for authenticating an individual. However, dynamic targets in the surveillance zone are always noncooperative and vulnerable, and are obstructed by nonlinear, nonstationary, and heterogeneous noise. Therefore, as an organization grows, the threat of attacks to security and privacy also evolve. The Sequential Subspace Estimator (SSE) in conjunction with the MultiBiometrics encryption method presented in Chapter 3 and Chapter 4 can be used to overcome these challenges. This integrated method is an ideal system for protecting, authenticating, and tracking a single individual in the surveillance zone.

Potential places for implementation of this system include airport security checkpoints and the self-exclusion program of the Lottery and Gaming Corporation (or Casino). In this system, the SSE method is used to extract quality biometric features and create biometric templates, while the MultiBiometrics encryption method protects these biometrics from security, privacy, and unlinkability attacks.

The proposed MultiBiometrics authentication and encryption method may also have an important impact on the military, civil aviation, and Secret Service; particularly if they are targeting a noncooperative individual (i.e. suspect) within their favorable surveillance zones. This method can be used to track and authenticate a subject while also protecting the security and privacy of the subject's biometric features. Furthermore, certain institutions including museums, nuclear facilities, and those in the financial sector may want to use a surveillance zone to restrict an unauthorized personnel from accessing certain sections. Proper implementation of this integrated method would allow them to track and authenticate the legitimacy of existing personnel in order to control unauthorized access. To enhance the authentication system of a noncooperative moving target, gait biometrics along with facial biometrics have been fused to create a MultiBiometrics template. In this system, the received facial and gait images at the input terminal are analyzed, quality biometrics features are extracted, and biometric templates are stored. This MultiBiometrics can be used to establish a sophisticated top level biometrics surveillance system.

The implementation process presented here is based on the challenges associated with the Lottery and Gaming Corporation's self-exclusion program and the airport security checking system. However, these programs don't require a 24/7 rigorous monitoring system; in most cases these security systems are dedicated to verifying the authenticity of an individual in their limited CCTV zone in the presence of the authorized person. Furthermore, in this environment the system needs to extract biometric features from the semi-dynamic individuals for which the system also has

an inexpensive processing time. Since there is little information to be gained about an individual's identity from the gait biometrics, they are considered as a unity (i.e. identity matrix) and don't play any role in the tracking and authentication process.

In this implementation process, the main focus has been the self-exclusion program. Therefore, a brief description of the fundamental structure of the self-exclusion program used by the most of the Lottery and Gaming Corporations, and the detailed analysis, implementation, and execution process of the proposed integrated system based on this program are presented below.

5.1.1 Lottery and Gaming Corporation (Self-Exclusion Program)

Most Casinos (or Lottery and Gaming Corporations) offer a self-exclusion program, which allows the self-defined "problem individuals" to voluntarily opt their names out of Casino gaming sites. There are thousands of self-excluded members that have already been enrolled in the program. In this case, the enrollees of this program will be restricted from visiting the Casino. The surveillance area is monitored by cameras that can capture facial images without having any interaction with an individual. The authorities continuously track and authenticate self-excluded members in order to maintain the security and privacy of their patrons. If for any reason self-excluded members are found in the Casino sites, authorities will escort them off the premises [28],[29]. This self-exclusion program is an identification (1 to many) problem, which means they would be able to track and identify the suspect under surveillance. The integrated biometrics system presented here has addressed two important goals of the Lottery and Gaming Corporation: (i) authenticate a self-excluded member amongst the crowd, and (ii) protect the security and privacy of the members. However, the viability of its implementation based on the Casino's existing technology hasn't been addressed. Furthermore, it has also been considered that surveillance cameras have the ability to capture an individual's facial image. In this chapter, the detailed

implementation, execution, and performance evaluation of the proposed integrated method for the self-exclusion program of the Lottery and Gaming Corporation (or Casino) is presented.

The remainder of the chapter is organized as follows: Section 5.2 outlines the detailed system overview, operational principle, implementation, and execution process of the proposed integrated method for the Casino self-exclusion program; Section 5.3 contains the experimental results and analysis; discussions are presented in Section 5.4; and conclusions are given in Section 5.5.

5.2 MultiBiometrics Authentication and Encryption –Integrated System

In this section, a parallel and decentralized biometric tracking system based on facial and fingerprint physiologies and gait behavioral characteristics is presented. The objective of this biometric system is to implement a tracking system that can authenticate an individual in the surveillance zone, while also protecting their security and privacy. The detailed system overview and operational principle of this implementation method is presented in Fig. 5.1.

5.2.1 Operational Principle

In this case, the received facial and gait (i.e. speed and step size) biometrics of the subject are compiled separately as templates. These templates are then verified against the stored templates or pointer from the temp tracking database as shown in Fig. 5.1. If there are no stored templates in the database, the database pointer processes a positive Null signal and allows the tracking system to store the newly created templates in the temp database as a new entry. Otherwise, the new templates undergo the subject verification process (at matching score level fusion) using the

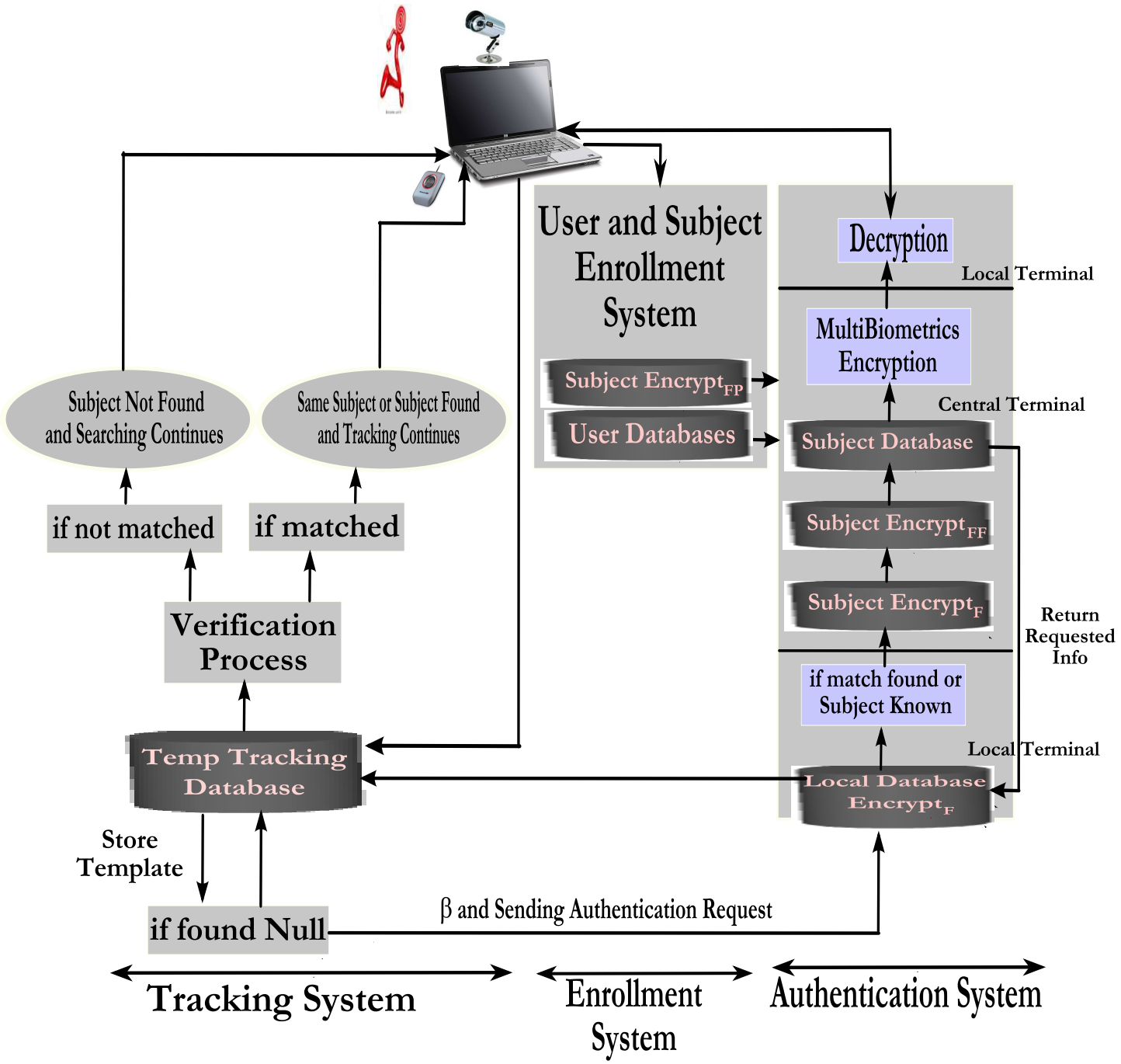


Figure 5.1: MultiBiometrics Authentication and Encryption -Integrated System

previously stored templates. If the matched score level is positive (if match found), then the new templates replace the old. Moreover, the tracker works like a close loop, continuously searching or tracking the moving subject (i.e. self-excluded member) within the surveillance region.

A trigger pulse for the authentication process is generated by the tracking system once in a complete tracking cycle to request biographic information regarding the subject of interest from the central terminal. This authentication signal is processed parallel to the tracking signal, and is initiated by the Null pointer when the Null verification pointer output is positive. The encryption method presented in Section 4.3.1 is implemented on the processed facial biometric template sent from the tracking section, and is compared with the stored encrypted face template. This comparison is essentially an initial identification process amongst biometric templates in the local database. The local database sends a biometric signal to the central station to perform a searching operation using the incoming face template, and complete a second layer of authentication for the subject if the initial authentication signal is positive. If a positive match is found at the second level, another triggering signal initiates additional layers of authentication processes to provide a description of the subject. The description is encrypted and fused with the user encrypted fingerprint biometrics at the central terminal before they are sent to the local station through the transmission line. The subject information received from the central databases is stored in local and temp tracking databases which then can be decrypted by the authorized user at the local terminal.

The overall process of this integrated system is divided into the following subsections.

5.2.2 Enrollment Process

As mentioned in Chapter 4, the enrollment and authentication processes of this integrated method are designed for two categories of people: user and target (self-excluded member or suspect). In this process, the fingerprint and facial biometrics of the suspected member are enrolled using the same method studied in Chapter 3 and Chapter 4. Authorized users are enrolled using only fingerprint biometrics as stated in Chapter 3 and Chapter 4. This enrollment process can be completed in the central terminal and the information can be stored in the databases. The system includes the extraction of quality biometrics from users and targets, and the generation of secret cryptographic bonds (*BioCryptoBond*s), the Hot-Key function, and the data segmentation process discussed in Chapter 4. The execution process of the enrollment system is presented in Fig 5.2 (see also Figs. 4.4 and 4.5), and the steps involved in this enrollment process can be stated as follows:

5.2.2.1 User Enrollment

The user under consideration is an authorized staff member of the Lottery and Gaming Corporation.

- Capture user fingerprint features.
- Extract physiological features from areas of interest (i.e. ridges, minutiae points, and core point).
- Implement Sequential Subspace Estimator (SSE) method and generate biometric template.
- Extract orientation angle $'\theta'$.
- Generate 32-bit cryptographic key K^u.

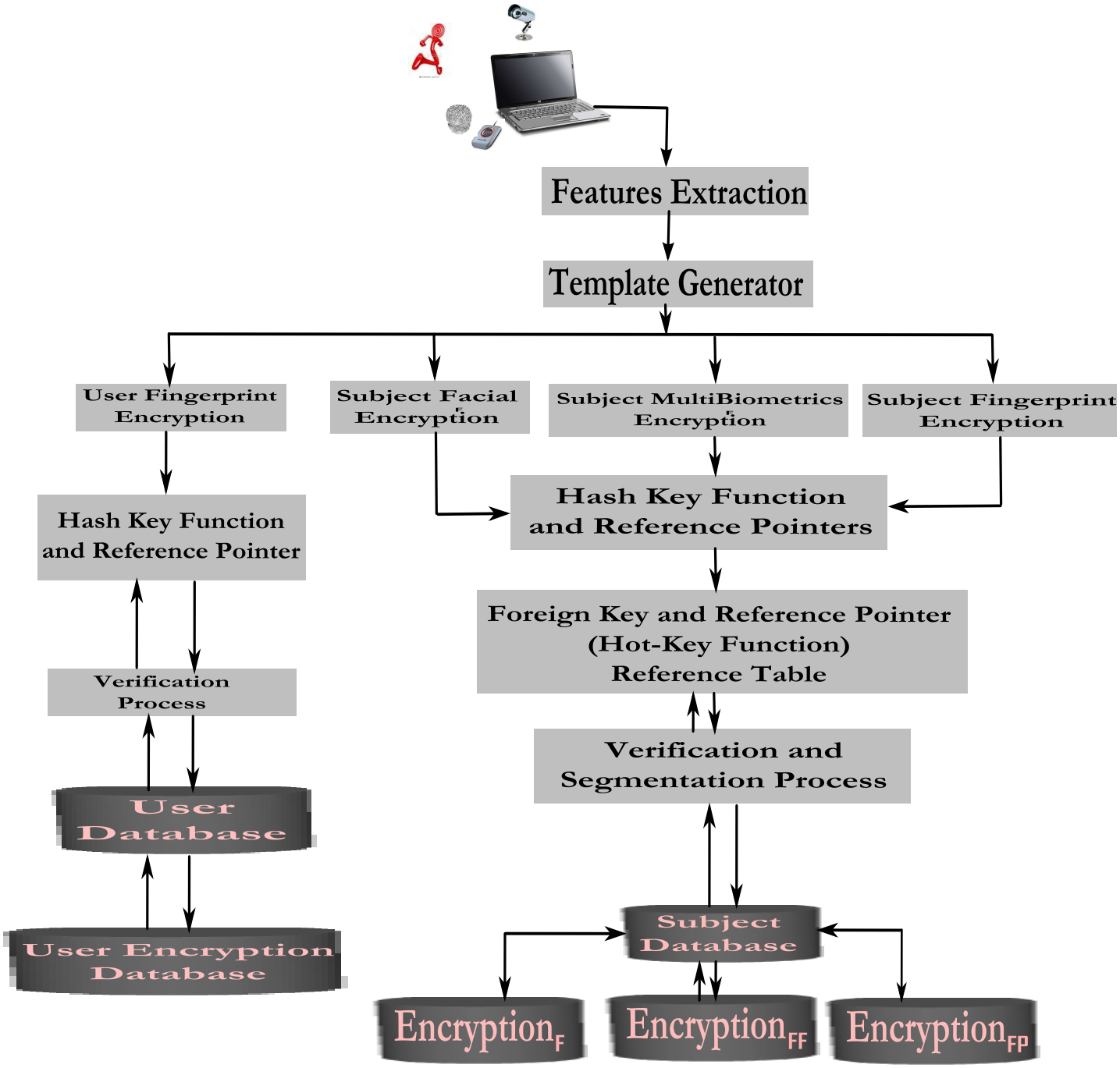


Figure 5.2: MultiBiometrics Encryption and Authentication -Enrollment Process

- Implement tensor operation on fingerprint biometric features as a function of orientation angle, and also perform orthogonal operation (see Eq. (4.3)).
- Implement encryption algorithm using output received from the previous stage and secret key K^u, and generate cryptographic bond, $BioCryptoBond_u$, for the user.
- Perform hash key operation and fuse with the encrypted template along with the user biographic information, and generate index pointer.
- Verify user authenticity with stored templates.
- Store templates (if user not found) into user databases dB_u and $Enryption_u$, and complete the enrollment process.

5.2.2.2 Subject or Member Enrollment

The subject under consideration is a self-excluded member of the Lottery and Gaming Corporation.

- Receive interface pointer β upon successful user authentication.
- Capture subject's facial geometry and fingerprint features.
- Implement Sequential Subspace Estimator (SSE).
- Extract biometrics from facial physiology (i.e. face area; relative locations and size of lips and eyes), and fingerprint (i.e. ridge, minutiae points, and core point).
- Generate three separate templates (i.e. facial, fingerprint, and fusion of face and fingerprint).
- Generate two cryptographic keys, K^s and $K^{s'}$.

- Implement tensor operation on facial biometrics as a function of β (see Eq. (4.5)).
- Perform orthogonal operation.
- Implement encryption algorithm using output received from the previous step.
- Generate first cryptographic bond $BioCryptoBond_F$.
- Implement tensor operation on same cryptographic key K^s.
- Implement encryption algorithm using transformed key K^s and fingerprint template (see Eq. (4.4)).
- Generate second cryptographic bond $BioCryptoBond_{FP}$.
- Fuse fingerprint and facial templates to create MultiBiometrics.
- Implement tensor operation on MultiBiometrics template.
- Implement encryption algorithm using transfomed MultiBiometrics and cryptographic key $K^{s'}$.
- Generate third MultBiometrics cryptographic bond $BioCryptoBond_{FF}$ (see Eq. (4.6)).
- Perform hash operation and fuse with encrypted biometrics along with the member's biographic information.
- Generate and share reference pointers among templates.
- Implement Hot-Key method.
- Generate reference data table to track and link data flow.
- Verify member authenticity (if not enrolled).

- Implement data segmentation method.
- All together create a Biometrics Data Management System (BDMS).
- Store template (if member not found) into databases: dB_s, $Encryption_F$ (face), $Encryption_{FP}$ (fingerprint), and $Encryption_{FF}$ (MultiBiometrics).

5.2.3 Tracking Process

The main objective of the tracking process is to track the member within the area of interest. The system includes the features extraction from the captured image, the data mining operation, and verification process. The execution process of the tracking system is presented in Fig. 5.3, and the steps involved in this tracking process can be stated as follows:

- Capture face and gait (gait is considered to be unity).
- Implement Sequential Subspace Estimator (SSE) method.
- Extract face and gait biometric features.
- Generate face and gait templates, respectively.
- Verify these generated templates with pointers, or templates previously stored in the $'Temp\ Tracking\ Database'$ as shown in Fig. 5.3.
- A positive Null pointer output indicates a new tracking process.
- Activate a new tracking signal and store both templates as a new entry in $'Temp\ Tracking\ Database'$, if Null pointer is positive.
- Send a triggering signal (required once in a complete tracking process) along with interface pointer β and facial biometric features to the central terminal through the local database $'Encrypt_F'$, and request the subject's biographic (identification) information.

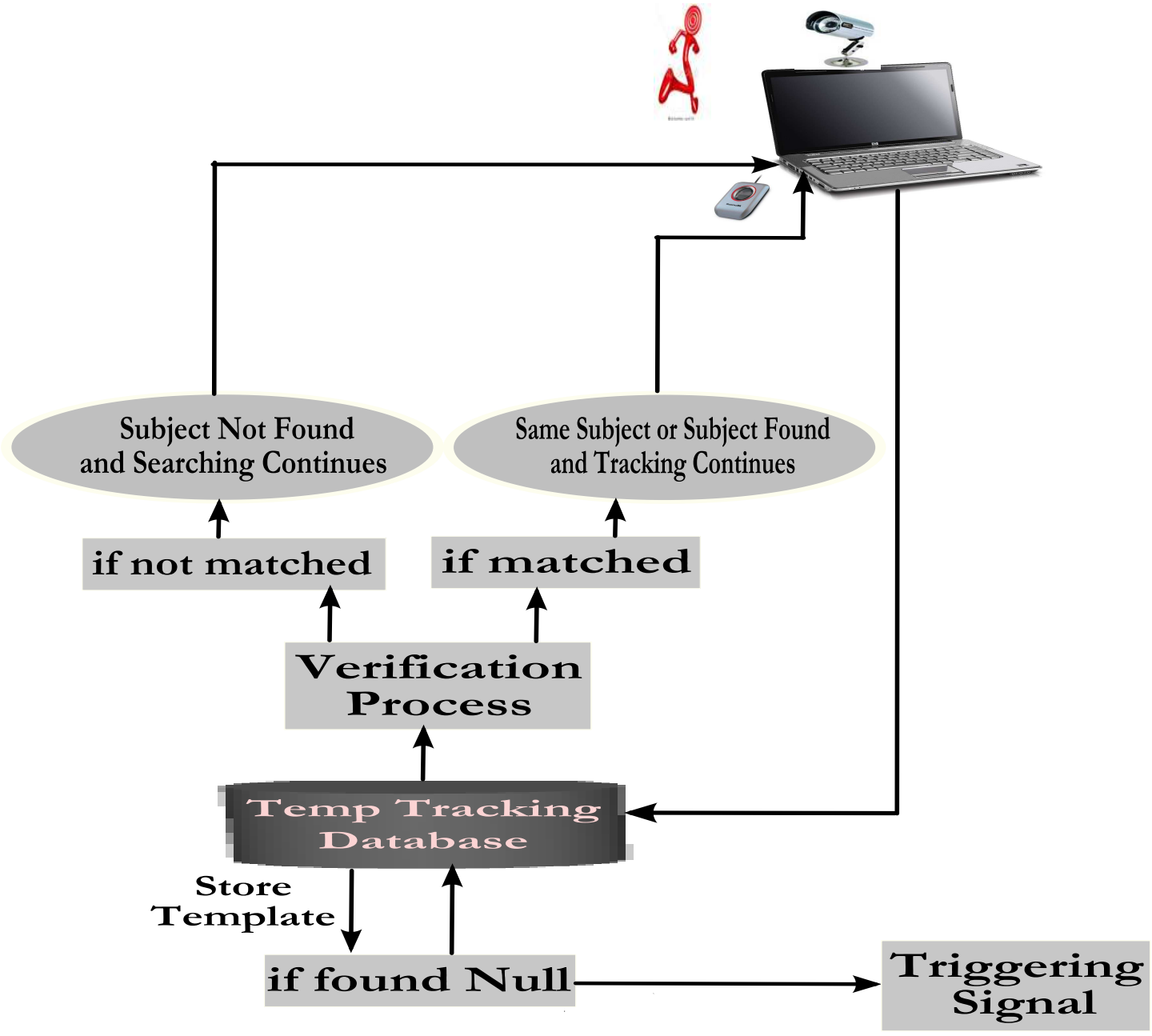


Figure 5.3: MultiBiometrics Encryption and Authentication -Tracking Process

- Otherwise, a negative Null pointer output indicates the continuation of the existing tracking process, thus no triggering signal is needed for processing in the central terminal.
- Tracking process continues.
- Verify subject with stored templates in $'Temp\ Tracking\ Database'$.
- Positive verification (match found) indicates the same member, so the tracking process continues; otherwise, the searching operation continues.

5.2.3.1 Verify if member is in *Temp Tracking Database* or Not

The method for creating the encrypted databases implemented here has already been discussed, and the steps involved in this process can be stated as follows:

- If a member match is found in $'Temp\,Tracking\ Database'$, then the same subject is found; the tracking and verification processes continue.
- If a member match is not found in $'Temp\,Tracking\ Database'$, the same subject is not found; the searching and verification processes continue.

5.2.3.2 *Temp Tracking Database* is NULL

- No subject is processed yet.
- Store current subject templates in $'Temp\ Tracking\ Database'$.
- Generate a triggering signal and send the signal to local database $'Encrypt_F'$ for authentication.
- Follow steps stated in tracking process.

5.2.3.3 *Temp Tracking Database* is Not NULL

- Tracking process already in progress, no triggering signal is needed to process the local database $'Encrypt_F'$.
- Verify if same subject is in $'Temp\ Tracking\ Database'$ or not.
- If verification is positive, a subject match is found in $'Temp\ Tracking\ Database'$; tracking and verification continue for the next scanning cycle.
- If verification is negative, a subject match is not found in $'Temp\ Tracking\ Database'$; searching and verification continue for the next scanning cycle.

5.2.3.4 Member Not in (or in) Local Database $Encrypt_F$

The method for creating the encrypted database $Encrypt_F$ implemented here has already been discussed, and the steps involved in this process can be stated as follows:

- If subject is not in the $'Encrypt_F'$ database, the subject hasn't been enrolled in central databases.
- Subject or target is not known.
- Tracker will not process identification request signal to central station or terminal. But, if member is in the database go to Section 5.2.4 and also do the rest of the steps (in this section) in parallel.
- Tracking or searching process continues using steps stated in the tracking process.
- Verify subject of interest with templates previously stored in $'Temp\ Tracking\ Database'$.
- If match score at matching level fusion is positive, the same subject is found and tracking continues.

- Otherwise, the searching process continues.

5.2.4 Tracking and Authentication Process

The identification system is designed to authenticate the member under surveillance once an authentication request is received from the tracking system. In this stage, the authentication system provides multilayered data security protection for the member databases. As well, the authentication request must also pass through a multilayered security protocol. Otherwise, a signal is generated indicating that the member is unknown, at which point the tracking process continues for the next suspected members. The MultiBiometrics encryption method developed in Chapter 4 has been implemented as an integral part of this system. The method for creating the encrypted databases and cryptographic bonds have already been discussed in Chapter 4 and previous sections. The execution process of the identification system is presented in Fig. 5.4, and the steps involved in this authentication process can be stated as follows:

- If the member is in the local database $'Encrypt_F'$, the subject has already been enrolled in central databases $'Encrypt_{FF}'$, $'Encrypt_F'$, $'Encrypt_{FP}'$ and $'Subject\ Database'$.
- Self-excluded member or subject is known (or recognized).
- Receive member facial template and interface key β.
- Implement tensor operation with the same algorithm used during the subject enrollment process involving facial biometrics.
- Fuse and compare (1 to many) with a previously stored member's cryptographic bond, $BioCryptoBond_F$, in the member facial database, $'Encrypt_F'$, at the local terminal.

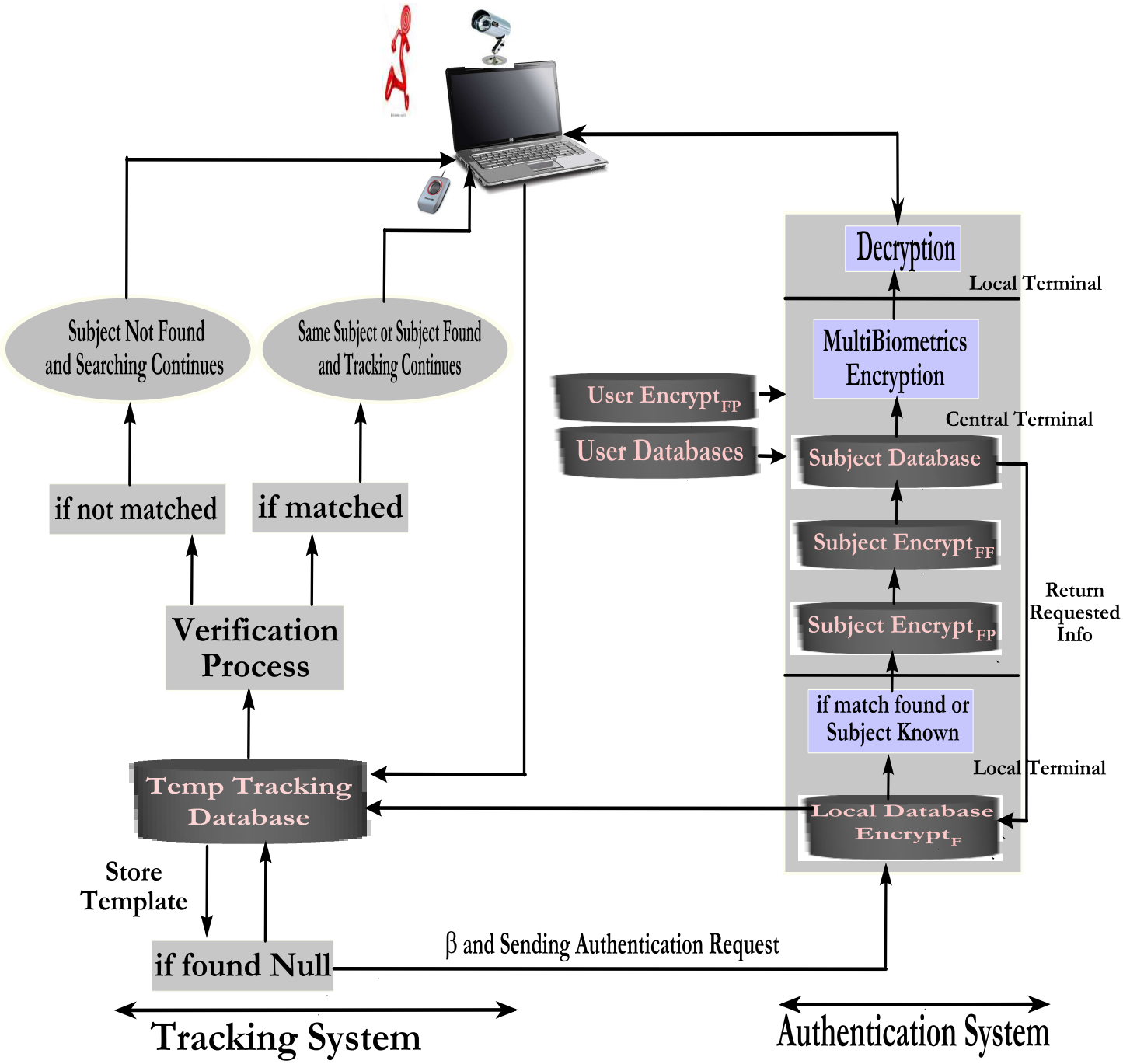


Figure 5.4: MultiBiometrics Encryption and Authentication -Tracking and Authentication Process

- Release secret key, K^s, if a match is found; and perform the tensor operation on the released secret key with the same algorithm used during the member enrollment process involving fingerprint biometrics.

- Search for cryptographic bond, $BioCryptoBond_{FP}$, corresponding to the transformed secret key, in $'Encrypt_{FP}'$ database in the central terminal, using the Hot-Key function.

- Fuse $BioCryptoBond_{FP}$ with the transformed secret key, and retrieve the member fingerprint biometric features.

- Fuse or concatenate facial and fingerprint biometric features to create a Multi-Biometrics template with the same algorithm used during the MultiBiometrics member enrollment process.

- Implement tensor operation with the same algorithm used during the subject enrollment process involving MultiBiometrics member biometric features.

- Fuse the MultiBiometric template from the previous stage with the secret Multi-Biometrics cryptographic bond, $BioCryptoBond_{FF}$, and release the secret key, $K^{s'}$.

- If a positive match is found, the secret key in conjunction with the Hot-Key function (reference and composite foreign key) locates and retrieves member identification information stored in the *Subject Database* in the central terminal.

- Fuse and encrypt member identification with the user secret key, K^u, at the central terminal before sending through transmission line.

- Send encrypted fused data to local terminal through transmission line.

- Verify user authenticity, then authorized user can retrieve or decrypt member identification information at local terminal.

- MultiBiometrics authentication and tracking system executes this authentication process in parallel to the tracking process once in a complete cycle.

Authentication and retrieval of the requested information at the central terminal can be formulated as follows:

$$\begin{aligned} T &= \beta \times \digamma_1(s) \\ \Pi_f &= T_{or} \\ K^s &= \Pi_f \times BioCryptoBond_F \ \ [Encryption_F] \\ \digamma_2(s) &= K^s_{or} \times BioCryptoBond_{FP} \ \ [Encryption_{FP}] \\ \mathbb{C}(s) &= \mathbb{C}([\digamma_1(s)][\digamma_2(s)]) \\ \Pi_{ff} &= \mathbb{C}_{or} \\ K^{s'} &= \Pi_{ff} \times BioCryptoBond_{FF} \ \ [Encryption_{FF}] \\ \text{Requested Info} &= Hot - Key(K^{s'}) \ \ [dB_s] \end{aligned} \tag{5.1}$$

5.3 Results and Analysis

The proposed integrated tracking and authentication method is a sophisticated system for establishing a top level surveillance zone in order to authenticate a single individual. This method uses MultiBiometrics, a fusion of facial and gait biometrics, for this purpose. It has been tested on a model being developed for the the Lottery and Gaming Corporation using 30 self-excluded members. In this experiment, the gait biometrics have been considered as a unity (i.e. identity matrix), and therefore

don't play any role in the tracking and authentication process. The integrated system has been divided into two parts: tracking and authentication; and the results and analysis presented here are based on these two parts. The data obtained from this experiment is included in $Appendix - C$.

5.3.1 Tracking

The tracking system is basically an automated authentication process performed in the local terminal. In the case of verification, the tracking system had to compare the captured facial biometric template of the suspected member with the biometric template stored in the "$Temp\ \ Tracking\ Database$". Identification was performed by comparing the captured template with the stored templates from the "$Encryption_F$" database. The "$Temp\ \ Tracking\ Database$" is a temporary biometric database created at the time of subject tracking. The encrypted facial database "$Encryption_F$" was created using 30 different members, each member having one biometrics template. The performance of the verification process for the tracking system has been evaluated based on the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). The experimental results are recorded in Table 5.1, and the graphical outcome is presented in Fig. 5.5. The performance of the identification process has also been analyzed based on the Correct Recognition Rate (CRR), and the experimental result of this identification system is recorded in Table 5.2. Finally, upon successful identification, a cryptographic key K^s has been released.

5.3.2 Tests and Results

The tracking system deals with two subject databases, $Temp\,Tracking\ Database$ and $Encryption_F$, and one user database: $User\ Database$ (dB_u). The $Temp\,Tracking\ Database$ is a temporary database whose information is being deleted at the end of the tracking

Table 5.1: *Performance Evaluation in (%) -FAR, FRR, and EER (Integrated System)*

Database	**FAR**	**FRR**	**EER**
Temp Tracking Database	6.5	5.8	5.6
$Encryption_{FP}$	7.3	4.8	4.25
$Encryption_{FF}$	1.5	4.6	3.1
Subject Database	1.1	4.3	3.8
Average	4.10	4.87	4.19

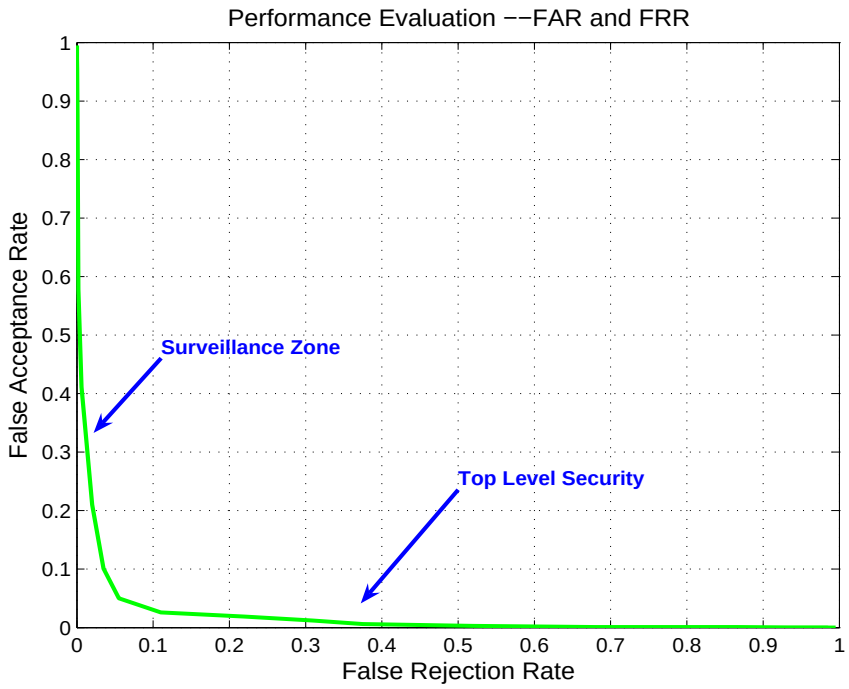
Table 5.2: *Performance Evaluation in (%) -CRR (Integrated System -*$Encryption_F$*)*

Database	**CRR**
$Encryption_F$	72.5

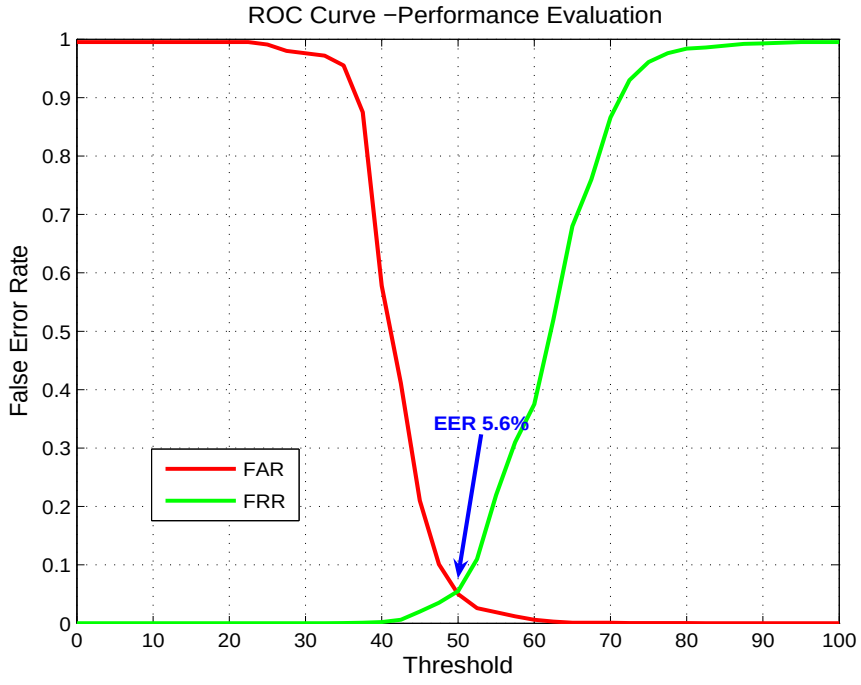
cycle. On the other hand, the $Encryption_F$ database is being created with facial biometrics of 30 different subjects (self-excluded members) and the user database dB_u contains 20 user accounts. The tests and their results from attempting to retrieve the user fingerprint and subject facial biometric features from dB_u and $Encryption_F$ databases, respectively are presented in Table 5.3:

5.3.3 Authentication

The authentication system for this integrated biometrics method is essentially an automated multilayered verification process. The entire authentication process has been performed in the central terminal. In this stage, three verifications of the databases $Encryption_{FP}$, $Encryption_{FF}$, and "Subject Database" were performed. These



(a) FAR and FRR



(b) ROC Curve

Figure 5.5: Integrated System -Tracking (*Temp Tracking Database*)

Table 5.3: *Test Results -dB_u and $Encryption_F$ Databases*

Retrieval from	**Input**	**Attempts**	**Successful**
$Encryption_F$	By user with subject	40	38
$Encryption_F$	By unauthorized user with subject	40	0
$Encryption_F$	By user with unauthorized subject	40	3
$Encryption_F$	When both are unauthorized	40	0
dB_u	By user	40	39
dB_u	By unauthorized user	40	0

three encrypted databases have been created for 30 self-excluded members using the methodology stated in the enrollment section of this chapter. In the first verification process, the released cryptographic key K^s from the previous stage was compared to the encrypted fingerprint template stored in the $Encryption_{FP}$ database, in order to release the member's fingerprints. Afterwards, the received facial (from the tracking part) and fingerprint biometrics from the previous two authentication processes were fused to create the MultiBiometrics template. This template was verified against the MultiBiometrics stored in the encrypted database $Encryption_{FF}$ in order to release the reference key $K^{s'}$ for the suspected member. The reference key was then validated using the key stored in the "Subject Database" database, and the member's information was released. Thus the requested information was sent and the authorized Casino user could retrieve the member's information at their terminal.

The performance of these three layers of the verification process was evaluated using the Equal Error Rate stated in Section 1.1.4. The percentages of FAR and FRR, and the corresponding EER points, were determined and experimental results were recorded. The experimental results based on the proposed method for the Lottery and Gaming Corporation are presented in Table 5.1. The graphical outcome of these results is also presented in Figs. $5.6 - 5.8$.

5.3.4 Tests and Results

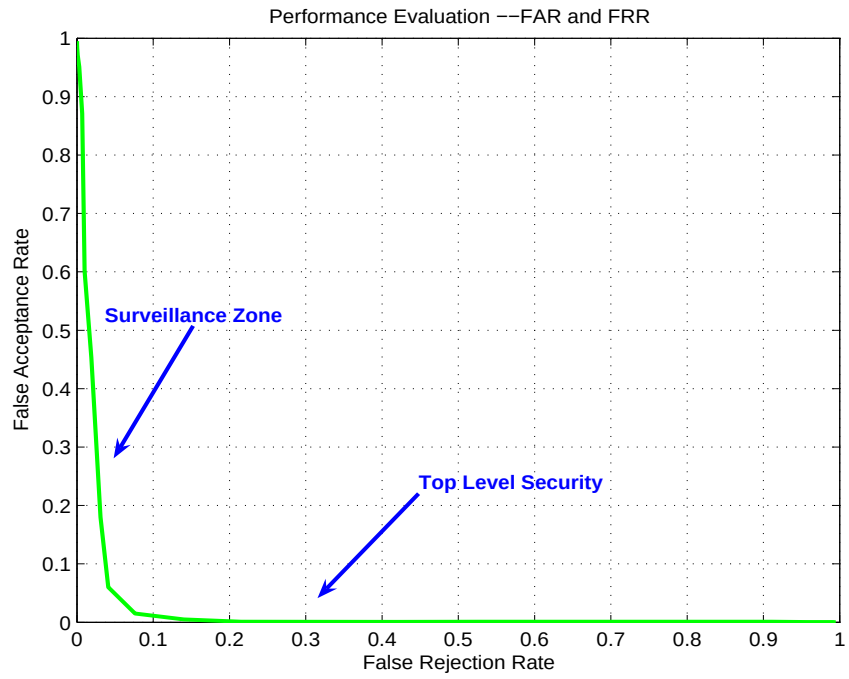
The authentication system deals with three subject databases: $Encryption_{FP}$, $Encryption_{FF}$, and *Subject Database* (dB_s). The tests and their results from attempting to retrieve the subjects' (self-excluded members) biometrics and biographic information from these subject databases are presented in Table 5.4:

Table 5.4: *Test Results -*$Encryption_{FP}$*,* $Encryption_{FF}$*, and* dB_s

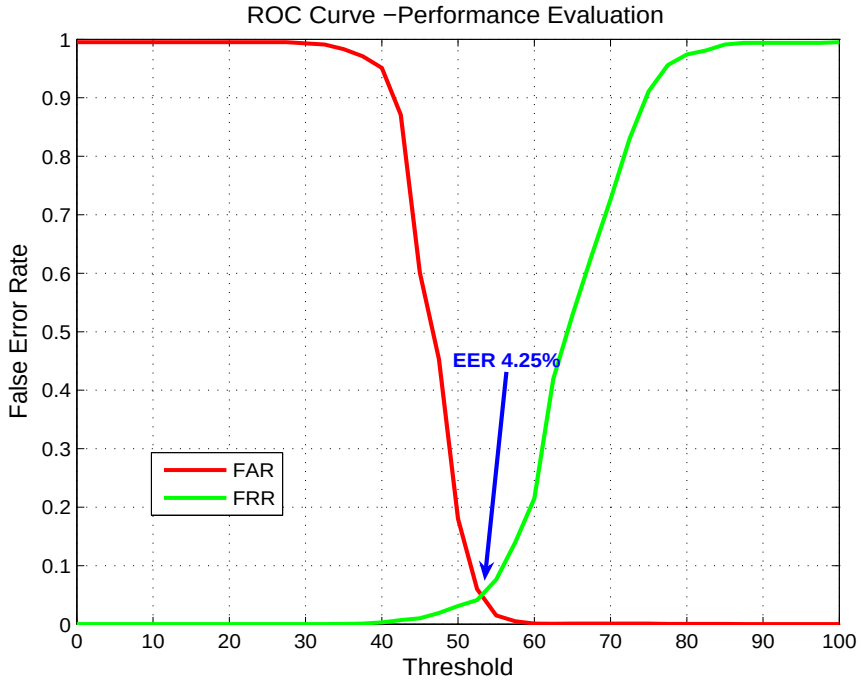
Retrieval from	**Input**	**Attempts**	**Successful**
$Encryption_{FP}$	Received from previous stage	40	37
$Encryption_{FP}$	Received from outside (unauthorized)	40	1
$Encryption_{FF}$	Received from previous stage	40	39
$Encryption_{FF}$	Received from outside (unauthorized)	40	0
dB_s	Received from previous stage	40	39
dB_s	Received from outside (unauthorized)	40	2

5.4 Discussions

In this experiment, a system for the Lottery and Gaming Corporation involving 30 self-excluded members has been presented. This system is the integration of the MultiBiometrics authentication and encryption methods presented in this dissertation. In this automated method, two important aspects of the Lottery and Gaming Corporation's self-exclusion program–the extraction of facial biometrics from the noisy environment and the information security and privacy-have been addressed. In this system, the combined effects of nonlinear, nonstationary, and heterogeneous noise due to illumination, position orientation, and background interferences of the extracted facial biometrics from the members under surveillance have been considered. The Sequential Subspace Estimator method presented in Chapter 3 has been implemented to overcome the noise associated with these extracted features. As well, the MultiBiometrics encryption method studied in Chapter 4 was implemented in

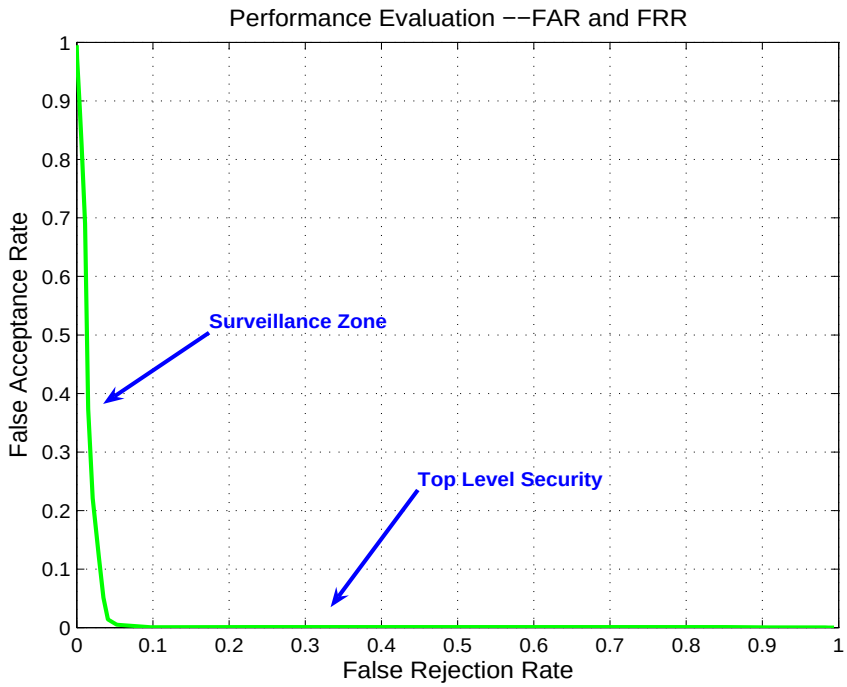


(a) FAR and FRR

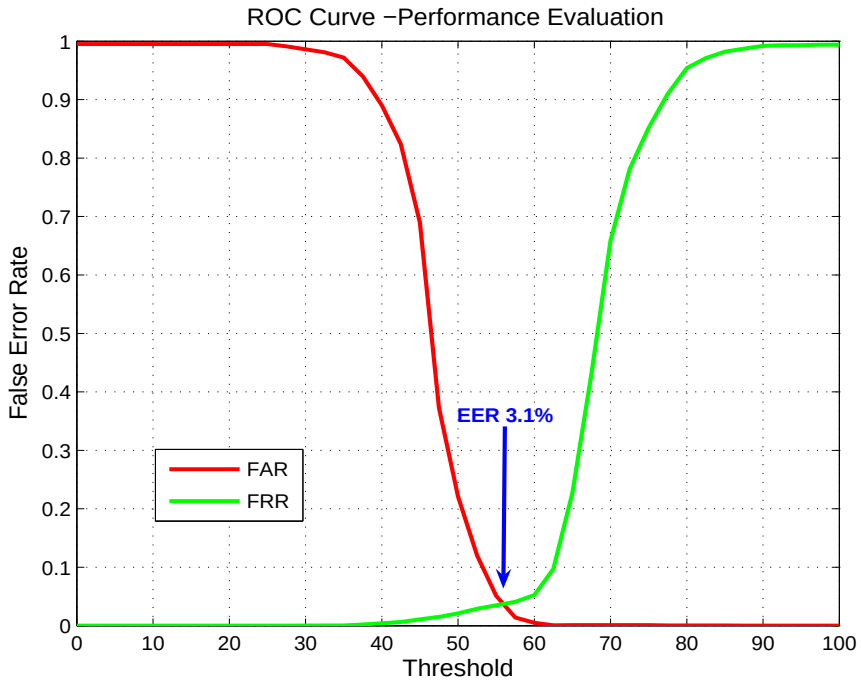


(b) ROC Curve

Figure 5.6: Integrated System -Authentication ($Encryption_{FP}$ Database)

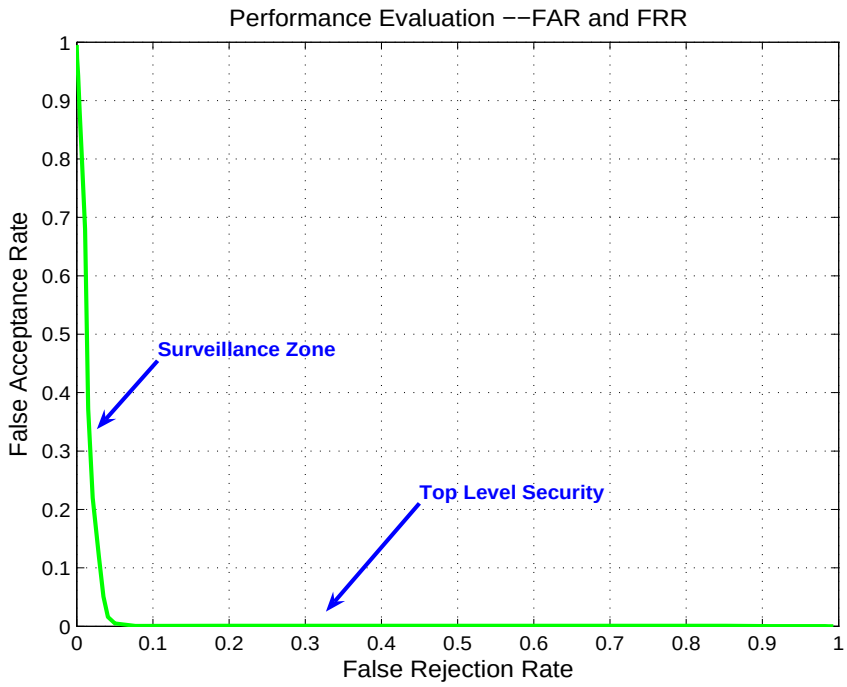


(a) FAR and FRR

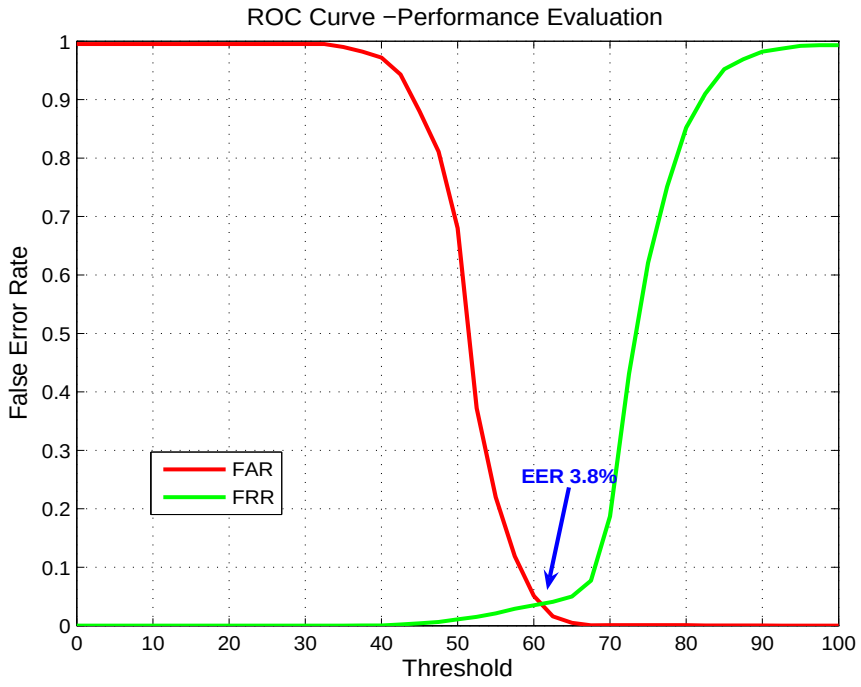


(b) ROC Curve

Figure 5.7: Integrated System -Authentication ($Encryption_{FF}$ Database)



(a) FAR and FRR



(b) ROC Curve

Figure 5.8: Integrated System -Authentication (*Subject Database*)

order to address security and privacy issues, allowing the system to be able to protect the biometric features against attacks. This system was developed under the assumption that the Lottery and Gaming Corporation has the technical and logistic ability to implement this integrated system. In this experiment, the extracted gait biometrics are being considered as a unity (i.e. identity matrix).

In the proposed integrated system, the enrollment process outlined in Section 5.2.2 is basically the enrollment process studied in Chapter 4. In this case, a step by step implementation and execution process has been presented. The tracking process presented in Section 5.2.3 is designed for a sophisticated top level surveillance zone. This integrated system has two main parts. In the case of the tracking system, the two databases "*Temp Tracking Database*" and $Encryption_F$ were created. Verification and identification processes were performed based on the extracted facial features as stated in the previous section. For the authentication system, three databases $Encryption_{FP}$, $Encryption_{FF}$, and *Subject Database* were created. In this case, three levels of verifications were performed before the requested member information was sent. This information can then be decoded at the local terminal by the Casino's authorized personnel. The experimental results for the verification process were recorded in Table 5.1 and the graphical outcome is presented in Figs. 5.5-5.8. According to the experimental results, an average EER of 4.19% and FAR of 4.10% at the cost of FRR 4.87% have been achieved. Furthermore, a CRR of 72.5% has been achieved for the identification process performed with the facial biometrics stored in the $Encryption_F$ database. As this is a model for the Lottery and Gaming Corporation, based on a sample of 30 members, the results could vary in a real life scenario as these institutions deal with a large volume of datasets.

5.5 Conclusions

The importance of a reliable, secure, robust, and cost-effective tracking and authentication system is of paramount importance for the Lottery and Gaming Corporation's self-exclusion program. This is especially important since the self-excluded members are always dynamic and mixed in amongst the crowd of other loyal patrons. Therefore, a step in the direction of facial and gait biometrics is being regarded as the promising solution for this program, since they facilitate the extraction of biometrics without intruding on the subject. In this chapter, a detailed implementation and execution process for the proposed MultiBiometrics authentication and tracking system for the Lottery and Gaming Corporation's self-exclusion members has been presented. The main objective of this integrated method is to locate and verify the identities of the members, while protecting the biometric features from security, privacy, and unlinkability attacks. This method is being developed under the assumption that their surveillance cameras are able to capture images of an individual. In addition, it is assumed that the Lottery and Gaming Corporation would be able to provide technological support in order to implement this biometrics self-exclusion system. This system is being designed using 30 self-exclusion members. However, in a real life scenario, the Lottery and Gaming Corporation deals with large-scale databases.

In this automated tracking method, facial physiology in conjunction with gait behavioral characteristics has been used to enhance the authentication accuracy of the suspect in the surveillance zone. However, in this experiment, only facial biometric features have been used, while gait biometric features are considered as a unity. The extraction process of the facial biometric features is being designed based on the proposed Sequential Subspace Estimator method, while the MultiBiometrics encryption method presented in Chapter 4 has been implemented to protect the biometric features. From the experimental outcome, it is evident that the proposed integrated

system is efficient, robust, and heuristic, since an average EER of 4.19% has been achieved in this integrated multilayered environment. This system is also highly secure, since multilayered, MultiBiometrics security management architectures have been implemented to protect against attacks. Furthermore, all the stored extracted target biometrics will be erased permanently from the system (temp database) at the end of the tracking process. The security and privacy of the transmitted data through communication channels have also been considered. More importantly, there is no direct link between the tracking and main systems. Tracking is completed in the local terminal and multilayered MultiBiometrics authentication and security agreements need to be fulfilled by the authorized user in the presence of the subject before they are granted access into the system and the member's information is released.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

Biometric systems rely on extracted human measurable physiological and behavioral features. These features are unique and sensitive, and are not irrevocable or reissuable if compromised. The performance of biometric systems is largely dependent on the quality of these extracted features. Acceptance and exploration of the biometrics are dependent on the security and privacy of these extracted features. This dissertation has addressed the two important aspects of the biometric system; namely the quality of the extracted biometric features to ensure an efficient authentication, and their associated computational complexity, security and privacy issues.

Most biometric systems are modeled under the assumption that the associated noise that obstructs the biometric features is linear, stationary, and homogeneous. But this assumption weakens the performance of the systems as they often deal with a nonlinear, nonstationary, and heterogenous noise environment. In addition, the biometric traits that are selected as potential candidates for the biometric systems are vulnerable to security, privacy, and unlinkability attacks. Most situations dealt with by biometric systems involve managing databases that contain higher dimensional

datasets. This makes computational complexity a vital issue, as the performance of the system is largely dependent on this factor. This dissertation addresses the deficiency in this regard and systematically investigates a biometric authentication and encryption process in the nonlinear, nonstationary, and heterogeneous environment.

In this dissertation, a Sequential Subspace Estimator (SSE) algorithm in the image subspace has been proposed. Typical, PCA, LDA, MLE, LMS, Bayesian, and Wiener methods are inadequate to deal with nonlinear, nonstationary, and heterogeneous noise; however they are optimal methods in a linear and stationary environment. The integration of PCA with Wiener, Bayesian, and MLE methods is being used to over these challenges. The other promising alternative for dealing with this situation is the sequential estimator. The main concern with the sequential estimator is its inadequacy when dealing with higher dimensional datasets. These datasets pose a problem for the sequential estimation method, since it needs to compute the covariance matrix and perform the matrix inversion operation. As a result, the proposed SSE algorithm is modeled in the image subspace under the assumption that the associated noise with the biometric features is nonstationary, nonlinear, and heterogeneous. In this case, the subspace algorithm is modeled in the image space to deal with the challenges associated with the sequential estimator. In the proposed SSE method, higher dimensional image space is transformed into L linearly independent images so that the dimension of the biometric features reduces from $N \times N$ to $M \times M$, where $M << N$.

This dissertation also proposed a MultiBiometrics encryption algorithm to guard biometric features from security, privacy, and unlinkability attacks. The encryption method is based on Biometric Encryption (BE), since this method provides more protection for security and privacy compared to its counterpart, the Feature

Transformation-based method. In this method, fingerprint and facial biometric features are used to create a cryptographic bond, called a "*BioCryptoBond*". Furthermore, a data management system is also proposed to enhance security protection and to improve performance and accuracy. The proposed MultiBiometrics encryption method is designed to deal with two categories of people: user and subject (target). In this method, one cryptographic bond "$BioCryptoBond_u$" for the user and three cryptographic bonds "$BioCryptoBond_F$", "$BioCryptoBond_{FP}$", and "$BioCryptoBond_{FF}$" for the subject are created. Furthermore, an orthogonal tensor projection method and its detailed algorithmic structure as a function of fingerprint orientation angle are developed. In addition, the system generates a random private key, which is monotonically bound to the extracted facial and fingerprint biometric features. This creates a cryptographic bond in such a way that neither the cryptographic key nor the biometric features can be released or decrypted independently without a successful biometric authentication. The Hot-Key algorithm and data segmentation techniques are implemented in order to develop a secure Biometrics Data Management System (BDMS). Three subject cryptographic bonds are created with the objective of providing multilayered security protection for the subject biometric features. It is evident that the neither the secret key nor the biometric features can be retrieved from this cryptographic bond. Moreover, to gain access to the subject's biometrics, both an authorized user and the subject are required to be present during the authentication process.

An integrated system based on the proposed MultiBiometrics authentication and encryption method has also been presented in this dissertation. The main objective of this integration is to track and authenticate a noncooperative moving target while protecting the security and privacy of the biometric features under consideration. This integrated system is being implemented in the Lottery and Gaming Corporation's self-exclusion program. Facial biometrics in conjunction with gait (gait is considered to be

unity) behavioral features of the moving target are used to track and authenticate the self-excluded members. In this case, the tracking system locates the moving target under surveillance and sends the request for the target identification information to the central system. Then the proposed multilayered MultiBiometrics encryption method authenticates the legitimacy of the the received request before the requested information is sent back to the local terminal.

The proposed method has been compared with the other state-of-the-art methods and its performance has been evaluated based on the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Correct Recognition Rate (CRR). The experimental results found that the proposed method outperformed its counterparts.

The main highlights of the chapters included in this dissertation are given below:

- Chapter 1: This chapter presents introductory information in regards to the biometric system and its associated challenges. The motivations and objectives of the proposed dissertation have also been included in this chapter.

- Chapter 2: A comprehensive literature review and associated challenges, along with supporting statements in favor of the proposed MultiBiometrics authentication and encryption method are presented in this chapter. This chapter also outlines several prerequisites required for the proposed method before getting into the detailed analysis, formulation, implementation, and execution process.

- In Chapter 3: The proposed Subspace Sequential Estimator (SSE) method is presented in this chapter. The main objective of this method is to ensure the quality of the biometric features and reduce the computational complexity in the estimation process, which would otherwise be obstructed by the nonstationary, nonlinear, and heterogeneous noise. This is one of the core chapters of this dissertation. At the beginning of this chapter, the SSE method is compared to other state-of-the-art methods, such as PCA, MLE, Bayesian, Extended Kalman, and

Wiener methods. The problem generation and formulation methodology are also included in this chapter. In the middle of this chapter, model formulation and detail methodology of the subspace process are included. An algorithmic flowchart and the analysis of the computational complexity of the proposed SSE method are also discussed. The proposed method is made independent of the biometric traits; however, the SSE method is tested using the facial images of two public databases "Put Face Database " and "Indian Face Database". The performance of the proposed algorithm is evaluated by the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Correct Recognition Rate (CRR). Finally, the experimental results and analysis, and comparisons to its counterparts are presented at the end of this chapter. It is apparent from the experimental analysis and outcome that the proposed SSE method outperformed its counterparts.

- Chapter 4: This chapter is another core chapter of this dissertation. In this chapter, the proposed MultiBiometrics encryption method and its management system are presented as a solution for protecting biometric features against security, privacy, and unlinkability attacks. This chapter is divided into encryption, enrollment, and the authentication process for two categories of people: user and subject. The method of developing the user's and subject's cryptographic bonds is presented at the beginning of this chapter. As well, a detailed user and subject enrollment process and its biometrics information management system are also presented in this chapter. The user authentication process and its management architecture are also discussed. The model evaluation and computational complexity of this encryption method are included in the middle of this chapter. Finally, the performance of the proposed method is analyzed based on the facial images of two public databases, the "Put Face Database" and "Indian Face Database", and fingerprint images from the "CASIA Fingerprint Image

Database Version 5.1" database. The performance of the proposed algorithm is evaluated by the False Acceptance Rate (FAR), False Rejection Rate (FRR), and Correct Recognition Rate (CRR).

- Chapter 5: The implementation and execution process of the integrated Multi-Biometrics authentication and encryption method is presented in this chapter. This integrated system can be utilized by the Lottery and Gaming (or Casino) Corporation, airport security, and surveillance zones. However, the implementation and execution process presented here is based on the Lottery and Gaming Corporation's self-exclusion program.

6.2 System Vulnerability and Failure

The proposed MultiBiometrics authentication and encryption method is being developed to provide security protection for two categories of people: user and subject.

The user's fingerprint biometric features are being extracted and transformed as a function of orientation angle to create a user template in the orthogonal domain. Afterwards, the data segmentation method is implemented to store user biometrics and biographic information into two user databases: $Encryption_u$ and dB_u, respectively, and a reference pointer is used to create a link between these databases. In the proposed system, the user biometric system is vulnerable to two types of attacks: i) attack on the reference pointer and ii) attack on the data or stored information. The attack on the reference pointer is a vital issue, since this pointer is the key to accessing and completing the system operation for the proposed method. Any changes to the reference pointer may cause interruption or failure of the system. On the other hand, attacks on user data include deletion or modification of stored information, and addition of new information to the database systems. These attacks should be a crucial consideration, since they may also cause system failure or interruption of

system operations.

But, both attacks cannot affect the security and privacy of the user's biometric features. Obtaining or creating a system specific reference point is tedious work, since passing the multifactor authentication requests is a requirement. The user system is unlinkable, so even if the attacker is able to create or obtain a reference pointer, they won't be able to get the complete user information unless the attacker can establish a link between two segmented user databases. Attempts to delete or modify the reference pointer are also tedious for the same reasons stated above. Attacks on user data or stored information may only serve to modify or delete an anonymous user record. But, the ability to cause the complete system or specific record to fail is not possible without having the system specific reference pointer in addition to establishing a relationship between two segmented user databases. In the worse case scenario, where the attacker deletes or modifies the system, system operation would be partially interrupted but the security and privacy of the user biometrics would not be affected.

The subject biometric system is more secure than the user biometric system. The subject biometrics and biographic information are being segmented and stored in four databases: dB_s, $Encryption_F$, $Encryption_{FP}$, and $Encryption_{FP}$. The Hot-Key function discussed in Chapter 4 (Section 4.4.1) is being used as a reference pointer to establish the relationship among these subject databases. In this case, the subject biometrics system is unlinkable and protected by the multilayered and Multi-Biometrics encryptions. It is almost impossible for the attacker to obtain complete information about the subject from these segmented databases, since the retrieval of the subject's biometric features also requires the physical presence of the subject along with a successful user authentication process. The only vulnerability that may be considered here, is an attack on the subject data or stored information. In this case, an attack on the subject data may only cause the modification or deletion of an

anonymous record. It won't be possible to make the complete system fail or to target a specific subject record without having the Hot-Key function and establishing the relations between the four subject databases. Obtaining the reference pointer and establishing the relationship are very tedious tasks, since the system is segmented, unlinkable, and multifactor transactions have to be processed to verify the legitimacy of the authentication request.

Finally, no system is 100% secure. The proposed system is vulnerable to system attacks as well as attacks to obtain reference pointers, which may allow the attacker to modify the anonymous data. The resultant effect may cause system interruption and may also fail to show the system performance and efficiency. However, the system is unlinkable, so access to specific user and subject biometrics information is not possible without having the reference pointers and without successfully completing the MultiBiometrics authentication process. But, obtaining a system specific reference pointer and completing the multifactor authentication process would be very tedious work for an unauthorized individual as per the reasons stated before. Administrative security and network access control systems can be implemented to avoid these system attacks. However, implementation of these securities is beyond the scope of this study.

6.3 Future Work

This dissertation has investigated two important aspects of the biometric system: the quality of biometric features leading to computational complexity and the authentication process, and Biometric Encryption (BE). In addition, the methodology of its integrated implementation and execution process is also presented in Chapter 5. However, in the implementation process, one aspect that is not vigorously defined is the protection of the extracted biometric features from the moving subject. It may be possible that the extracted features are vulnerable to security and privacy

attacks. In these circumstances, it is recommended to ensure that these features are protected during the implementation cycle studied in Chapter 5. However, this protection hasn't been considered since it is a time-consuming process and the extracted features of the moving target would be erased at the end of the tracking process. The implementation process developed here is for tracking and authenticating one target in a single tracking cycle; but in some cases, surveillance systems may need to deal with multiple targets. Therefore, an interesting option might be to make the proposed method able to locate multiple targets in the surveillance zone in a specific time slot. More importantly, the implementation, execution, and testing processes for tracking and authenticating the Lottery and Gaming Corporation self-excluded members are based on the small database of 30 self-excluded members. However, in a realistic environment, the Lottery and Gaming Corporation always deals with large dimensional datasets. So, the reader might be interested in testing the system in an operating environment that uses large dimensional datasets.

Furthermore, according to the proposed theory, the dissertation also claimed that the proposed Sequential Subspace Estimator (SSE) is independent of the biometric traits. However, since the testing is performed on the public fingerprint image database "CASIA Fingerprint Image Database Version 5.1", and two public facial image databases "Put Face Database " and "Indian Face Database", the reader may wish to see further tests using different biometric traits, including iris and hand geometry, in support of this claim.

In addition, the execution time for the verification process presented in Chapter 3 is slightly higher (but within the acceptable range) for facial recognition. The main reason for this longer execution time is due to the use of Microsoft Access databases in conjunction with Matlab. In this process, the system needs to search and locate the record of a person that contains the biometric features that need to be verified. However, the biometrics verification (1:1) process has been performed only

with the biometric features that the individual claimed to have. More observations and adjustments of the filter parameters as well as changing the combination of the training dataset may be useful to reduce the execution time of the verification process, even though the execution time of the identification process is within the promising range. Furthermore, in Chapter 4, the encryption method is tested using the "CASIA Fingerprint Image Database Version 5.1" database in conjunction with the two facial image databases discussed previously. Further testing of the method using other public databases is also encouraged. The proposed method has been tested on a facial image database with a maximum size of 600 images. A tracking system in conjunction with the authentication and encryption method is being proposed to implement in large institutions including the Lottery and Gaming Corporation (or Casino), museums, airport security, and those in the financial sector who want to use a surveillance zone to restrict unauthorized personnel from accessing certain sections in real time. These types of institutes always deal with massive database systems, so it may also be an interesting option to test the method within a large range of database environments.

Moreover, file structure also plays an important role in system performance; and the acceptability and feasibility of a biometrics system in a realistic operating environment are also largely dependent on it. In this dissertation, Microsoft Access database architecture in conjunction with Matlab have been used. Matlab is an efficient scientific program for the research community because of its simplistic and predefined coding structure. For the implementation of the biometric system in the real time domain, especially in the case of large scale databases, Object Oriented Programming language is recommended for use in the front end with the SQL or Oracle based database architecture in the back end. However, the details of the Object Oriented database architecture, implementation, and its processing methodology are beyond the scope of this dissertation.

Finally, the proposed Sequential Subspace Estimator (SSE) method has been tested with four state-of-the-art algorithms, namely the Kalman Filter, PCA, PCA-MLE, and PCA-Wiener. As well, it has been tested with the nonlinear (heterogeneous and nonstationary) "Put Face Database" and the less nonlinear (less heterogeneous and less nonstationary) "Indian Face Database". The experimental results have been presented and it is apparent from their outcome that the proposed method outperformed its counterparts. As well, the proposed MultiBiometrics encryption method is highly secure, since a multilayered authentication in the presence of the subject and authorized user must be performed in order to retrieve the biometrics and biographic features.

Appendix A

Possible Attacks

The main objective of this study is to extract quality biometric features that would otherwise be obstructed by nonstationary, nonlinear, and heterogeneous noise. It is also to protect the stored and dynamic biometric features against security, privacy, and unlinkability attacks. The following subsections address the possible attacks and the methodologies for protecting biometric features and systems against these attacks.

A.1 User Enrollment

The user enrollment process has been carried out under favorable conditions using fingerprint biometric features (minutiae points) at the central teminal. Fig. $A.1$ is a snapshot of Fig. 4.5 presented in Chapter 4 and shows the possible attacks on the user enrollment system.

In this process six different attacks have been considered. The details of these attacks and the security protections provided by the proposed MultiBiometrics method are discussed below:

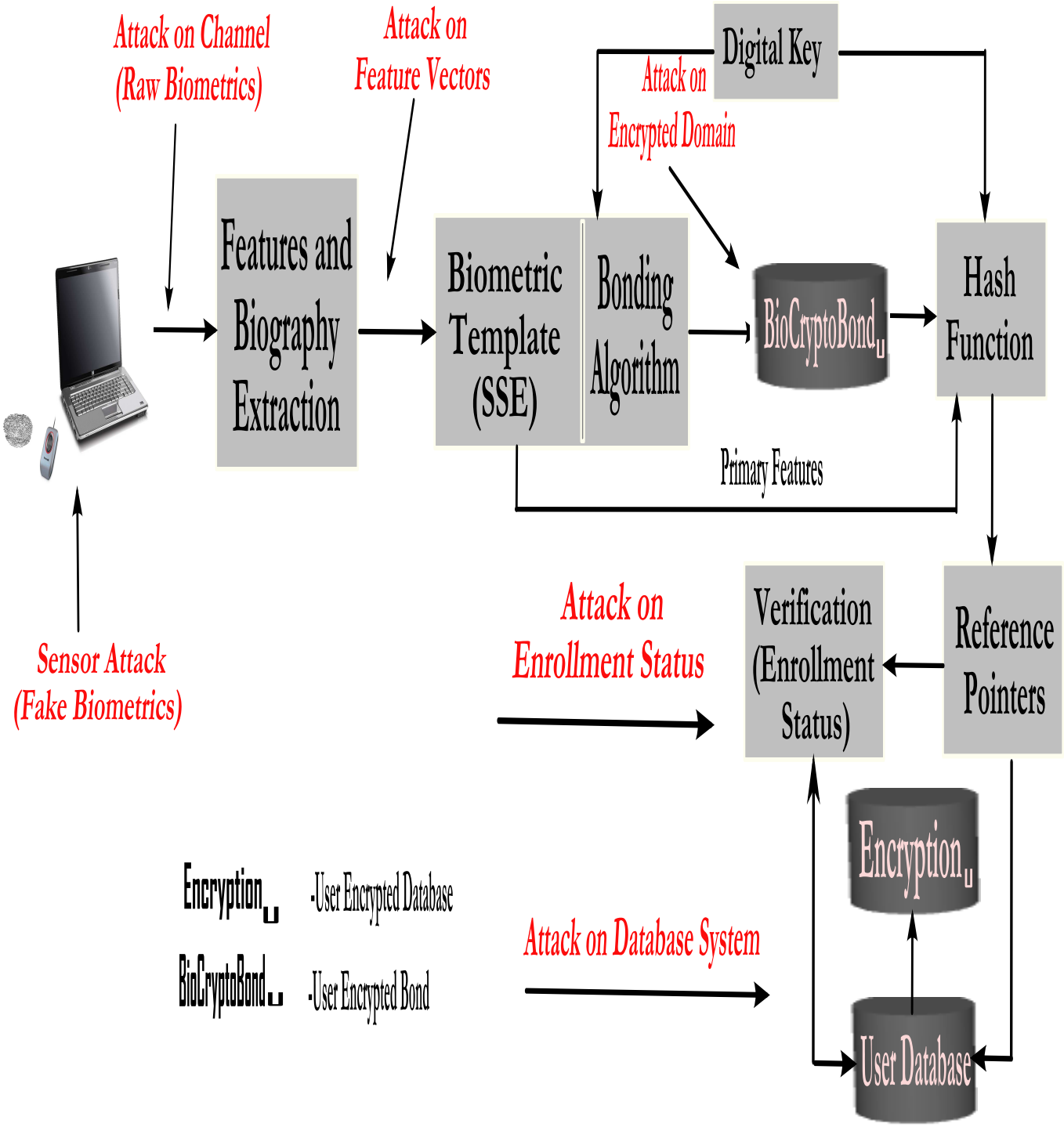


Figure A.1: Attacks on User Enrollment Process

A.1.1 Attack on Sensor

This type of attack is known as an attack on the biometric sensor. Here, the attackers present a fake biometrics that can imitate the authenticity of an authorized individual [116],[117].

Security Protection: This attack is performed before the implementation of the fusion and encryption method (see Fig. A.1). As mentioned before, in the proposed method the user biometric template is processed along with the digital secret key to cerate an encrypted bond and genrate a reference pointer. This reference pointer is then verified against the stored reference pointer before storing the biometrics (enrollment) into the database systems. Therefore, even if the attacker is able to present the fake biometrics, the system won't allow the attacker to complete the enrollment process. This is because the attacker needs to have the system specific reference pointer in order to process and store the user biometrics. However, the creation of this reference pointer without knowing the digital secret key and methodology for doing that is very tadious task. In the worst case scenario, the attacker is able to complete the enrollment using fake biometrics, but will still only have access to their own information and not the other users or subjects. The system is unlinkable as well, so access to the subject's information would require the physical presence of the subject in front of the authorized user.

A.1.2 Attack on Communication Channel

Sometimes this attack is combined with an attack on the biometric sensor. However, this attack is being considered to be an attack on the raw biometrics between the scanner and the feature extraction method. In this case, the attacker can intercept and relay the intercepted (i.e. stolen) biometrics to the feature extractor in order to bypass the biometric scanner [116],[117].

Security Protection: The proposed system is also protected against this type

of attack for the same reasons stated for attacks on sensors.

A.1.3 Attack on Feature Extraction Method

In this case, an attacker can replace the biometric features extraction method and implement a remotely controlled methodology to generate biometric templates [116],[117].

Security Protection: This attack is conducted before the implementation of the fusion process and encryption method. So, the system is also protected against this type of attack for the same reasons stated for attacks on the sensor.

A.1.4 Attack on Encrypted Domain

This attack is considered to be an attack on the cryptographic bond, which is the most vital stage of the MultiBiometrics encryption method. In this case, attackers can replace the encryption method with thier own remotely controlled method or can decrypt the encrypted bond to obtain the biometric features.

Security Protection: This attack can be performed in the encrypted domain at the time of encryption to replacee the encryption method, afterwards to decrypt the bond. If the encryption method is replaced by the attacker at the time of the encryption process, the newly created bond would be different. The resultant effect would be the creation of a system specific reference pointer required to process and store the user biometric template. If the attacker tries to decrypt the bond, they still won't be able to complete the enrollment process. To complete the enrollment process, the attacker has to recreate the encrypted bond using the proposed methodology. Even if the attacker is able to obtain the biometrics and other information from their unauthorized decryption process, they won't be able to obtain the original biometric features. This occurs because, in this encryption process, user fingerprint biometrics have been transformed as a function of orientation angle in the orthogonal domain. Afterwards, this tranformed biometric template is fused with the digital secret key

before the encrypted bond is created.

A.1.5 Attack on Enrollment Status

During attacks on the enrollment verification process, the attacker can override the user enrollment status or decisions made by the proposed system. In this case, the attacker can override two types of decisions: show the enrolled user hasn't been enrolled yet, and show the unenrolled user has already been enrolled.

Security Protection:

This is another vital stage of the enrollment process. If an attacker is able to override the first decision and complete the enrollment process, they won't be able to use this enrolled user to access the system. In this case, the attacker just overrides the dicision, not the reference pointer, even if the attackers use the fake reference pointer to create a new enrollment. It might be possible to have a duplicate entry for the user, but this duplicate entry won't effect the system's security and privacy. The system cannot read that reference pointer and the attacker cannot have access to the system, because the structure of the reference pointer generated during the authentication process would be completely different than the fake reference pointer. To override the second decision by the attacker would be long and tedious. Even if the attacker is able to generate fake reference pointer and tries to override the second decision, the system won't allow it, since the reference pointer has to match with the reference pointer stored in the system. In order to match, the attacker must have the authorized user fingerprint and successfully pass through the all of the attacks mentioned above. Therefore, this attack won't affect the system performance or the security and privacy of the biometrics. The worst case scenario would be if the enrollment status was successfully attacked; in this case, they would still only have access to their own information, not other users or subjects, for the same reasons discussed in Section A.1.1.

A.1.6 Attack on Database

Attacks on user biometric templates stored in the database system include the addition of a new template, modification of an existing template, or deletion of a template [116],[117].

Security Protection: In the proposed method, user information is being segmented and stored in two user databases: *User Database* (dB_u) and $Encryption_u$. The dB_u and $Encryption_u$ databases contain the user biographic and biometrics information, respectively. The link between two databases has been established by the reference pointer. This linking process is essential in order to have the complete user information. In this case, the attacker cannot add a new recond, since in order to do so, the attacker has to gererate a reference pointer through the process outlined in Chapter 4, and also must have the authorized user biometrics and biographics information. The attacker cannot modify or delete the existance or targeted template, since each user has two templates stored in two different databases. Without the reference pointer, the attacker cannot establish the relationship between the two databases, and without this relationship the attacker cannot locate and delete the the targeted templates. The system is unlinkable and multifactor authentication processes have to overcome this to access the database systems. A single point entry would not allow the attacker to access the system in order to add, modify, and delete the user.

A.2 Subject Enrollment

The subject enrollment process has been completed using the facial, fingerprint, and MultiBiometrics features. Possible attacks on the subject enrollment system are shown in Fig. *A*.2. Fig. *A*.2 is a snapshot of Fig. 4.6 presented in Chapter 4. Possible attacks and security protection of the subject's biometrics are the same that

for the user.

As well as the user's security protection, an authorized user must also be in the presence of the subject at the time of subject enrollment. In this case, the unlinkable multilayered encryption method is protected by a 32-bit digital key in conjunction with the reference pointer. Even if the attackers are be able to access the digital key and reference pointer, the original biometrics are not retrievable from the cryptographic bond. The extracted biometric features need to be transformed as a function of β before the bonding process occurs. In addition, the retrieval of subject information from the databases again requires the presence of the subject in front of the authorized user. The segmentation method is used to store subject biometrics and biographic information in the four subject databases. The Hot-Key function (see Chapter 4, Section 4.4.1) is used as a reference pointer to link between the subject databases. Furthermore, the reference table that contains the reference pointers only has address information representing the locations of the segmented subject record, not subject information. This makes the system unlinkable so that a single point entry would not allow the attacker to access unauthorized information from the databases or distinguish the identity of the subject from the received information.

A.3 Authentication

The possible attacks on the user authentication process are shown in Fig. $A.3$. Fig. $A.3$ is a snapshot of Fig. 4.7 presented in Chapter 4. The subject authentication is dependent on a successful user authentication process, and the types of attacks on it are almost the same. The details of the possible attacks and the security protection against these attacks have already been addressed in above sections.

In addition, the experimental results of the subject (and user) authentication process are presented in Section 4.6. User fingerprint biometrics have been used during

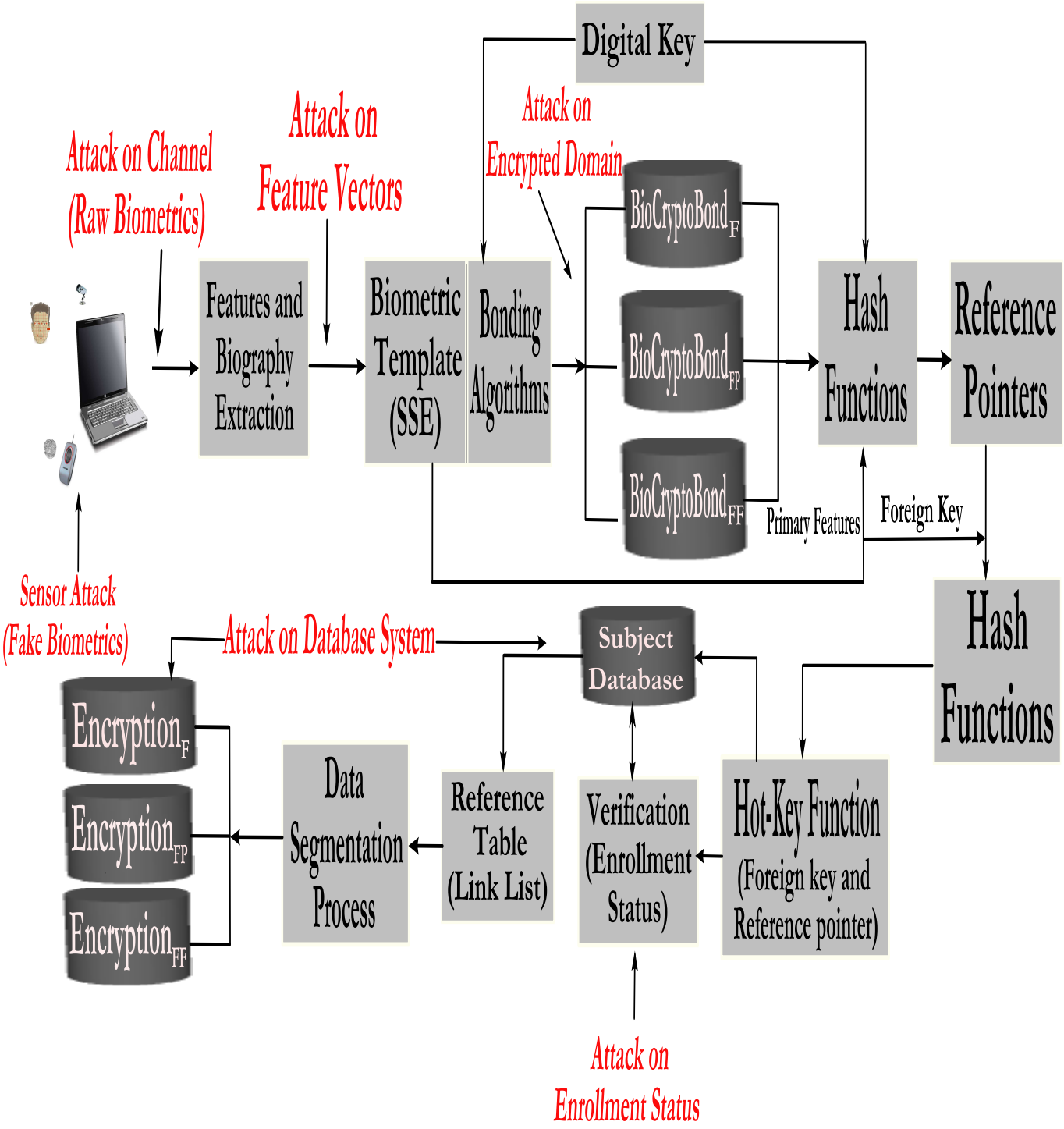


Figure A.2: Attacks on Subject Enrollment Process

the authentication process. If attackers are able to intervene at the sensor or communication channel, they still won't be able to access the system, since the biometric features need to be transformed as a function of the user fingerprint orientation angle before authentication occurs. Even if the attackers are able to obtain access to the system through a single point, they won't have the right to access other users' or subjects' information, since the biometric systems are unlinkable and the physical presence of the subject is required along with the user in order to retrieve the biometrics and biographic information. The databases are protected by multilayered encryption; hence single point access ability won't allow the attacker to retrieve unauthorized information or distinguish the identity of the subject (or user) from the received information.

Furthermore, the biometric information is segmented, and reference pointers are used to establish a link between them. In this method, it is not possible to obtain the original biometrics from these reference pointers and vice versa. As well, it is not possible to know the individual's identity or construct (or guess) the original biometric features of an individual from the segmented biometrics stored in the databases. Databases (or information) are segmented and transformed, and complete authorized processing is required in order to access the system. Therefore, this system is invincible to unlinkable attacks, and imposters cannot retrieve data based on information found in other parts of the system.

A.4 Tracking and Authentication

Fig. *A*.4 is a snapshot of Fig. 5.4 presented in Chapter 5. This tracking and authentication request is considered to be processed from a highly unfavorable environment, typically from a local terminal.

In the case of the tracking system, the extracted biometric features from the

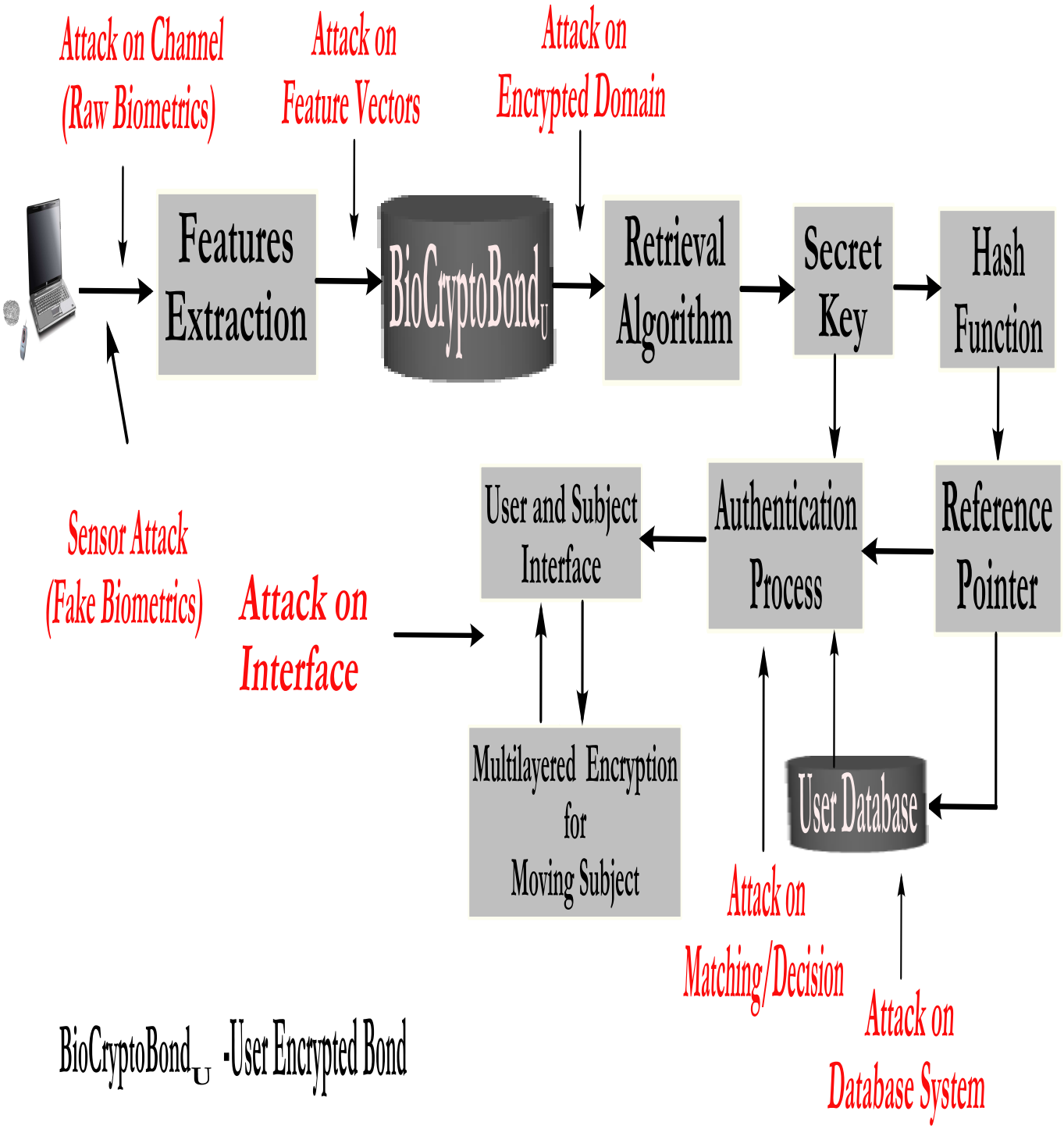


Figure A.3: Attacks on User Authentication Process

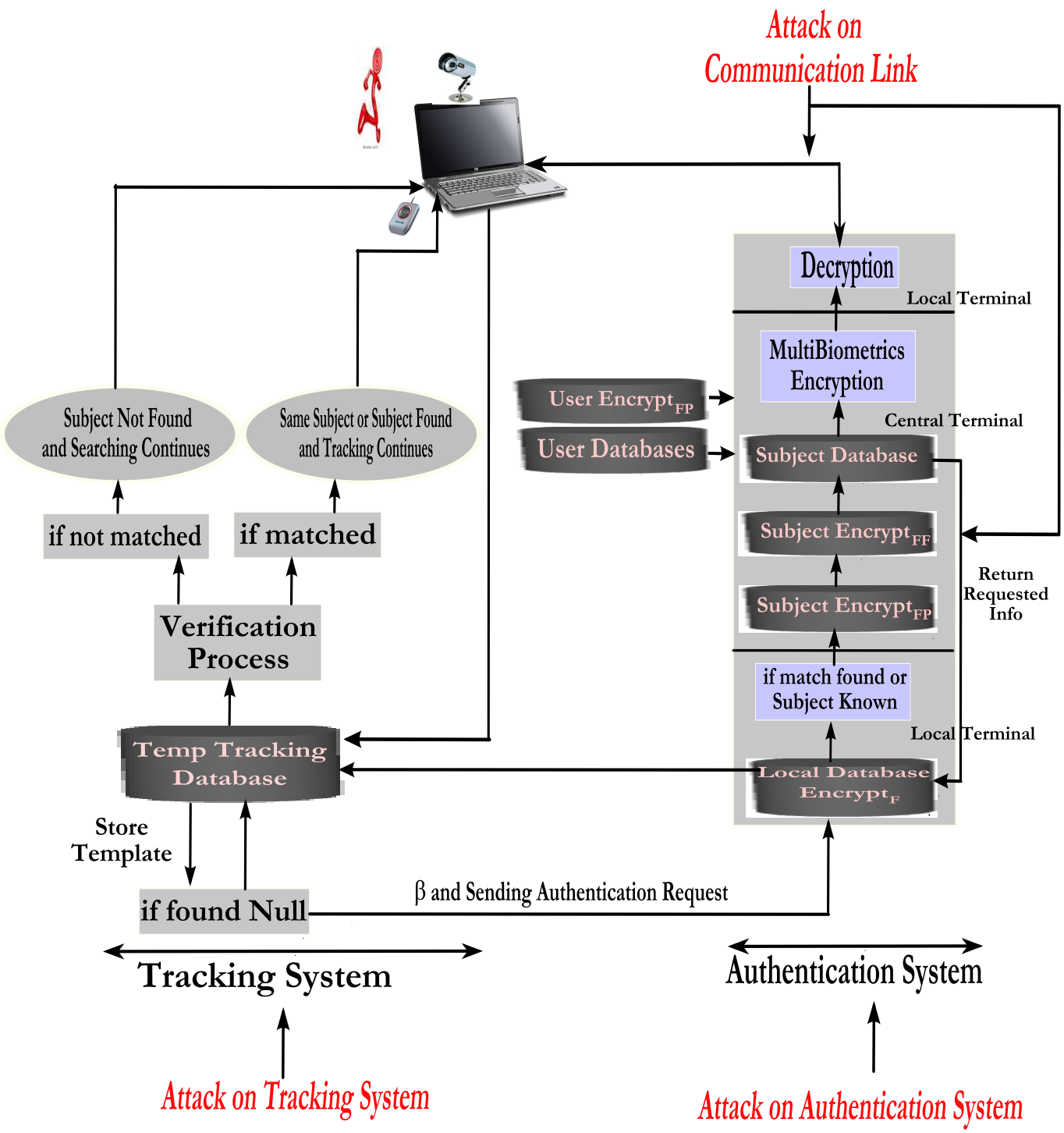


Figure A.4: Attacks on Tracking and Authentication Process

moving target (attack on the tracking system) are vulnerable to security, privacy, and unlinkability attacks. These attacks won't effect the privacy and security of the moving target in the surveillance zone, since the extracted information won't be permanently stored in the databases but will be deleted at the end of the tracking cycle. Furthermore, access to the temporary biometric features of the moving target won't give the attacker access to other parts of the system. Only the authentication request along with the facial biometric features of the suspected subject are sent from the tracking to the authentication system, where they face the multifactor authentication process.

Finally, the authentication system is protected by the multilayered and MultiBiometrics encryption method. The attacker cannot access the biometric system from any signal point entry. Even if the attackers are able to access the system, they cannot retrieve the original biometric features or distinguish the biometric information for the same reasons stated above. Furthermore, the requested biographic description of the subject sent through the communication channel is also protected from the attacks under consideration. The transmitted subject's information is unlinkable and encrypted by the user's transformed fingerprint biometrics at the central terminal before it is sent through the transmission channel. Therefore, attacks on the communication channel shown in Fig. $A.4$ could not allow the attackers to access the original biometrics information or other parts of the biometric system.

Appendix B

Hash-Function and Foreign Key

A hash function $\mathbb{H}$ is a mapping algorithm that projects an arbitrary length of a large data block to a data block of fixed (smaller) length. Typically, the hash system has two parts: bucket and directory [118]. A bucket is the physical address on the database that contains the records, and a directory contains the hash key and the reference pointer pointing to the bucket that contains the records. The hash function can be stated as follows:

$$\mathbb{H}(k) = k \ \% \ N \tag{B.1}$$

where %, k, and N are the MOD operator, the key value, and the number of buckets respectively.

In the proposed model, a $32-bit$ randomly generated key is hashed with primary biometric key features to create $16-bit$ reference pointers. Afterwards, reference pointers are used to access the database records. In this case, a one way cryptographic hash function is used, where the primary key features $\mathbb{I}$ are difficult to retrieve for $\mathbb{I}' \neq \mathbb{I}$ such that $\mathbb{H}(\mathbb{I}') = \mathbb{H}(\mathbb{I})$. The structure of the reference pointer is presented in Table: 1:

As previously mentioned, a primary key is a key that uniquely identifies a record or a subject (or user) in a database. The primary key is not shareable and cannot

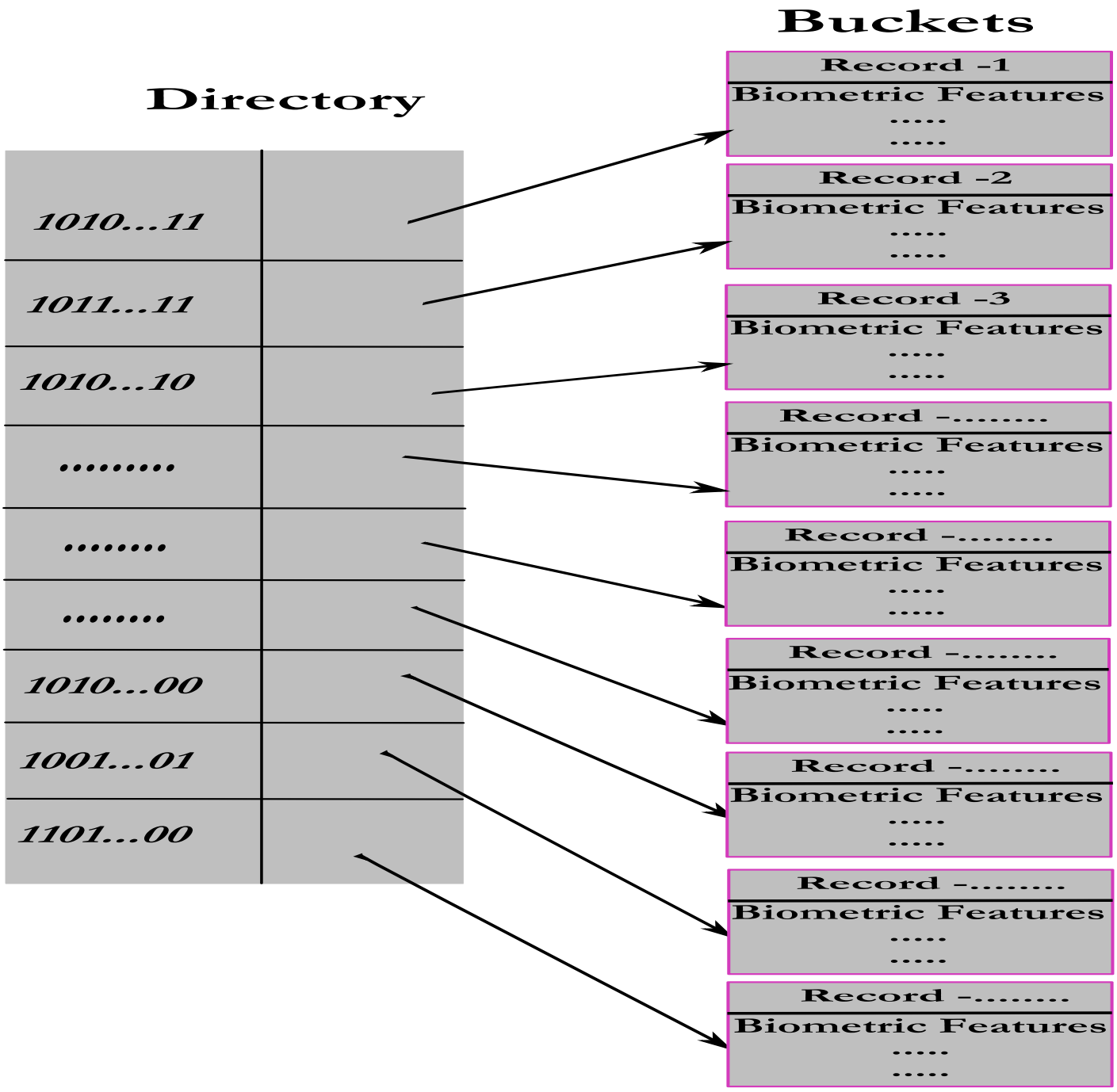


Figure B.1: Hashing Process

Table B.1: Reference Pointer Generation

Primary Features	32-bit Digital Key	16-bit Pointer
Subject/ User-1	011000...011	1010...11
Subject/ User-2	001011...010	0010...01
Subject/ User-3	101000...001	1101...10

be used (or assigned) by the other subject (or user). On the other hand, a foreign key is a field or a collection of fields of the database that are used with the primary key to establish links among the tables in the database system. The establishment of this type of relationship among the tables in the database system is known as the relational database system.

In this method, using the analogy of the relational database, the primary and foreign keys in conjunction with the reference pointers are used to create a link between the segmented databases. This structure allows the legitimate user to locate and access the database records without losing the data consistency, while at the same time protecting the security and privacy of the information. A typical structure of this relationship among the databases is presented in Fig. $B.2$ and Fig. $B.3$.

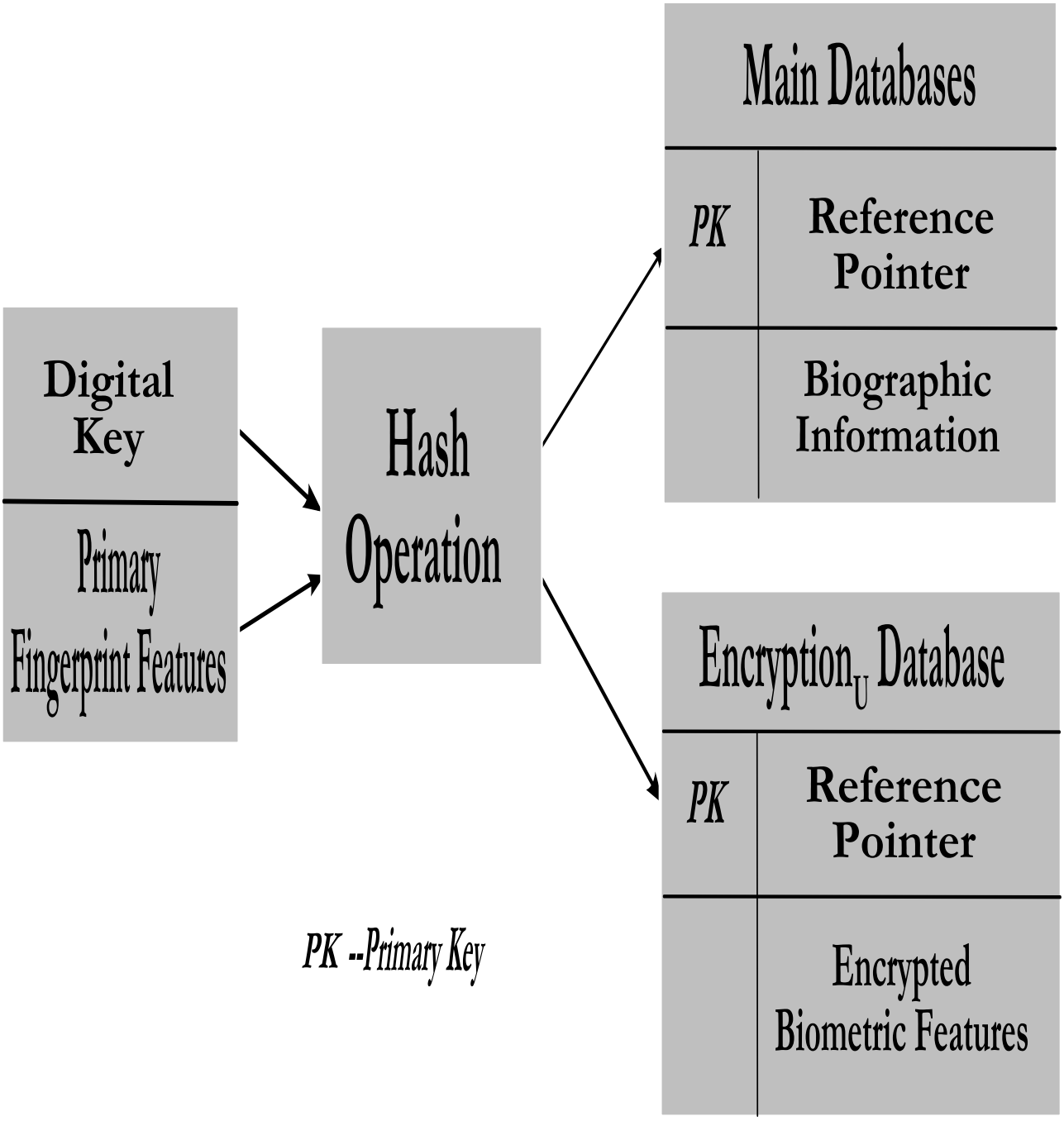


Figure B.2: Relational Database -Reference Key

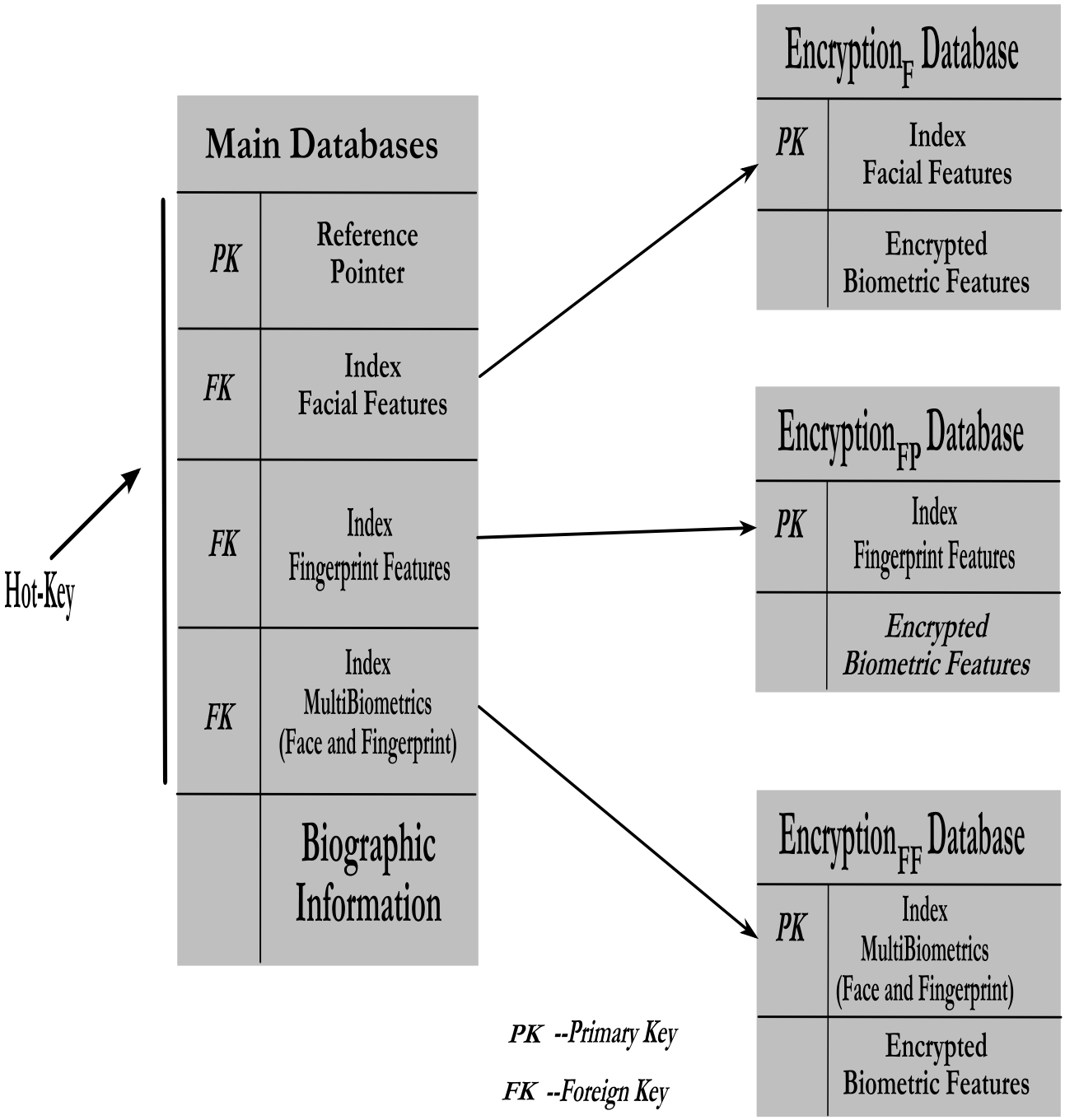


Figure B.3: Relational Database -Hot-Key

Appendix C

Experimental Data

Chapter -3 . Figure 3.12 (dB1)

False Acceptance Rate (FAR)

SSE	EKF	PCA	Wiener	MLE
0.995	0.995	0.995	0.995	0.995
0.994	0.995	0.995	0.995	0.995
0.994	0.995	0.995	0.995	0.995
0.993	0.995	0.995	0.995	0.995
0.993	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.985	0.984	0.995	0.995	0.995
0.98	0.96	0.995	0.995	0.995
0.95	0.92	0.995	0.995	0.995
0.89	0.78	0.995	0.975	0.995
0.78	0.71	0.99	0.928	0.974
0.678	0.61	0.958	0.872	0.921
0.378	0.317	0.781	0.712	0.803
0.177	0.2	0.712	0.51	0.597
0.101	0.12	0.41	0.34	0.39
0.07	0.06	0.31	0.25	0.24
0.041	0.041	0.241	0.18	0.17
0.03	0.02	0.202	0.101	0.123
0.01	0.005	0.138	0.0701	0.09
0.005	0.001	0.115	0.052	0.0801
0.001	0.001	0.111	0.041	0.059
0.001	0.001	0.091	0.021	0.039
0.0005	0.0005	0.072	0.011	0.026
0.0005	0.0005	0.051	0.005	0.011
0.0005	0.0005	0.031	0.005	0.005
0.0005	0.0005	0.015	0.0005	0.001
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0001	0.0005
0.0005	0.0005	0.0005	0.0001	0.0005
0.0005	0.0005	0.0005	0.0001	0.0005
0.0005	0.0005	0.0005	0.0001	0.0005
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001

Chapter -3 . Figure 3.12 (dB1)

False Rejection Rate (FRR)

SSE	EKF	PCA	Wiener	MLE
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.001	0.0001	0.0001	0.0001
0.001	0.002	0.0001	0.0001	0.0001
0.001	0.003	0.01	0.0001	0.0001
0.004	0.003	0.02	0.01	0.01
0.008	0.005	0.031	0.02	0.021
0.01	0.007	0.043	0.025	0.033
0.0172	0.01	0.051	0.032	0.047
0.0192	0.0256	0.072	0.044	0.058
0.046	0.046	0.096	0.067	0.081
0.13	0.083	0.109	0.081	0.111
0.226	0.136	0.177	0.17	0.185
0.322	0.262	0.322	0.292	0.311
0.623	0.523	0.603	0.573	0.61
0.725	0.689	0.789	0.819	0.859
0.875	0.819	0.961	0.92	0.94
0.941	0.91	0.995	0.96	0.97
0.966	0.955	0.995	0.99	0.995
0.981	0.97	0.995	0.995	0.995
0.99	0.98	0.995	0.995	0.995
0.99	0.989	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995

Figure C.1: Experimental Data -Chapter-3 (Fig. 12)

Chapter -3 . Figure 3.13 (dB2)

False Acceptance Rate (FAR)

SSE	EKF	PCA	Wiener	MLE
0.998	0.995	0.995	0.995	0.995
0.998	0.995	0.995	0.995	0.995
0.996	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.994	0.994	0.995	0.995	0.995
0.993	0.992	0.995	0.995	0.995
0.991	0.991	0.995	0.995	0.995
0.99	0.99	0.995	0.995	0.995
0.987	0.981	0.995	0.995	0.995
0.98	0.977	0.995	0.995	0.995
0.978	0.962	0.995	0.995	0.995
0.95	0.86	0.995	0.995	0.995
0.78	0.73	0.995	0.982	0.992
0.686	0.61	0.982	0.957	0.971
0.55	0.49	0.971	0.88	0.92
0.45	0.33	0.898	0.69	0.73
0.152	0.126	0.49	0.521	0.481
0.07	0.05	0.37	0.301	0.251
0.03	0.02	0.291	0.119	0.154
0.015	0.01	0.172	0.071	0.11
0.01	0.0005	0.121	0.055	0.061
0.0005	0.0005	0.08	0.04	0.051
0.0005	0.0005	0.043	0.013	0.024
0.0005	0.0005	0.022	0.008	0.01
0.0005	0.0005	0.001	0.0005	0.0009
0.0005	0.0005	0.0005	0.0005	0.0006
0.0005	0.0005	0.0005	0.0003	0.0005
0.0005	0.0005	0.0005	0.0003	0.0005
0.0005	0.0005	0.0005	0.0001	0.0005
0.0001	0.0001	0.0001	0.0001	0.0003
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001

Chapter -3 . Figure 3.13 (dB2)

False Rejection Rate (FRR)

SSE	EKF	PCA	Wiener	MLE
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.001	0.0001	0.0001
0.001	0.0001	0.001	0.0001	0.0001
0.001	0.0001	0.002	0.0001	0.0001
0.002	0.0001	0.003	0.0001	0.0001
0.002	0.001	0.005	0.0001	0.0001
0.003	0.002	0.006	0.0001	0.0001
0.004	0.003	0.008	0.0001	0.001
0.006	0.004	0.011	0.02	0.021
0.009	0.006	0.023	0.025	0.022
0.0172	0.007	0.031	0.032	0.029
0.0192	0.0121	0.052	0.044	0.039
0.028	0.0187	0.081	0.057	0.057
0.031	0.021	0.105	0.071	0.069
0.034	0.023	0.116	0.11	0.095
0.0381	0.0287	0.137	0.13	0.151
0.091	0.0623	0.179	0.245	0.245
0.38	0.18	0.789	0.619	0.71
0.56	0.439	0.956	0.87	0.89
0.79	0.691	0.995	0.96	0.98
0.896	0.84	0.995	0.99	0.995
0.96	0.91	0.995	0.99	0.995
0.98	0.94	0.995	0.995	0.995
0.99	0.97	0.995	0.995	0.995
0.99	0.981	0.995	0.995	0.995
0.99	0.99	0.995	0.995	0.995
0.99	0.99	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995

Figure C.2: Experimental Data -Chapter-3 (Fig. 13)

Chapter -3 . Figure 3.14 (dB3)

False Acceptance Rate (FAR)

SSE	EKF	PCA	Wiener	MLE
0.998	0.995	0.995	0.995	0.995
0.998	0.995	0.995	0.995	0.995
0.996	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.994	0.995	0.995	0.995	0.995
0.993	0.99	0.995	0.995	0.995
0.991	0.988	0.995	0.995	0.995
0.99	0.9841	0.995	0.995	0.995
0.989	0.979	0.995	0.995	0.995
0.986	0.965	0.995	0.995	0.995
0.982	0.96	0.995	0.995	0.995
0.979	0.95	0.995	0.995	0.995
0.96	0.92	0.995	0.995	0.995
0.93	0.75	0.995	0.995	0.995
0.65	0.42	0.995	0.985	0.99
0.45	0.22	0.975	0.965	0.98
0.188	0.12	0.914	0.914	0.92
0.11	0.067	0.819	0.801	0.85
0.06	0.035	0.71	0.72	0.75
0.04	0.02	0.549	0.615	0.579
0.019	0.01	0.351	0.391	0.344
0.012	0.0005	0.21	0.18	0.21
0.008	0.0005	0.129	0.11	0.119
0.005	0.0005	0.092	0.072	0.085
0.0005	0.0005	0.05	0.03	0.04
0.0005	0.0005	0.03	0.018	0.02
0.0005	0.0005	0.02	0.0005	0.012
0.0005	0.0005	0.015	0.0005	0.011
0.0005	0.0005	0.01	0.0005	0.004
0.0001	0.0001	0.0005	0.0005	0.0005
0.0001	0.0001	0.0004	0.0004	0.0004
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001

Chapter -3 . Figure 3.14 (dB3)

False Rejection Rate (FRR)

SSE	EKF	PCA	Wiener	MLE
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.001	0.0001	0.0001
0.0001	0.0001	0.002	0.0001	0.0001
0.0001	0.0001	0.005	0.001	0.002
0.0001	0.0001	0.006	0.001	0.003
0.0001	0.0001	0.009	0.002	0.005
0.0001	0.0001	0.025	0.009	0.008
0.0001	0.0001	0.037	0.014	0.011
0.001	0.0001	0.048	0.021	0.018
0.007	0.0001	0.053	0.043	0.04
0.009	0.0002	0.06	0.054	0.06
0.012	0.004	0.072	0.066	0.065
0.0172	0.005	0.085	0.075	0.074
0.0192	0.007	0.091	0.079	0.078
0.027	0.014	0.11	0.095	0.105
0.031	0.017	0.126	0.11	0.12
0.034	0.03	0.14	0.12	0.132
0.039	0.036	0.153	0.131	0.141
0.056	0.078	0.171	0.152	0.162
0.12	0.1323	0.19	0.172	0.18
0.21	0.21	0.232	0.198	0.21
0.375	0.319	0.31	0.269	0.279
0.51	0.41	0.489	0.519	0.529
0.646	0.52	0.781	0.681	0.698
0.7354	0.71	0.91	0.831	0.891
0.81	0.78	0.98	0.91	0.95
0.87	0.83	0.995	0.955	0.975
0.915	0.88	0.995	0.985	0.995
0.94	0.91	0.995	0.995	0.995
0.97	0.94	0.995	0.995	0.995
0.98	0.965	0.995	0.995	0.995
0.99	0.975	0.995	0.995	0.995
0.99	0.98	0.995	0.995	0.995
0.99	0.985	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995

Figure C.3: Experimental Data -Chapter-3 (Fig. 14)

	Chapter -3 . Figure 3.15 (dB5)					Chapter -3 . Figure 3.15 (dB5)				
	False Acceptance Rate (FAR)					**False Rejection Rate (FRR)**				
	SSE	**EKF**	**PCA**	**Wiener**	**MLE**	**SSE**	**EKF**	**PCA**	**Wiener**	**MLE**
	0.995	0.995	0.995	0.995	0.995	0.0001	0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.994	0.995	0.0001	0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.994	0.995	0.0001	0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.994	0.994	0.0001	0.0001	0.0001	0.0001	0.0001
	0.993	0.99	0.995	0.994	0.994	0.0001	0.0001	0.0001	0.0001	0.0001
	0.992	0.985	0.994	0.991	0.992	0.0001	0.0001	0.0001	0.0001	0.0001
	0.98	0.968	0.993	0.982	0.987	0.0001	0.0001	0.0001	0.0001	0.0001
	0.963	0.943	0.991	0.974	0.979	0.0001	0.0001	0.0001	0.0001	0.0001
	0.93	0.918	0.975	0.951	0.96	0.0001	0.0001	0.0001	0.0001	0.0001
	0.782	0.781	0.952	0.892	0.891	0.0001	0.0001	0.0001	0.0001	0.0001
	0.689	0.692	0.885	0.782	0.801	0.0007	0.0005	0.0001	0.0001	0.0001
	0.612	0.616	0.788	0.715	0.711	0.001	0.001	0.0017	0.001	0.0018
	0.301	0.291	0.605	0.474	0.512	0.002	0.001	0.001	0.001	0.001
	0.228	0.224	0.502	0.397	0.425	0.004	0.004	0.008	0.004	0.006
	0.111	0.113	0.427	0.284	0.271	0.006	0.005	0.011	0.007	0.01
	0.071	0.068	0.291	0.135	0.211	0.008	0.006	0.013	0.01	0.009
	0.041	0.043	0.175	0.11	0.102	0.012	0.012	0.031	0.017	0.021
	0.024	0.011	0.109	0.059	0.081	0.0156	0.0149	0.052	0.0192	0.039
	0.005	0.001	0.065	0.041	0.052	0.027	0.028	0.076	0.048	0.062
	0.001	0.001	0.057	0.014	0.031	0.058	0.054	0.109	0.129	0.106
	0.001	0.001	0.031	0.011	0.016	0.106	0.105	0.177	0.226	0.181
	0.001	0.001	0.019	0.006	0.009	0.262	0.262	0.322	0.322	0.301
	0.0005	0.0005	0.01	0.001	0.005	0.523	0.519	0.643	0.623	0.601
	0.0005	0.0005	0.008	0.0005	0.004	0.689	0.683	0.789	0.725	0.71
	0.0005	0.0005	0.005	0.0005	0.002	0.819	0.817	0.971	0.895	0.925
	0.0005	0.0005	0.001	0.0005	0.0001	0.91	0.94	0.995	0.961	0.975
	0.0005	0.0005	0.0005	0.0005	0.0005	0.955	0.966	0.995	0.981	0.99
	0.0005	0.0005	0.0005	0.0005	0.0005	0.97	0.979	0.995	0.99	0.992
	0.0005	0.0005	0.0005	0.0005	0.0005	0.98	0.985	0.995	0.99	0.993
	0.0005	0.0005	0.0005	0.0005	0.0005	0.989	0.995	0.995	0.99	0.993
	0.0005	0.0005	0.0005	0.0005	0.0005	0.995	0.995	0.995	0.99	0.994
	0.0005	0.0005	0.0005	0.0005	0.0005	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0005	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0004	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0001	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0001	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0001	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0001	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0001	0.995	0.995	0.995	0.99	0.995
	0.0001	0.0001	0.0001	0.0001	0.0001	0.995	0.995	0.995	0.99	0.995

Figure C.4: Experimental Data -Chapter-3 (Fig. 15)

Chapter 4

False Acceptance Rate (FAR)				
Fig 4.9 (User) (CASIA)	Fig 4.10 20 Subjects (Put Face)	Fig 4.11 40 Subjects (Put Face)	Fig 4.12 10 Subjects (Indian Face)	Fig 4.13 20 Subjects (Indian Face)
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.994	0.995	0.995	0.995	0.995
0.99	0.995	0.995	0.995	0.995
0.98	0.995	0.995	0.993	0.995
0.971	0.995	0.995	0.992	0.995
0.962	0.995	0.995	0.98	0.995
0.95	0.995	0.995	0.975	0.995
0.91	0.995	0.995	0.94	0.99
0.782	0.99	0.995	0.882	0.955
0.689	0.9871	0.995	0.789	0.94
0.57	0.98	0.995	0.712	0.912
0.301	0.975	0.989	0.501	0.801
0.228	0.96	0.98	0.328	0.72
0.09	0.95	0.961	0.209	0.61
0.036	0.92	0.91	0.086	0.41
0.015	0.75	0.83	0.045	0.23
0.008	0.42	0.51	0.024	0.11
0.003	0.22	0.32	0.015	0.05
0.005	0.12	0.23	0.005	0.02
0.001	0.057	0.145	0.001	0.01
0.001	0.015	0.075	0.001	0.007
0.0005	0.005	0.014	0.0005	0.002
0.0005	0.001	0.0011	0.0005	0.0008
0.0005	0.0005	0.001	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0005	0.0005	0.0005	0.0005	0.0005
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001

Chapter 4

False Rejection Rate (FRR)				
Fig 4.9 (User) (CASIA)	Fig 4.10 20 Subjects (Put Face)	Fig 4.11 40 Subjects (Put Face)	Fig 4.12 10 Subjects (Indian Face)	Fig 4.13 20 Subjects (Indian Face)
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.002	0.0001	0.0001
0.0001	0.0001	0.0002	0.0007	0.0009
0.0001	0.0001	0.0003	0.001	0.002
0.0001	0.0001	0.0004	0.002	0.003
0.0001	0.0002	0.0005	0.004	0.004
0.0003	0.003	0.007	0.006	0.006
0.008	0.004	0.009	0.01	0.011
0.021	0.007	0.014	0.022	0.016
0.033	0.012	0.012	0.031	0.021
0.065	0.015	0.015	0.04	0.029
0.127	0.025	0.021	0.087	0.055
0.18	0.031	0.029	0.18	0.191
0.259	0.072	0.042	0.359	0.351
0.425	0.112	0.086	0.425	0.441
0.605	0.19	0.18	0.611	0.56
0.719	0.319	0.321	0.739	0.641
0.78	0.41	0.63	0.79	0.731
0.82	0.52	0.75	0.83	0.811
0.866	0.71	0.87	0.896	0.878
0.91	0.85	0.982	0.93	0.938
0.94	0.9	0.995	0.95	0.97
0.956	0.93	0.995	0.966	0.982
0.967	0.98	0.995	0.977	0.99
0.975	0.99	0.995	0.985	0.995
0.98	0.99	0.995	0.98	0.995
0.99	0.995	0.995	0.99	0.995
0.991	0.995	0.995	0.992	0.995
0.992	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995
0.995	0.995	0.995	0.995	0.995

Figure C.5: Experimental Data -Chapter-4

		Chapter 5							Chapter 5	
False Acceptance Rate (FAR)						False Rejection Rate (FRR)				
	Fig 5.5	Fig 5.6	Fig 5.7	Fig 5.8			Fig 5.5	Fig 5.6	Fig 5.7	Fig 5.8
	(Temp Track)	Fingerprint M	MultiBiometrics	Subject-dB			(Temp Track)	Fingerprint M	MultiBiometrics	Subject-dB
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.995	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.991	0.995	0.995	0.995			0.0001	0.0001	0.0001	0.0001
	0.98	0.995	0.991	0.995			0.0001	0.0001	0.0002	0.0001
	0.972	0.991	0.981	0.995			0.0001	0.0002	0.0003	0.0001
	0.955	0.983	0.972	0.99			0.0004	0.0004	0.0005	0.0002
	0.875	0.971	0.94	0.982			0.0009	0.001	0.002	0.0003
	0.578	0.951	0.89	0.972			0.002	0.003	0.004	0.0005
	0.411	0.871	0.824	0.943			0.006	0.007	0.0065	0.002
	0.21	0.601	0.69	0.88			0.02	0.01	0.011	0.004
	0.101	0.453	0.373	0.811			0.035	0.019	0.015	0.0065
	0.05	0.18	0.221	0.68			0.055	0.031	0.021	0.011
	0.026	0.06	0.12	0.372			0.11	0.0411	0.0291	0.015
	0.019	0.015	0.053	0.22			0.22	0.0762	0.035	0.021
	0.012	0.005	0.014	0.119			0.31	0.14	0.041	0.0291
	0.006	0.001	0.005	0.051			0.375	0.215	0.0525	0.035
	0.003	0.0008	0.0008	0.016			0.519	0.419	0.097	0.041
	0.001	0.0009	0.0009	0.005			0.68	0.528	0.227	0.05
	0.0009	0.001	0.0009	0.0008			0.76	0.629	0.431	0.077
	0.0009	0.0009	0.0009	0.0009			0.866	0.726	0.659	0.187
	0.0005	0.0009	0.0009	0.0009			0.93	0.83	0.781	0.431
	0.0005	0.0009	0.0009	0.0009			0.961	0.911	0.852	0.621
	0.0005	0.0005	0.0005	0.0009			0.976	0.956	0.91	0.751
	0.0005	0.0005	0.0005	0.0009			0.984	0.974	0.954	0.852
	0.0001	0.0005	0.0005	0.0005			0.986	0.981	0.971	0.91
	0.0001	0.0005	0.0005	0.0005			0.989	0.991	0.982	0.952
	0.0001	0.0001	0.0001	0.0005			0.992	0.994	0.987	0.969
	0.0001	0.0001	0.0001	0.0005			0.993	0.994	0.992	0.982
	0.0001	0.0001	0.0001	0.0001			0.994	0.994	0.993	0.987
	0.0001	0.0001	0.0001	0.0001			0.995	0.994	0.993	0.992
	0.0001	0.0001	0.0001	0.0001			0.995	0.994	0.994	0.993
	0.0001	0.0001	0.0001	0.0001			0.995	0.995	0.993	0.991

Figure C.6: Experimental Data -Chapter-5

Lips

159	166	164	159	154	151	151	153	155	156	154	155	156	154	153	153	155	158	
162	170	171	166	161	159	159	160	158	156	153	154	155	155	155	155	156	156	
160	166	164	159	154	154	156	157	153	149	154	153	153	154	156	157	156	155	
166	166	163	157	153	154	161	165	165	162	158	155	151	151	154	156	157	157	
164	157	143	138	133	136	144	154	159	160	157	153	148	146	147	152	157	160	
132	122	117	113	109	110	116	125	134	138	145	144	142	140	141	146	155	162	
110	105	120	119	116	112	111	115	122	127	124	129	134	135	136	142	153	162	
123	127	120	121	118	112	104	102	106	110	107	117	128	133	134	140	151	161	
117	113	111	116	119	116	108	101	99	99	97	102	110	116	123	131	141	148	
136	137	133	136	138	133	125	118	116	116	103	103	102	103	110	123	138	150	
143	146	142	144	144	141	134	129	128	129	126	123	118	115	119	130	144	154	
147	147	145	147	148	146	143	141	142	143	150	148	146	144	144	147	150	153	
162	160	160	160	161	160	159	158	159	159	156	155	154	153	152	151	150	149	

Eyes

183	179	184	186	178	173	179	177	173	179	174	179	185	185	182	178	177	178	179	177	175	175		
161	156	160	171	174	179	189	186	178	179	177	175	174	176	179	179	176	173	168	172	175	176		
128	130	133	142	144	148	158	158	154	160	181	173	166	169	177	180	174	166	163	168	172	172		
128	127	137	146	148	151	163	167	168	177	177	170	165	168	177	178	171	162	166	166	165	162		
96	79	94	106	112	119	134	140	144	155	160	160	163	169	175	175	169	164	164	161	157	154		
112	108	103	107	99	95	105	115	129	147	146	151	159	167	172	172	169	166	155	154	151	147		
107	107	123	124	112	100	102	106	116	133	152	155	161	167	170	170	167	164	152	153	150	140		
129	124	116	131	138	139	140	129	118	121	169	167	166	169	171	170	165	160	156	158	152	133		
136	145	140	143	143	145	152	154	137	116	144	130	173	149	119	113	148	127	163	124	134	124		
139	147	133	137	139	142	151	156	145	129	234	161	172	76	107	96	82	70	118	94	126	120		
102	107	129	135	139	142	153	164	160	150	97	173	131	165	163	156	167	177	160	130	137	100		
111	111	122	129	135	139	150	163	165	157	113	154	150	151	175	168	156	166	159	150	148	115		
110	106	111	120	126	130	141	154	154	146	165	174	164	172	176	188	183	171	153	161	147	130		
124	113	111	119	126	132	143	151	146	133	143	195	167	221	153	160	177	158	171	177	155	142		
126	109	115	124	132	140	151	156	143	124	184	155	205	163	171	186	173	177	151	156	163	160		
134	113	115	123	132	142	154	157	138	115	169	182	181	184	178	192	172	173	180	157	159	134		
116	104	108	114	125	149	169	166	138	109	176	181	187	190	187	182	178	175	158	159	164	167		
124	119	130	133	133	143	150	151	124	127	177	181	187	189	187	182	177	175	174	169	164	157		
121	120	138	141	136	141	143	149	116	158	178	182	187	188	186	181	177	176	174	169	162	154		
120	121	135	140	136	146	152	155	112	169	180	183	187	187	185	181	178	177	168	168	168	164		
132	137	138	141	134	145	159	150	113	161	183	186	188	188	185	181	179	179	174	173	174	170		
139	146	138	142	134	140	157	135	134	168	187	188	190	188	185	182	181	181	174	170	166	163		
139	142	137	153	152	149	157	117	162	182	190	191	191	189	186	184	183	183	173	166	160	159		
144	141	146	174	180	167	161	99	172	180	192	192	192	190	187	184	184	185	179	172	166	166		
152	155	174	155	155	125	119	130	180	188	195	194	191	189	186	184	183	182	174	173	174	166		

Figure C.7: Sample of Extracted Data (Grayscale) -Chapter-3 (Section-3.3)

Bibliography

[1] A. Jain and A. Kumar, "Biometrics history", Available: http://www.biometrics.gov-documents-biohistory.pdf, pp. 127, Oct. 2012.

[2] D. Stinson, "Cryptography: theory and practice", Ed.: 3rd, Chapman Hall/CRC Press Inc., Jan. 2006.

[3] D. Moss, "FBI techs shy away from facial recognition: spends 40 years losing face", Internet: www.theregister.co.uk-2009-11-03-fbio-face-recognition, [Nov. 2012].

[4] J. Klontz and A. Jain, "A case study of automated face recognition: The Boston Marathon bombings suspects", IEEE Security and Privacy, Nov. 2013.

[5] A. Menezes, P. Oorschot, and S. Stone, "Handbook of applied cryptography", Ed.: CRC press, Mar. 2006.

[6] Y. Imamverdiev and L. Sukhostat, "A method for cryptographic key generation from fingerprints", Automatic Control and Computer Sciences, vol. 46, no. 2, pp. 66-75, Apr. 2012.

[7] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, "Handbook of fingerprint recognition", Ed.: 2nd, Springer, Sep. 2009.

[8] B. Rosistem, "Fingerprint feature extrcation", Internet: http://www.barcode.ro/tutorials/biometrics/fingerprint.html, [Dec. 2011].

[9] J. Lee, "Technical definition and description: Fingerprint identification", Internet: http://www.personal.psu.edu/jbl5036/blogs/engl202c/technical-definition-description.html, [Dec. 2011].

[10] Griaule Biometrics, "Orientation map extraction", Internet: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/types/feature-extraction/orientation, [Nov. 2012].

[11] "Fingerprint singular points detection", Internet: http://biostar.fe.up.pt/Projects.html, [Nov. 2012].

[12] E. Kremic and A. Subasi, "The implementation of face security for authentication implemented on mobile phone", The International Arab Journal of Information Technology, pp. 1-6, Sep. 2011.

[13] C. Le and R. Jain, "A survey of biometrics security systems", Internet: http://www.cse.wustl.edu/ jain/cse571-11/ftp/biomet/, [Oct. 2013].

[14] M. Kelly, "Biometric Identification", Internet: http://vceit.com/p/biometric-index.htm, [Oct. 2013].

[15] E. Chabrow, "Iris recognition: NIST computer scientist patric grother", Available: http://www.bankinfosecurity.com/interviews/iris-recognition-nist-computer-scientist-patrick-grother-i-368, Nov. 2009, [Oct. 2013].

[16] M. Veen, T. Kevenaar, G. Schrijen, T. Akkermans, and F. Zuo, "Face biometrics with renewable templates", SPIE Proceedings-Security, Steganography, and wantermarking of Multimedia, vol. 6072, pp. 1-12, Jan. 2006.

[17] K. Bowyer, K. Chang, P. Flynn, and X. Chen, "Face recognition using 2-D, 3-D, and infrared: Is multimodal better than multisample?", IEEE Proceeding-Invited Paper, vol. 94, no. 11, Nov. 2006.

[18] "Facial recognition biometrics", Internet: http://www.myfingerprintreader.com/category/facial-recognition-biometrics, Oct. 2011, [Jan. 2012].

[19] M. Lane, "BBC News: Can you tell who it is yet?", Available: http://news.bbc.co.uk/2/hi/uk-news/magazine/6981500.stm, Sep. 2007, [Jan. 2011].

[20] "Detection, Inspection, and Enforcement", Internet: http://www.nist.gov/mml/mmsd/security-technologies/dietbiom.cfm, Oct. 2012, [Jan. 2013].

[21] B. Bhanu and X. Zhou, "Feature fusion of side face and gait for video-based human identification", ELSEVIER Journal of Pattern the Recognition Society, vol. 41, pp. 778-795, Feb. 2008.

[22] H. Lu, J. Wang, and K. Plataniotis, "A review on face and gait recognition: system, data, and algorithms", Department of electrical and Computer Engineering University of Toronto, Canada, Apr. 2008.

[23] H. Lu, K. Plataniotis, and A. Venetsanopoulos, "A layered deformable model for gait analysis", Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition, Southampton, UK, pp. 249-254, UK, Apr. 2006.

[24] J. Boyd and J. Little, "Gait Recognition", Internet: http://www.springerreference.com/docs/html/chapterdbid/70822.html, [Oct. 2013].

[25] "Biometrics France", Internet: http://www.contemplas.com/motion-analysis-partner/biometrics-france.aspx, [Nov. 2013].

[26] "Gait", Internet: http://fingerchip.pagesperso-orange.fr/biometrics/types/gait.htm, [Nov. 2013].

[27] D. Royer, "A study on PKI and biometrics: Soft biometrics", Internet: http://www.fidis.net/resources/deliverables/hightechid/int-d32000/doc/21/, [Jan. 2014].

[28] A. Cavoukian and T. Marinelli, "Privacy-protective facial recognition: biometric encryption proof of concept", Information and Privacy Commissioner, Ontario, Canada. Nov. 2010.

[29] A. Cavoukian and A. Stoianov, "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy", Information and Privacy Commissioner Ontario, Mar. 2007.

[30] G. Salvendy and M. Smith, "Human Interface and the management of information: Information and interaction", Springer, Sep. 2009.

[31] S. Mayhew, "Special report: Biometrics and national security", Biometrics Research Group Inc., Mar. 2014.

[32] T. Sabareeswari and S. Stuwart, "Identification of a person using multimodal biometric system", International Journal of Computer Applications", vol. 3, no. 9, pp. 12-16 Jul. 2010.

[33] M. Elalami, A. Amin, and A. El-alfi, "A personal identification framework based on facial image and fingerprint fusion biometric", International Journal of Computer Application, vol. 51, no. 7, pp. 41-48, Aug. 2012.

[34] S. Prabhakar, S. Prankanti and A. Jain,"Biometric recognition: security and privacy concerns ", IEEE Security and Privacy, Published by IEEE Computer Society, pp. 33-42, Last Update Oct. 2013.

[35] D. Zizhe, Z. Xianda, and Z. Xiaolong, "Nonlinear Principal Component Analysis using Strong Tracking Filter", Tsinghua Science and Technology, vol. 12, no. 6, pp. 652-657, Dec. 2007.

[36] "A face recognition", National Science and Technology Council, Tech. Rep., Apr. 2006.

[37] "Biometrics", Internet: www.bromba.com/faq/biofaqe.htm, [Jul. 2011].

[38] L. Chan, S. Salleh, and C. Ting, "Face biometrics based on Principal Component Analysis and Linear Discriminant Analysis", Journal of Computer Science, vol. 6, pp. 693-699, Jul. 2010.

[39] P. Selvi and N. Radha, "Multimodal biometrics based authentication against dictionary attacks", International Journal on Computer Science and Engineering, vol. 2, pp. 2652-2658, May 2010.

[40] G. Lakshmi, "Fingerprint identification system combined with cryptography for authentication", International Journal of Engineering, Science and Technology, vol. 2, pp. 3054-3077, Mar. 2010.

[41] C. Nandini, C. Ashwini, M. Aparna, N. Ramini, P. Kini, and K. Sheeba, "Biometrics authentication by dorsal hand vein pattern", International Journal of Engineering and Technology, vol. 2, pp. 837-840, Jan. 2012.

[42] H. Lu, K. Plataniotis, and A. Venetsanopoulos, "Uncorrelated multilinear Principal Component Analysis for unsupervised multilinear subspace learning", IEEE Transactions on Neural Networks, vol. 20, no. 11, pp. 1820-1836, Nov. 2009.

[43] M. Law and A. Jain, "Incremental nonlinear dimensionality reduction by manifold learning", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 3, pp. 377-391, Aug. 2006.

[44] J. Suo, L. Lin, and S. Shan, "High-resolution face fusion for gender conversion", IEEE Transactions on Systems, Man and Cybernetics, vol. 41, no. 2, pp. 226-237, Sep. 2011.

[45] E. Carlos, D. Gillies, and R. Feitosa, "A new covariance estimate for Bayesian classifiers in biometric recognition", IEEE Transactions on Circuits Systems and Video Technology, vol. 14, no. 2, pp. 214-223, Mar. 2004.

[46] L. Lin, T. Wu, J. Porway, and Z. Xu, "A stochastic graph grammer for compositional object representation and recognition", Pattern Recognition, Elsevier, vol. 42, no. 7, pp. 12971307, Feb. 2009.

[47] K. Nandakumar, "Integration of multiple cues in biometric systems", Masters thesis, Michigan State University, Department of Computer Science and Engineering, Oct. 2005.

[48] M. Nounou, B. Bakshi, P. Goel, and X. Shen, "Bayesian Principal Component Analysis", Journal of Chemometrics, vol. 11, pp. 576-595, Jun. 2002.

[49] K. Martin, H. Lu, F. Bui, K. Plataniotis, and D. Hatzinakos,"A biometric encryption system for the selfexclusion scenario of face recognition", IEEE Systems Journal: Special Issue on Biometrics Systems, vol. 3, no. 4, pp. 440-450, Mar. 2009.

[50] W. Zhang, X. Wang, and X. Tang, "Lighting and Pose Robust Face Sketch Synthesis", Proceedings of European Conf. Computer Vision, Nov. 2010.

[51] K. Nandakumar and A. Jain, "Multibiometric template security using fuzzy vault", Proceedings of 2nd IEEE International Conference on Biometrics: Theory, Applications, and Systems, pp. 1-6, Jun. 2008.

[52] A. Jain, "Hiding biometric data", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1449-1498, Nov. 2003.

[53] A. Ross, K. Nandakumar, and A. Jain, *Handbook of multibiometrics*, Springer, Chapter 2, Mar. 2006.

[54] B. Klare, Z. Li, and A. Jain, "Matching forensic sketches to mugshot photos", IEEE Transection Pattern Analysis and Machine Intelligence, vol. 33, no. 3, pp. 639-646, Mar. 2011.

[55] X. Wang and X. Tang, "Random sampling for subspace face recognition", International Journal of Computer Vision, vol. 70, no. 1, pp. 91-104, Oct. 2006.

[56] S. Bucak, R. Jin, and A. Jain, "Multiple kernel learning for visual object recognition: A review", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 36, no. 7, pp. 1354-1369, Jul. 2014.

[57] U. Park, H. Choi, A. Jain, and S. Lee, "Face tracking and recognition at a distance: A coaxial and concentric PTZ camera system", IEEE Transaction on Information Forensics and Security, vol. 8, no. 10, pp. 1665-1677, Oct. 2013.

[58] N. Srinivas, G. Aggarwal, P. Flynn, and W. Bruegge, "Analysis of facial marks to distingush between identical twins", IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1536-1550, Oct. 2012.

[59] A. Paulino, F. Jianjiang, and A. Jain, "Latent fingerprint matching using descriptor-based hough transform", IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 31-45, Jan. 2013.

[60] B. Klare and A. Jain, "Heterogeneous face recognition using kernel prototype similarities", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 2, Feb. 2013.

[61] F. Hao and C. Chan, "Private key generation from on-line handwritten signatures", Information Management and Computer Security, no. 2, pp. 159-164, Aug. 2002.

[62] A. Teoh, T. Connie, O. Ngo, and C. Ling, "Remarks on biohash and its mathematical foundation", Information Processing Letter, no. 4, pp. 145-150, Sep. 2006.

[63] C. Lee, J. Choi, K. Toh, S. Lee, and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutiae information", IEEE Transactions on Systems, Man and Cybernetics, Part B, vol. 37, no. 4, pp. 980-992, Oct. 2007.

[64] O. Song, A. Teoh, and D. Ngo, "Application specofic key release scheme from biometrics", Intenational Journal of Network Security, vol. 6, no. 2, pp. 127-133, Mar. 2008.

[65] Y. Wang, "Changeable and privacy preserving face recognition", PhD Thesis, University of Toronto, Sep. 2010.

[66] M. Savvides, B. Kumar, and P. Khosla, "Cancelable biometric filters for face recognition", Proceedings of the 17th International Conference on Pattern Recognition, pp. 922-925, Aug. 2004.

[67] D. Maio and L. Nanni, "Multihashing, human authentication featuring biometrics data and tokenised random number: a case study", Elsevier Neurocomputing, vol. 69, no. 1, pp. 242-249, Jun. 2006.

[68] A. Goh and D. Ngo, "Computation of cryptographic keys from face biometrics", Communications and Multimedia Security, Security Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 1-13, Jun. 2003.

[69] R. Gonzalez and R. Woods, *Digital Image Processing*, Ed.: 3rd Singapore: Prentice Hall, Nov. 2008.

[70] Y. Bar-Shalom, X. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*, New York, NY, USA: John Wiley & Sons, Inc., Sep. 2002.

[71] S. Haykin, *Kalman Filtering and Neural Networks*, Wiley-Interscience, Oct. 2001.

[72] O. Malek, A. Venetsanopoulos, and A. Anpalagan, "A comparison study between wiener and adaptive state estimation (STAP-ASE) algorithms for space time adaptive radar processing", Proceedings SPIE: Mathematics of Data/Image Coding, Compres- sion, and Encryption with applications XII, vol. 7799, no. 6, pp. 1-10, Aug. 2010.

[73] S. Haykin, *Adaptive Filter Theory*, Upper Saddle River, NJ, USA: Prentice-Hall Inc., Ed.: 4th, Sep. 2001.

[74] A. Kak, "ML, MAP and Bayesian - The holy trinity of parameter estimation and data prediction", Purdue University, Technical Report, Jul. 2013.

[75] A. Kasiski, A. Florek, and A. Schmidt, "The PUT Face Database", Image Processing and Communications, vol. 13, no. 3-4, pp. 5964, 2008.

[76] V. Jain and A. Mukherjee, "The Indian Face Database", Avaiable: http://www.cs.umass.edu/ vidit/IndianFaceDatabase/, 2002, [Dec. 2012].

[77] "Facial recognition", Internet: http://findbiometrics.com/solutions/facial-recognition/, [Feb. 2014].

[78] S. Milborrow, J. Morkel, and F. Nicolls, "The MUCT Landmarked Face Database", University of Captown, Oct. 2009.

[79] C. Bouman, "Digital image processing -Nonlinear filtering", Internet: http://biometricjournalweb/papers/nolinerafiltering.pdf, Jan. 2014, [Mar. 2014].

[80] G. Arce, J. Bacca, and J. Paredes, "Nonlinear filtering for image analysis and enhancement", Internet: http://biometricjournalweb/papers/essencial/20guide/20wmf.pdf, Jan. 2009, [Mar. 2014].

[81] V. Balakirsky, A. Ghazaryan, and A. Vinck, "An algorithm for biometric authentication based on the model of nonstationary random processes", [Apr. 2014].

[82] S. Bowker, "White paper -A guide to data analysis and segmentation", Publish by Legal, Data and Best Practice Hub, DMA Email Marketing Council, Jun. 2011.

[83] "Data protection act", Internet: http://www.getsafeonline.org/business/data-protection-act/, [June 2014].

[84] A. Delehanty, "Security issues in biometric identification", Internet: https://wiki.umn.edu/pub/ummcsciseniorseminar/spring2011talks /anthonydelehanty.pdf, Apr. 2011, [Dec. 2013].

[85] M. Bruso, K. Chatzikokolakis, S. Etalle, and J. Hartog, "Linking unlinkability", Available:http://hal.archives-ouvertes.fr/doc/00/76/01/50/pdf/unlinkability.pdf, 7th International Symposium on Trustworthy Global Computing, Dec. 2012, [June 2014].

[86] A. Pfitzmann and M.Hansen, "Anonymity, unlinkability, pseudonymity, and identity management-A consolidated proposal for terminology", Available: http://dud.inf.tu-dresden.de/Anon-terminology.shtml, version v0.25, Dec. 2005, [Aug. 2013].

[87] L. Khan and B. Thuraisingham, " Data mining applications in biometrics systems", Technical Report UTDCS-05-05, Department of Computer Science, The University of Texas at Dallas, Feb. 2005.

[88] J. Jackson, "Data mining: A conceptual overview", Communications of the Association for Information Systems, vol. 8, pp. 267-296, Oct. 2002.

[89] J. Sun, D. Tao, S. Papadimitriou, P. Yu, and C. Faloutsos, "Incremental tensor analysis: Theory and applications", Journal of ACM Transections on Knowledge Discovery from Data, vol. 2, no., 3 Oct. 2008.

[90] J. Pato and L. Millett, "Biometric recognition: challenges and opportunities", The National Academies Press, 2010.

[91] O. Malek, D. Androutsos, A. Venetsonoupoulous, and L. Lian, "Subspace state estimator for facial biometric verification", IEEE Proceedings of The International Conference on Computational Science and Computational Intelligence, Las Vegas, USA, vol. 1, pp. 137-143, Mar. 2014.

[92] O. Malek, D. Androutsos, A. Venetsonoupoulous, and L. Lian, "Sequential subspace estimator for biometric authentication", ELSEVIER-Neurocomputing, Accepted June 2014, To Appear 2014.

[93] L. Smith, "A tutorial on Principal Components Analysis", Technical Report, 2002.

[94] B. Kozminchuk, "A comparison of Recursive Least Squares and Kalman Filtering excisors for swept tone interference", Technical Note 92-14, Defence Research Establishment Ottawa, Ottawa, Ontario, Canada, Tech. Rep., 1992.

[95] Y. Bar-Shalom, X. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*, Chapters 6 and 10, New York, NY, USA: John Wiley & Sons, Inc., Sep. 2002.

[96] I. Reid, "Estimation II", Internet: http://biometricjournalsweb/papers/lecturenotes2.pdf", [Mar. 2013]

[97] H. Lai, Y. Pan, C. Liu, L. Lin, and J. Wu, "Sparse learning-to-rank via an efficient primal-dual algorithm", IEEE Transactions on Computers, vol. 62, no. 6, pp. 1221-1233, Jun. 2013.

[98] A. El-Keyi, T. Kirubarajan, and A. Gershman, "Robust adaptive beam forming based on the Kalman Filter", IEEE Transactions on Signal Processing, vol. 53, no. 8-2, pp. 3032-3041, Aug. 2005.

[99] D. Simon and T. Chia, "Kalman Filtering with state equality constraints", IEEE Transactions on Aerospace and Electronic Systems, vol. 39, pp. 128-136, Mar. 2002.

[100] C. Wikle and N. Cressie, "A dimension-reduced approach to spacetime Kalman Filtering", Biometrika, vol. 86, no. 4, pp. 815-829, Jul. 1999.

[101] G. Schoenig, "Contribution to robust adaptive signal processing with application to space-time adaptive radar", Ph.D. dissertation, Faculty of Virginia Polytechnic and State University, 2007.

[102] S. Brown and S. Rutan, "Adaptive Kalman Filtering", NBS Journal of Research, vol. 90, pp. 403-407, Mar. 1985.

[103] Internet: https://www.ics.uci.edu/ welling/teaching/KernelsICS273B/MatrixCookBook.pdf, [Feb. 2013].

[104] M. Khan, Internet: http://www.cs.ubc.ca/ emtiyaz/Writings/MILandIF.pdf, [Dec. 2012]

[105] A. Jain and A. Kumar, "Biometric of next generation: An overview", To Appear in Second Generation Biometrics Springer, Aug. 2010.

[106] B. Bhanu and X. Zhou, "Feature fusion of side face and gait for video-based human identification", ELSEVIER Journal of Pattern the Recognition Society 41, pp. 778-795, 2008.

[107] H. Lu, J. Wang. and K. Plataniotis, "A review on face and gait recognition: system, data and algorithms", Apr. 8 2008.

[108] C. Le and R. Jain, "A survey of biometrics security system", Available: www.cse.wustl.edu/ jain/cse571-11/fpt/biomet/, Nov. 2011, [Oct. 2012].

[109] A. Jain, A. Ross, and U. Uludag, "Biometric template security challenges and solutions", Available: www.biometrics.cse.msu.edu, Apr. 2005, [Jan. 2013].

[110] "Fingerprint ridge orientation angle", Internet: www.google.ca/search?q/fingerprint/orientation/angle, [Aug. 2013].

[111] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security", EURASIP Journal of Advances in Signal Processing, vol. 2008, pp. 1-17, Mar. 2007.

[112] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively", IEEE Transactions on Computers, vol. 55, pp. 1081-1088, Jun. 2006.

[113] K. Nandakumar and A. Jain, "Multibiometric template security using fuzzy vault", To Appear in BTAS, Nov. 2008.

[114] A. Jain and U. Ulugad, "Hiding biometric data", Pattern Analysis and Machine Intelligence, IEEE Transactions, vol. 25, pp. 1494-1498, Jun. 2003.

[115] J. Chang and K. Fan, "A new model for fingerprint classification by ridge distribution sequences", The Journal of the Pattern Recognition Society, vol. 35, pp. 1209-1223, Nov. 2002.

[116] M. Kaur, S. Sofat, and D. Saraswat, "Template and database security in biometrics systems: A chanllenging task", International Journaal of Computer Applications, vol. 4, no. 5, Jul. 2010.

[117] A . Zamboni, "Attacking biometric access control systems", Internet: www.miskatoniclabs.com/biometrics/, [Dec. 2013].

[118] E. Navathe, "Extendible Hashing: Advanced Database Systems", Internet: http://www.smckearney.com/adb/notes/lecture.extendible.hashing.pdf, [May 2013].