A

Major Project Report

On

ASSOCIATING PRIVATE KEYS IN CRYPTOGRAPHY WITH USER GENERATED BIOMETRICS

Submitted in Partial Fulfilment of the Requirement for the Degree of

MASTER OF TECHNOLOGY

In

INFORMATION SYSTEMS

By

DINESH KUMAR

2K14/ISY/21

Under the Esteemed guidance of

Mr. MANOJ KUMAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

BAWANA ROAD, Delhi-110042.

JUNE-2016

CERTIFICATE

This is to certify that Major Project-II Report entitled **"Associating Private Keys in Cryptography with User Generated Biometrics"** submitted by **Dinesh Kumar, Roll No. 2K14/ISY/21** for partial fulfilment of the requirement for the award of degree Master of Technology (Information Systems) is a record of the candidate work carried out by him under my supervision.

Mr. Manoj Kumar
Associate Professor
Department Of Computer Science & Engineering
Delhi Technological University

DECLARATION

I hereby declare that the Major Project work entitled "**Associating Private Keys in Cryptography with User Generated Biometrics**" which is being submitted to Delhi Technological University, in partial fulfilment of requirements for the award of degree of Master Of Technology(Information Systems) is a bonafide report of Major Project-1I carried out by me. The material contained in the report has not been submitted to any university or institution for the award of any degree.

Dinesh Kumar

Roll No 2K14/ISY/21

M.Tech (Information System)

Department of Computer Science and Engineering

Delhi Technological University

ACKNOWLEDGEMENT

First of all, I would like to express my deep sense of respect and gratitude to my project supervisor Mr. Manoj Kumar for providing the opportunity of carrying out this project and being the guiding force behind this work. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

Secondly, I am grateful to Dr. O.P.Verma, HOD, Computer Science & Engineering Department, DTU for his immense support. I would also like to acknowledge Delhi Technological University library and staff for providing the right academic resources and environment for this work to be carried out. Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.

Dinesh Kumar
University Roll no: 2K14/ISY/21
M.Tech (Information Systems)
Department of Computer Science & Engineering
Delhi Technological University

ABSTRACT

The need for information security and privacy has increased in today's times. Since extremely useful data and files are stored in an organization server system and more personal information are being shared over WWW, the requirement for providing security and allowing only the authorized user is becoming absolutely necessary. To achieve this purpose, biometric authentication is used in several applications and it is gaining more attention in the field of research. Several biometrics like iris, retina, fingerprint, etc are used to provide security to the information or key. The cryptographic key generation from biometrics is used generally to secure the system. The storage and security of biometric templates and cryptographic keys are of major importance. The flexibility and effectiveness of the cryptographic key generation methods make it useful for combining it with the biometric features. In the present world security is one the major concerns and there is requirement for research to be carried out to deal with cryptographic key generation schemes based on biometrics.

Keyword: symmetric cryptography; key management; key generation; fingerprint template; fingerprint based cryptographic key.

List of Figures

Figure 1.1: Generic biometric system **4**

Figure 1.2: Generic cryptography **5**

Figure: 1.3 Cryptography Types **6**

Figure 2.1: Biometric Cryptography Process **13**

Figure 2.2: Fuzzy vault system **18**

Figure 2.3 Fingerprint minutiae features for image **19**

Figure 2.4: Fingerprint minutiae features for cropped image **20**

Figure *2.5:* **Fuzzy fingerprint vault** **22**

Figure 3.1: Ridges and Valleys of a fingerprint image **27**

Figure 3.2: Fingerprint image, histogram, ROI **31**

Figure 3.3: Orientation and segmentation of fingerprint image **33**

Figure 3.4: Examples of minutiae type **34**

Figure 3.5: Sample images, with different validity and quality **37**

Figure 4.1: Minutiae points extraction **39**

Figure 4.2: Key generation and message encryption process **41**

Figure 4.3: Process of Template generation **42**

Figure 4.4: Key regeneration and cipher text decryption process **43**

Figure 5.1: FNMR vs FMR **47**

Figure 5.2: FMR vs GRR **48**
Figure 5.3: FNMR vs GMR **48**

List of Abbreviations

AFAS	Automatic Fingerprint Authentication System
AFIS	Automatic Fingerprint Identification System
BE	Biometric Encryption
CBS	Cryptobiometric System
CRC	Cyclic Redundancy Check
EK	Encapsulated Key
EPK	Encryption Provider Key
FAR	False Acceptance Rate
FE	Fuzzy Extractor
FFV	Fingerprint Fuzzy Vault
FMR	False Matching Rate
FNMR	False None Matching Rate
FP	Fingerprint
FR	False Rate
FVS	Fuzzy Vault Scheme
GMR	Genuine Match Rate
GRR	Genuine Reject Rate
OAS	Object Area Segmentation
PCA	Principle Component Analysis
PKC	Public Key Cryptography
QA	Quality Assessment
QI	Quality Index
SWA	Slicing Window Algorithm
SW	Slicing Window
TAR	True Acceptance Rate
TM	Transformed Matrix
TR	True Rate
TRR	Threshold Ratio

TABLE OF CONTENTS

CERTIFICATE

DECLARATION

ACKNOWLEDGEMENT

ABSTRACT

LIST OF FIGURES

LIST OF ABBREVIATIONS

CHAPTER 1: INTRODUCTION

1.1Background 1

1.2Biometric Systems 3

1.3Cryptography 4

1.4 Biometric and Cryptography Merging 7

1.5 Aims and Objectives 8

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction 10

2.2 Cryptography and biometric keys 10

2.3. Summary 24

CHAPTER 3: FINGERPRINT IMAGE ANALYSIS

3.1 Introduction 26

3.2 Fingerprint Representation Area 27

3.3 Fingerprint Object Segmentation 28

3.3.1 Grey Level Segmentation 29

3.3.2 Directional Segmentation 31

3.4 Fingerprint Pattern Analysis 33

3.4.1 Local Analysis 34

3.4.2 Global Analysis 35

3.4.3 Validity Statistical Analysis 36

CHAPTER 4: PROPOSED WORK

4.1 Biometric Based Key Release 38

4.2 Biometric Based Key Generation 38

4.3 Biometric Based Key Generation 39

4.4 Key generation and message encryption 40

4.5 Key regeneration and cipher text decryption 43

CHAPTER 5: RESULT ANALYSIS 45

CHAPTER 6: CONCLUSION AND FUTURE WORK 50

REFERENCES 51

CHAPTER 1

INTRODUCTION

1.1 Background

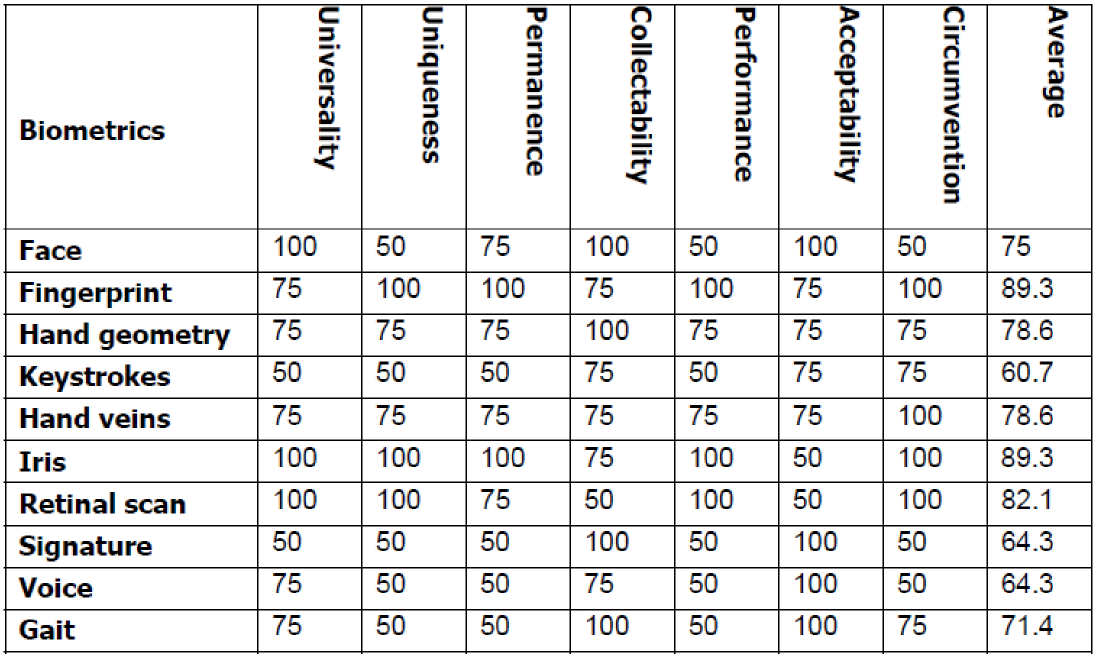
Technology bring a new aspect to biometrics in the information era, while biometrics brings a new aspect to individual identity verification. It provides a high level of consistency and accuracy over traditional methods. Biometrics means statistical analysis of biological observations and phenomena. It is using distinctive physical like palm, face, retina, hand geometry, iris, fingerprints and behavioral like signature, speech, gait characteristics for recognizing individuals. Biometric based identification depends on "something that you are", or "something that you do", and thus it differentiate between an authorized person and an imposter. Any behavioral or physiological characteristic of humans can be used as biometric if it satisfies the following requirements:

- Universality: every individual should have this characteristics.
- Uniqueness: no two individuals should have the match of a characteristic.
- Permanence: the characteristic should remain same throughout individual lifetime.
- Collectability: the characteristic should be quantifiable.
- Circumvention: it refers to the easiness to fool the system by fraudulent techniques.
- Performance : identification accuracies
- Acceptability: willingness of people to accept biometric system.

Biometric provides unique features for every individual and it is commonly accepted. While some of the characteristics mentioned above are easily verifiable like universality and collectability, while others like uniqueness and immutability require extensive testing on large no of samples for verification.

Each biometric has its own pros and cons. The biometric technique used is largely dependent on application domain. No single biometric can satisfy all the requirements which means we can't say some biometric as "optimal". Fingerprints provides large no of advantages over any other biometric in terms of acquisition ease, uniqueness, relative temporal invariance.

A comparative analysis of biometric techniques based on seven factors is provided in Table 1-1.



Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention	Average
Face	100	50	75	100	50	100	50	75
Fingerprint	75	100	100	75	100	75	100	89.3
Hand geometry	75	75	75	100	75	75	75	78.6
Keystrokes	50	50	50	75	50	75	75	60.7
Hand veins	75	75	75	75	75	75	100	78.6
Iris	100	100	100	75	100	50	100	89.3
Retinal scan	100	100	75	50	100	50	100	82.1
Signature	50	50	50	100	50	100	50	64.3
Voice	75	50	50	75	50	100	50	64.3
Gait	75	50	50	100	50	100	75	71.4

Table 1-1 Comparison of various biometric technologies, according to A. Jain [2], U. Uludag [5], the perception based on (High=100, Medium=75, Low=50)

In this sense, each biometric technique is admissible. For example, it is well known that both the fingerprint technique and the iris scan technique perform much better than the voice print technique in terms of accuracy and speed. As can be seen from Table 1-1, overall fingerprints perform better than other biometric techniques. Fingerprint has its own distinctiveness that has been used for personal identification for several years.

Fingerprint identification is based on two basic premises,

1. Persistence: the basic characteristics of fingerprints do not change with time.

2. Individuality: everybody has a unique fingerprint.

Biometrics can operate in one of two modes: the identification mode, in which the identity of an unknown user is determined, and the verification mode, in which a claimed identity is either accepted or rejected. On this basis biometrics were applied in many high end applications, with governments, defence and airport security being major customers. However, there are some arenas in which biometric applications are moving towards commercial application, namely, network/PC login security, web page security, employee recognition, time and attendance systems, and voting solutions.

While biometric systems have their limitations they have an edge over traditional security methods in that they cannot be easily stolen or shared. Besides bolstering security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords.

1.2 Biometric Systems

Biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological and or behavioural characteristic possessed by that person. The generic biometric system can be divided into five subsystems Figure (1-1): Data collection, Transmission, Data storage, Signal processing and decision systems.

Data Collection: This subsystem uses a sensor or camera to acquire the image of the biometric trait of the user.

Transmission: This subsystem transmits the data collected from data collection module after compressing it, to the data storage and signal processing module.

Data Storage: Stores the image and template of the user.

Signal Processing: This is the most important module of the system. It performs feature extraction by image processing techniques and pattern matching operations.

Decision: This module performs identification or verification by using the match scores. This thesis is concerned with the important issues of data collection, storage, and data processing to merge biometric and cryptography for binding and generating bio crypt.

The Figure (1-1) below shows that of the first point of any biometric system is the acquisition box which means acquiring of biometric data from the user. To this box this work will add an automated validity checker and quality assessor to enhance the system performance.

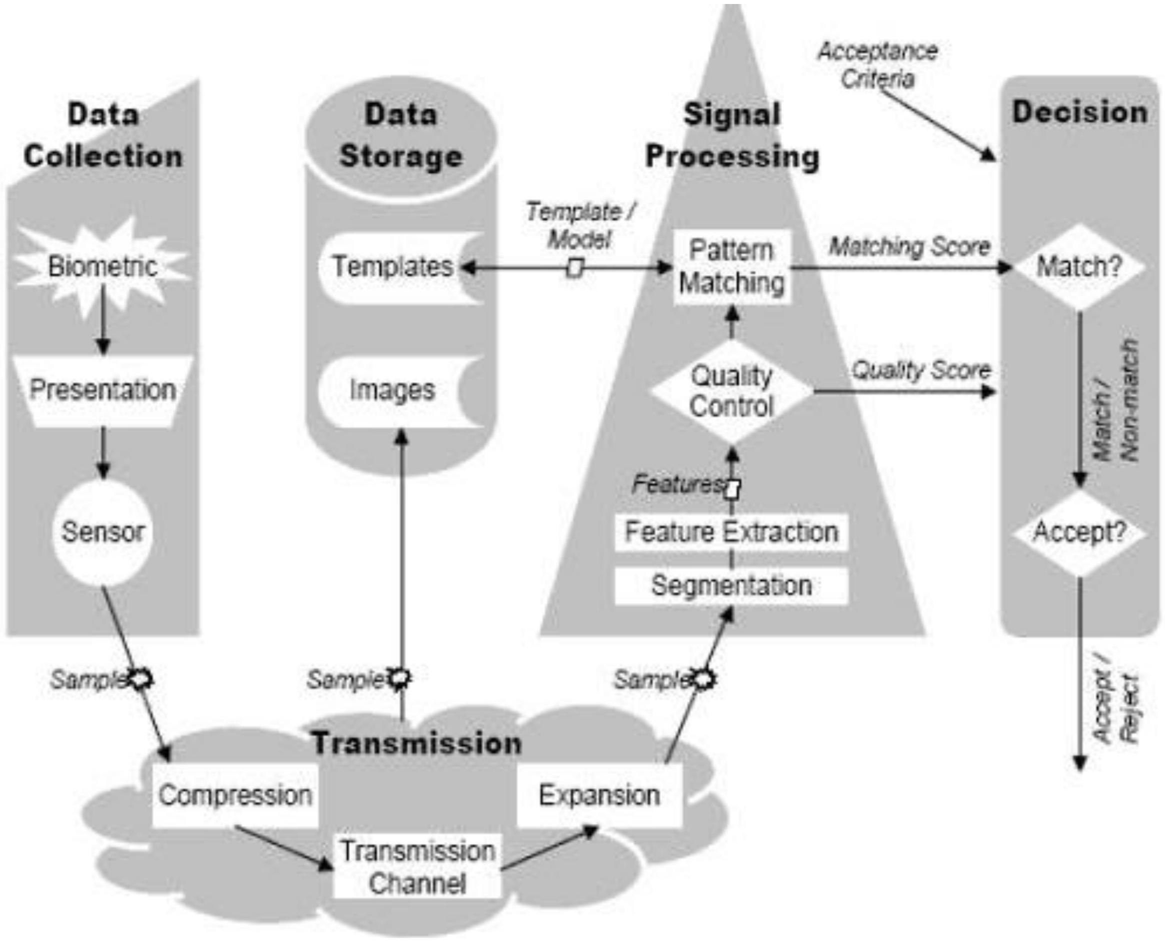


Figure 1-1 Generic biometric system

The performance of bio crypt based systems is dependent on the quality of the enrolled biometric. Enrolment quality can be affected by accidental or deliberate events and environmental conditions, and the result of low enrolment quality is almost inevitably due to poor system performance. If the performance is poor the security will be compromised, and there may be excessive dependence on the fallback system.

1.3 Cryptography

Cryptography is the practice and study of hiding information. Cryptography refers almost exclusively to encryption, the process of converting ordinary information, i.e. plain text, into unintelligible data, i.e. ciphertext. Decryption is the reverse, moving from unintelligible ciphertext to plaintext, Figure (1-2). A cipher is a pair of algorithms which perform this encryption and the decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter (ideally, known only to the communicants) for a specific message exchange context. Keys are important, as ciphers without variable keys are easily breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks.

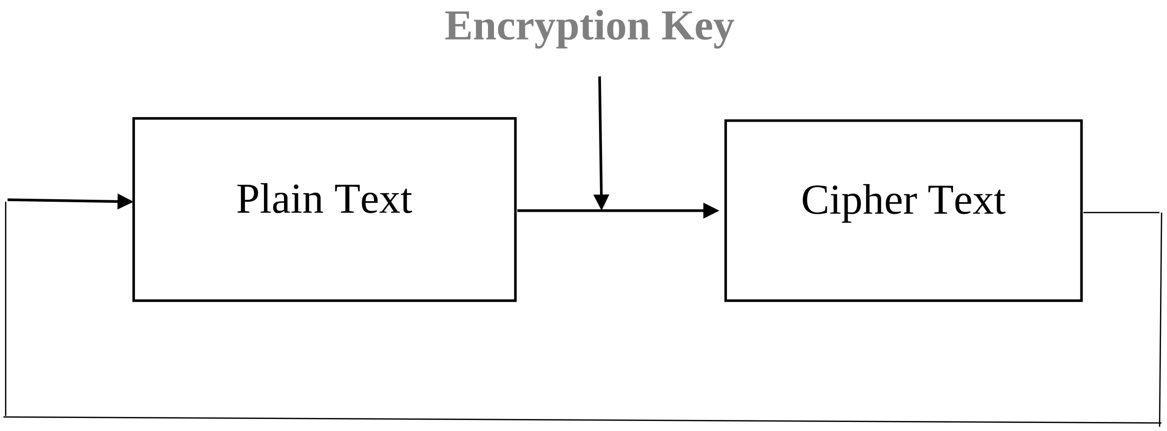
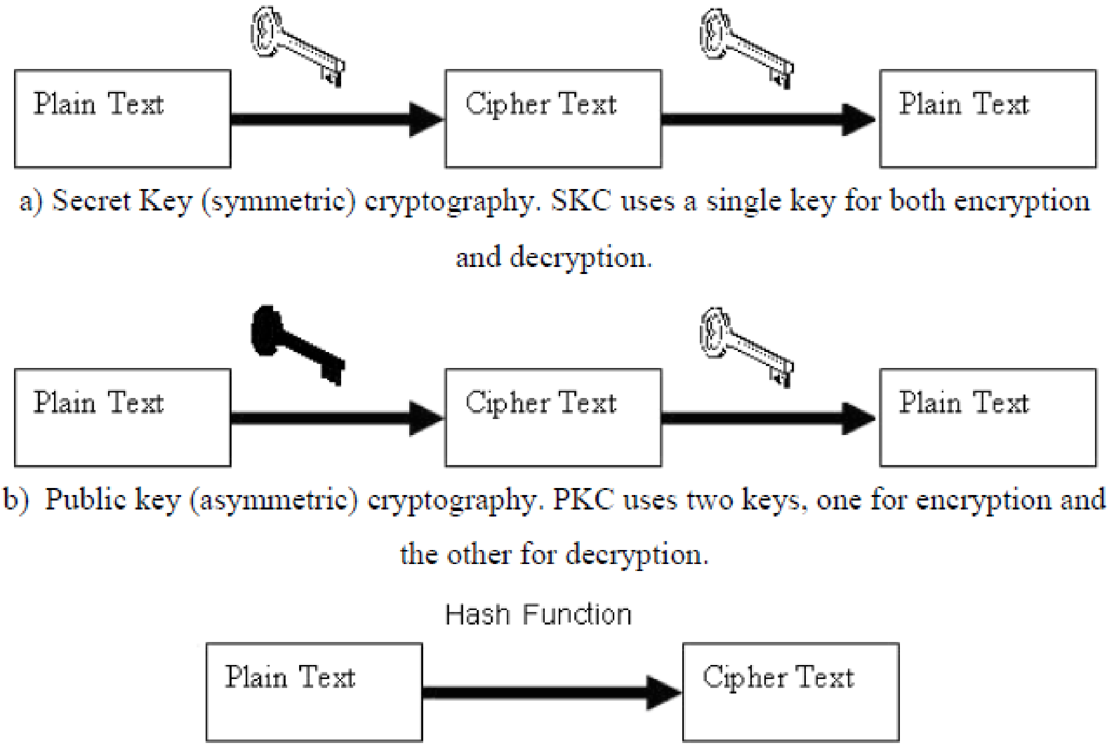


Figure 1-2 Generic cryptography

Cryptography is used in applications such as the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, these are shown in Figure (1-3).

In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext. A single key is used for both encryption and decryption in secret key cryptography; two keys are used in public key cryptography. Hash function uses a fixed-length value computed from the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Each cryptography scheme is optimized for some specific application. Hash functions, for example, are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Secret key cryptography, on the other hand, is ideally suited to encrypting messages. The sender can generate a session key on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message. Key exchange, of course, is a key application of public-key cryptography. Asymmetric schemes can also be used for non-repudiation; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message.



a) Secret Key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

b) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

c) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Figure 1-3 Cryptography types: a) secret-key, b) public key, and c) hash function.

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied. In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys.

1.4 Biometric and Cryptography Merging

Biometrics and cryptography are two potentially complementary security technologies. Biometrics has the potential to identify individuals with a high degree of assurance, thus providing a foundation for trust. Cryptography, on the other hand, concerns itself with the projection of trust: with taking trust from where it exists to where it is needed. Cryptography is an important feature of computer and network security. Using biometrics for security purposes becomes popular, but using biometrics by means of cryptography is a new hot research topic. Many traditional cryptographic algorithms are available for securing information, but all of them are dependent on the secrecy of the secret or private key.

To overcome this dependency, biometrics features consider secrecy of both keys and documents. There are various methods that can be deployed to secure a key with a biometric. The first involves remote template matching and key storage. In this method a biometric image is captured and compared with a corresponding template. If the user is verified, the key is released. The main problem here is using an insecure storage media. Second method hides the cryptographic key within the enrolment template itself via a secret bit-replacement algorithm. When the user is successfully authenticated, this algorithm extracts the key bits from the appropriate locations and releases the key. Using data derived directly from a biometric fingerprint image is another method. In this manner fingerprint templates are used as a cryptographic key. However, sensitivities due to environmental, physiological factors and compromising of the cryptographic keys stand as a big obstacle.

There have been a number of attempts to bridge the gap between the fuzziness of biometrics and the exactitude of cryptography, by deriving biometric keys from key stroke patterns, the human voice, handwritten signatures, fingerprints and facial characteristics. This thesis tackles the interaction between fingerprint biometrics and cryptography based on merging, generation and capsulation construction. Biometrics and cryptography should not be seen as competing technologies. Therefore, they have to be symbiotic rather than competitive.

Biometric Fingerprint was chosen because of its information strength, namely the uniqueness for random sequences, needed for cryptographic key generation. Biometry can be applied in the field of merging security if and only if the biometric parameters provide high enough entropy, stability and overall security of a system based upon this technology. The main obstacle to algorithmic combination is that biometric data are noisy; only an approximate match can be expected to a stored template.

Cryptography, on the other hand, requires that keys be exactly right, or protocols will fail. This thesis will attempt to bridge the gap between the fuzziness of biometrics and the exactitude of cryptography by directly deriving a biometric key from fingerprint biometric, using fuzzy vault construction to bind a crypto key with fingerprint vault, or by using a proposed capsulation construction approach to overcome the key management and secret key protection problems by considering security engineering aspects. Research on Fingerprint Based Biometric Cryptography should address the following problems for the sake of tying both technologies. Each of the points made below must be taken into account when designing a secure biometric system:

- Key diversity problem as a result of instability and inconstancy of biometric features because it is impossible to reproduce the same biometric data from user.
- To overcome the security management problem of keys and insecure storage media.
- Poor quality of biometric source images may affect the system performance.

1.5Aims and Objectives

The aim of performing scientific research into imaging and security fields is to create acceptance for, and quality of, fingerprint based authentication methods, with the intention of meeting the trust and security requirements in information technology (IT) transmission. The aims and objectives of this research can be summarized as follows:

- GTo provide a better understanding of the relationship between image processing techniques and security approaches for cryptographic based key generation.
- To identify, describe and produce analysis of fingerprint image region of interest for authenticated features.
- To provide a better understanding of the fingerprint quality analysis benchmark and to develop improved methods of validity and quality estimation for functional fingerprint imaging.
- To facilitate the development of methods for studying fingerprint in cryptography key infrastructure, and to incorporate authenticated fingerprint features into cryptography.
- To exploit the claimed merging of biometric and cryptography for integration usage, and contribution addition in the field of Bioscrypt and Biosecurity within obtaining practical results and investigating Bioscrypt's Embedded Solution.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

For biometric applications and systems to be accurate, a biometric template must be generated using a desirable bio pattern sample and qualified image source. A biometric image quality assessment and validity analysis are defined as a predictor of an accuracy and performance of biometric security system.

Therefore, it is important to determine the validity and quality of the input image during the enrolment stage, avoiding a mismatch result later in the process. It is desirable to estimate the image quality of the fingerprint image before it is processed for feature extraction. This helps in deciding on the type of image enhancements that are needed and on the threshold levels for the matcher performance, e.g. a sample's quality score reflects the predictive positive or negative contribution of an individual sample to the overall performance of a fingerprint matching system. Investigations of fingerprint image validity analysis and quality estimation are important techniques for crypto key system construction and judgment. Image validity and quality are critical aspects in the crypto security environment where entire processes are built around a captured fingerprint image as well as other authentication and identification systems.

This literature survey presents the fingerprint validity, quality assessment and crypt construction based fields and to give a general description of the various considerations on the development and implementation of fingerprint image validity, quality assessment and fingerprint crypto based systems.

2.2 Cryptography and biometric keys

Cryptography is an important feature of computer and network security [1]. Using biometrics for security purposes is becoming more popular, but using biometrics by means of cryptography is a new, growing and promising research area. A number of researchers have studied the interaction between biometrics and cryptography, two potentially complementary security technologies. This section will survey the development of bio key and the cross relation between original source, i.e. source fidelity and quality, and bio key based results, i.e. releasing, generation and binding keys. Bodo [2] proposed that data derived from the template be used directly as a cryptographic key, Bodo's work was supported by [3,4]. As sample variability has no direct bearing on these templates, the same key can be generated at all times, but a major drawback of the approach is that if a user needs to change his template, the previous key may never be regenerated.

Tomko.et al [5] proposed a public key cryptographic system implementation. In an enrolment apparatus, the unique number, for use in generating the public key and private key of the system, is generated by manipulation of fingerprint information of a subscriber. A filter is then generated which is a function of both the Fourier transform of the subscriber's fingerprint(s) and of a unique number. This filter is stored on a subscriber card. When the subscriber wishes to generate his public or private key, he inputs his card to a card reader of an apparatus and places his finger(s) on a fingerprint input. The apparatus generates an optical Fourier transform from the fingerprint input. The Fourier transform signal is incident on to a spatial light modulator programmed with the filter information from the card. An inverse transform is generated from the filtered signal and this is used to regenerate the unique number. The apparatus also has a subsystem for utilizing the private key to decrypt an input encrypted message. Soutar.et al. [5] proposed biometric encryption algorithm using image processing. This algorithm binds a cryptographic key with the user’s fingerprint images at the time of enrolment. The key is then retrieved only upon a successful authentication.

Biometric Encryption (BE) has been developed to securely link and retrieve a digital key using the iteration of a biometric image, such as a fingerprint, with a secure block of data, known as a Bioscrypt. The key can be used as an encryption- decryption key. The Bioscrypt comprises a filter function, which is calculated using an image processing algorithm, and other information which is required to first retrieve, and then verify the validity of the key. The key is retrieved using information from the output pattern formed via the interaction of the biometric image with the filter function. Soutar.et al [6] proposed a merging of biometrics with cryptography by using a biometric to secure the cryptographic key. Instead of entering a password to access the cryptographic key, the use of this key is guarded by biometric authentication. Key release is dependent on the result of the verification part of the system.

Thus, biometric authentication can replace the use of passwords to secure a key. The proposed algorithm offers both conveniences, as the user no longer has to remember a password, and secure identity confirmation, since only the valid user can release the key. BE processes the entire fingerprint image. The mechanism of correlation is used as the basis for the BE algorithm. The correlation function $c(x)$, between a subsequent version of the input $f1(x)$ obtained during verification and f_0(x) obtained during an enrolment is formally defined as

$$c(x) = \int_{-\infty}^{\infty} f_1(v) f_0^*(x + v) \qquad 2\text{-}1$$

where * denotes the complex conjugate.

In a practical correlation system, the system output is computed as the inverse Fourier transform $\left(FT^{-1} \right)$ of the product of $F_1(u)$ and $F_0^*(u)$, where

$$c(x) = FT^{-1}\{F_1(u)F_0^*(u)\} \qquad 2\text{-}2$$

where $F_0^*(u)$ is typically represented by the filter function, $H(u)$, that is derived from $f_0(x)$. For correlation based biometric systems, the biometric template used for identification authentication is the filter function, $H(u)$. The process of correlation provides an effective mechanism for determining the similarity of objects, and has been successfully used for fingerprint authentication. Biometric Encryption algorithms consist of two parts: Enrolment and verification. The enrolment contains image processing, key linking and identification code creation blocks, while verification contains image processing, key retrieval and key validation blocks.

The main criticism of Soutar et al.'s work in the literature is that the method does not carry rigorous security guarantees. The authors do not explain how much entropy is lost at each stage of their algorithm. Further, the resulting False Matching Rate (FMR) and False None Matching Rate (FNMR) values are unknown. The authors also assume that the input and database templates fingerprint images are completely aligned. Even with a very constrained image acquisition system, it is unrealistic to acquire fingerprint images from a finger without any misalignment. Adler presented an approach to attack biometric encryption algorithm in order to extract the secret code with less than brute force effort. A potential vulnerability work was implemented against biometric encryption algorithm. This vulnerability requires the biometric comparison to "leak" some information from which an analogue for a match score may be calculated. Using this match score value, a "hill-climbing" attack is performed against the algorithm to calculate an estimate of the enrolled image, which is then used to decrypt the code. It could be summarized that Biometric Encryption allows individuals to use a single biometric for multiple accounts and purposes without fear that these separate identifiers or users will be linked together by a single biometric image or template.

Thus, if a single account identifier becomes compromised, there is far less risk that all the other accounts will also be compromised. Even better, Biometric Encryption technologies make possible the ability to change or recompute account identifiers. That is, identifiers may be revoked or cancelled, and substituted for newly generated ones calculated from the same biometric! Traditional biometric systems simply cannot do this. Costanzo [7] proposed an approach for generating a cryptographic key from an individual's biometric for use in proven symmetric cipher algorithms. According to this approach Figure (2-1), the encryption process begins with the acquisition of the required biometric samples.

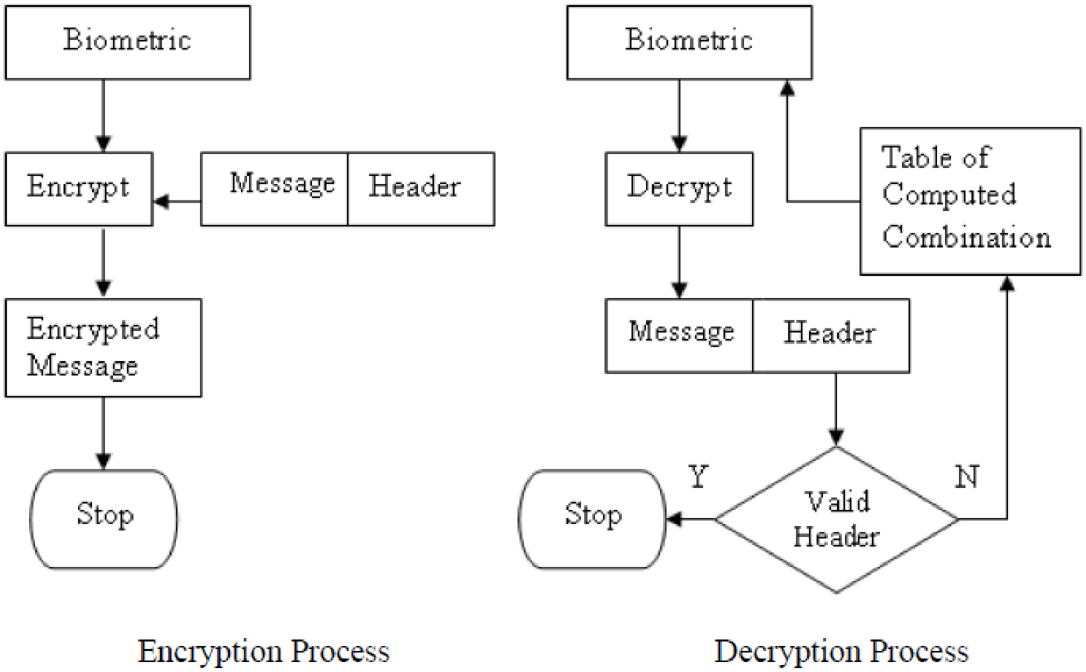


Figure 2-1 Biometric Cryptography Process

Features and parameters are extracted from these samples and used to derive a biometric key that can be used to encrypt a plaintext message and its header information. The decryption process starts with the acquisition of additional biometric samples from which the same features and parameters are extracted and used to produce a “noisy” key as done in the encryption process. Next, a small set of permutations of the “noisy” key are computed. These keys are used to decrypt the header information and determine the validity of the key. If the header is determined to be valid, then the rest of the message is decrypted. The proposed approach eliminates the need for biometric matching algorithms, reduces the cost associated with lost keys, and addresses non-repudiation issues. In Key Generation based on biometric aggregation several invariant features of different types of biometric are used to derive a bio-key that is used to encrypt a plain text message with header information. The decryption is based on a new generated bio-key which may not be exactly the same as the initial key. Different permutations of the newly computed bio-key are used to decrypt the header of the encrypted message after which the rest of the message is inferred. This approach was shown efficient and addressed thge nonrepudiation problems.

However, to be robust this scheme needs several biometrics. Davida et al, proposed an algorithm based on the iris biometric. They considered binary representation of iris texture, called Iris Code, which is 256 bytes in length. The biometric matcher computes the Hamming distance between the input and database template representations and compares it with a threshold to determine whether the two biometric samples are from the same person or not. The authors assume that the Iris Codes from different sampling of the same iris can have up to 10% error rate of the 256 byte vectors which means (204 bits) different from the same iris’s template Iris Code.

The authors also assume that the Iris Codes of different irises differ in as many as 45% of the 256 bytes (922 bits). Davida et al [8] argue that the database template of a user itself can be used as a cryptographic key (note that this key would always be the same for the same biometric identifier in contrast to cryptographic key binding algorithms such as biometric encryption algorithm. The main criticism of Davida et al.’s work is that they assumed that the input and database template Iris Codes are completely aligned.

Although constrained iris image acquisition systems can limit the misalignment among different acquisitions of the same iris, some degree of misalignment is natural. They have ignored this fact in their algorithm. Another criticism of Davida et al.’s work in is that no concrete implementation work was reported, and it was found that the majority of coding does not work with real iris data as errors are strongly correlated. Monrose et al [9] proposed a novel approach to improving the security of passwords by combining a short binary string which derived from a keystroke biometrics with passwords. In their approach, the legitimate user's typing patterns (e.g., durations of keystrokes, and latencies between keystrokes) are combined with the user's password (*pwd)* to generate a hardened password (*hpwd)* that is convincingly more secure than conventional passwords against both online and offline attackers.

During enrolment, the following information is stored in the user’s database template: 1) a randomly chosen large prime number (*r)* length 160 bit; 2) an “instruction table” which created on base of secret sharing scheme then encrypted with *pwd* , the instruction table is created using user’s keystroke features (the measurable keystroke features for an 8-character password are relatively few at most 15 on standard keyboards).

These features are thresholded to generate a binary feature descriptor, then the binary feature descriptors are used to create the instruction table using Shamir’s secret sharing scheme; and 3) an encrypted “history file” that contains the measurements for all features. At the time of authentication, the algorithm uses (*r)* and the instruction table from the user’s template and the authentication password (*pwd)*' and keystroke features acquired during the authentication to compute (*hpwd)*' . The (*hpwd)*' is used to decrypt the encrypted history file. If the decryption is successful, the authentication is successful, and the (*r)* and history file of the user are modified in the template; if the authentication is unsuccessful, another instance of (*hpwd)*' is generated from the instruction table in a similar way but with some error correction, and the authentication is tried again. If the authentication does not succeed within a fixed number of error-correction iterations, the authentication finally fails.

The authors claim that the hardened password itself can be used as an encryption key. A weakness of this work is that it only adds about 15 bits of entropy to the passwords, thus making them only marginally more secure. However, in, Monrose et al. made some minor modifications to their original scheme, applied it to spoken password, i.e. voice biometrics (which is more distinctive than keystroke biometrics), and were eventually able to generate cryptographic keys of up to 60 bits, which although much higher than the 15 bits achieved in their earlier work, is still quite low for most security applications.

Keystroke patterns are also used for the purpose of authenticating users accessing a computer system. Keystroke rhythms are a method that tries to understand individual's behaviour. In biometric data is assigned to a vector which carries all well known values of property. By using a minimum distance classifier, it will be easy to make a decision by finding the distance between the test pattern and the templates of each individual which are previously determined after a training phase. Proposed approach in [10] has four major steps. In the first step, parameters of users' keystroke are collected using a login form and stored in a database. Next step is the validation step where the users' parameters are processed by an efficient validation algorithm. At the end of this stage, new parameters are generated. In the decision making step, new values calculated during the validation phase are transferred to a decision function. In this step user is accepted or rejected. Final step, the parameters belong to the successful login are updated in the database. Keystroke pattern are low cost user specific data especially for biometric authentication and cryptography and it should be noted that they are usually difficult to detect and analyze. Similar to image type biometrics, human voice is a good biometric to generate a cryptographic key. In [11], Hao et al. made use of handwritten signatures. They defined forty-three signature features extracted from dynamic information like velocity, pressure, altitude and azimuth.

Feature coding was used to quantize each feature into bits, which were concatenated to form a binary string. Their key achieved on average 40-bit key entropy with a 28% false rejection rate; the false acceptance rate was about 1.2%. Derived key performs shape matching to rule out poor-quality signatures in the initial verification phase. The authors claim an Equal Error Rate (EER) of 8%, and mention that their test database contains forgeries, but unfortunately provide no details on how these were produced or their quality.

Kuan et al [12,13] presented a method for replaceable generating cryptographic keys from dynamic handwritten signature that can be replaced if the keys are compromised and without requiring a template signature to be stored or any statistical information that could be used to reconstruct the biometric data. Their replaceable key is accomplished using iterative inner product of Biohash method, and modified multiple-bit discretization that deters guessing from key statistics. They got encouraging results especially for skilled and random forgery whereby the equal error rates are <6.7% and ~0% respectively, indicating that the keys generated are sufficiently distinguishable from impostor keys. Some work on cryptographic key generation was done toward a fuzzy vault technique (which will be reviewed later) based on. Chang et al [14] proposed a framework to generate stable cryptographic keys from biometric data that is unstable in nature. Their proposed framework differs from prior work in that user-dependent transforms are utilized to generate more compact and distinguishable features. Thereby, a longer and more stable bit stream can be generated as the cryptographic key.

For feasibility verification, a proposed framework was performed on a face database. However he did not address the issue of setting the thresholds for distinguishable features, this issue was tackled by Zhang et al.'s work, they proposed a method to minimize the authentication error rate in terms of the false accept rate and the false reject rate of the bio key generation system by setting optimal thresholds of each feature. Previous reviewed works assumed that enrolled templates are noise free, and aligned. To turn noisy information into usable keys for any cryptographic application and, in particular, reliably and securely authenticating biometric data, Dodis et al.[15] proposed theoretical foundations for generating keys from the key material that is not exactly reproducible. They provided formal definitions and efficient secured techniques for cryptographic key generation. They defined fuzzy extractors (FE) to generate a variable (*R)* from the key material (*w),* and public (helper) data (*P)*. Given the variable (*P)*, FE again generates (*R)* from (*w)*' , if (*w)*' is “close” to (*w*).

The scheme fuzziness come from the variability of biometric data: even though the same biometric entity, the extracted biometric data will vary due to acquisition characteristics (e.g., placement of the finger on the sensor), sensor noise, etc. On the other hand, in traditional cryptography, if the keys are not exactly the same, the decryption operation will produce useless random data. Note that since the fuzzy vault can work with unordered sets (common in biometric templates, including fingerprint minutiae data); it is a promising candidate for biometric cryptosystems. Having said this, the fuzzy vault scheme requires pre-aligned biometric templates.

Namely, the biometric data at the time of enrolment (locking) must be properly aligned with biometric data at the time of verification (unlocking). This is a very difficult problem due to different types of distortion that can occur in biometric data acquisition. Further, the number of feasible operating points (where the vault operates with negligible complexity, e.g., conveyed via the number of required access attempts to reveal the secret, for a genuine user and with considerable complexity for an impostor user) for the fuzzy vault is limited: for example, the flexibility of a traditional biometric matcher (e.g., obtained by changing the system decision thresghold) is not present. Based on the fuzzy vault scheme, Clancy et al proposed [17] a fingerprint vault using multiple minutiae location sets per finger (based on 5 impressions of a finger), they first find the canonical positions of minutia, and use these as the elements of the set (*A*). They add the maximum number of chaff points to find (*R*) that locks (*k*). However, their system inherently assumes that fingerprints (the one that locks the vault and the one that tries to unlock it) are pre-aligned.

This is not a realistic assumption for fingerprint-based authentication schemes. Clancy et al. simulated the error-correction step without actually implementing it. They found that 69-bit security (for False Accept Rate (FAR)) could be achieved with a False Reject Rate (FRR) of 20-30%. Note that the cited security translates to 269 ≈ 1.7 ∗10−21 FAR. Further, FRR value suggests that a genuine user may need to present his/her finger multiple times to unlock the vault. Uludg and Jain used lines based fingerprint minutiae representation to design fuzzy vault system Figure (2-9) but it was without the actual implementation. It differs from Clancy system in the way that both location and angle of minutiae are used to extract lines for forming the templates. Uludag et al [18] present their implementation of fuzzy vault, operating on the fingerprint minutiae features. These features are represented as (*x*, *y*, θ) of ridge ending or bifurcation, where (*x*, *y*) is minutiae coordination and (θ) is the angle of the associated ridge Figure (2-10)

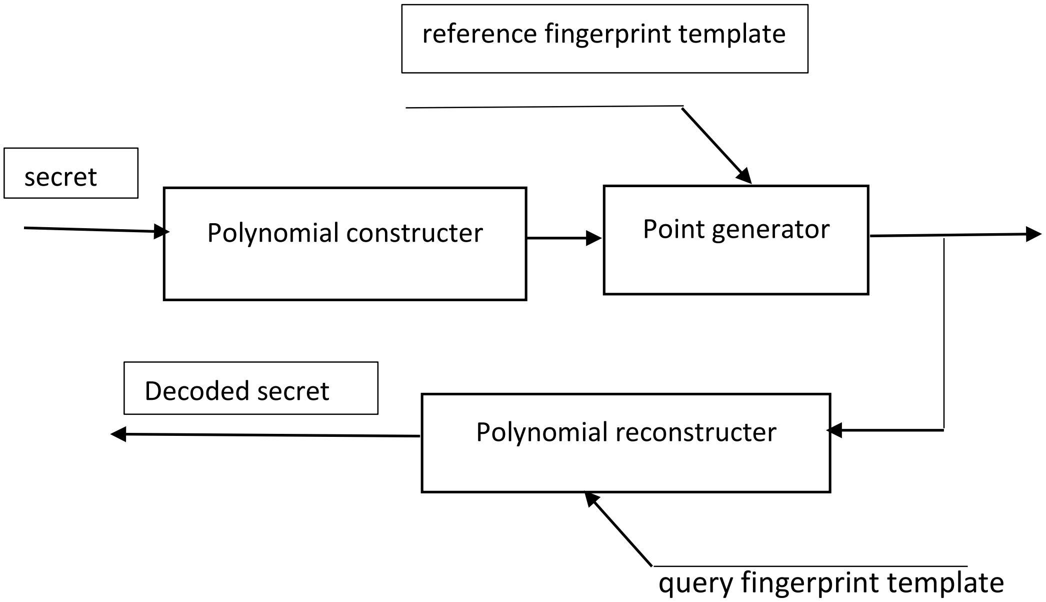
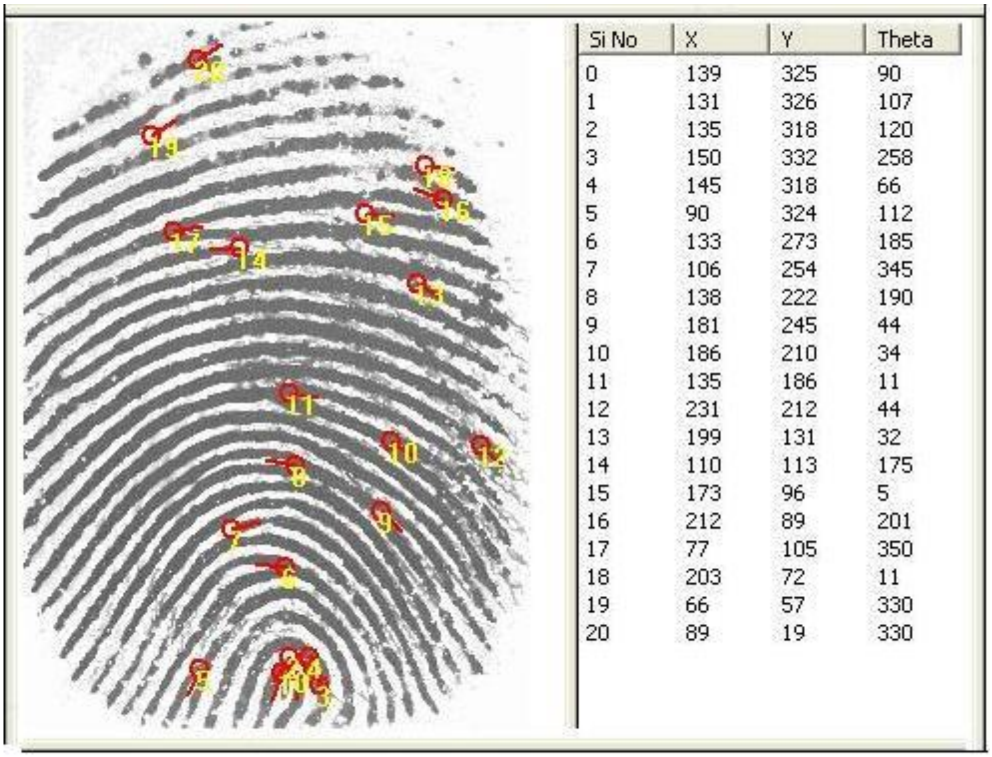


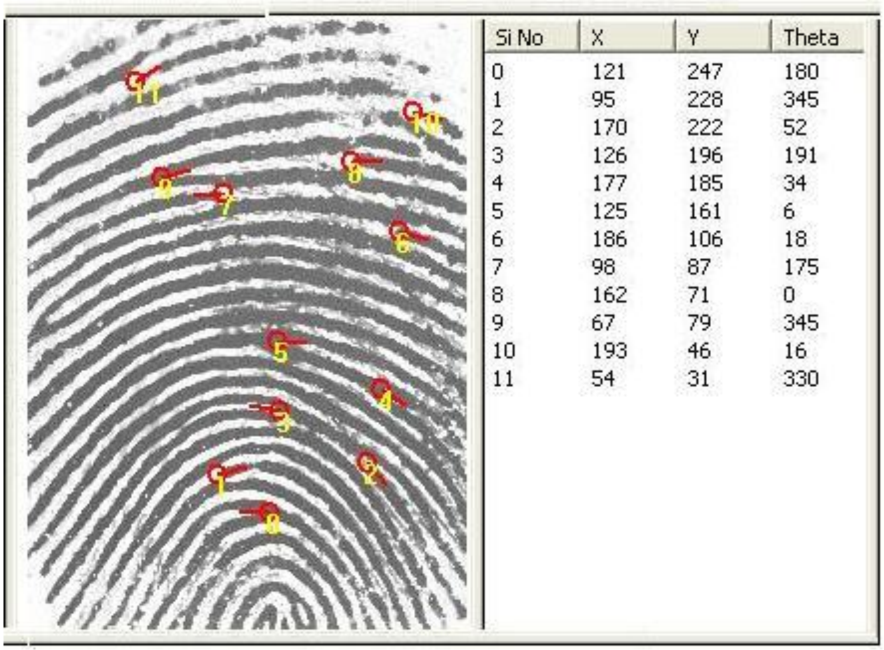
Figure 2-2 Fuzzy vault system

They extend into where chaff points generated according to minutiae points and protected secret, which is clear in secret check block (cyclic redundancy check encoding),and chaff generation block differ from work’s in decoding implementation does not include any correction scheme, since there are serious difficulties to achieve error-correction with biometric data. Developing the necessary polynomial reconstruction via error-correction has not been demonstrated in the literature. Fuzzy vault for fingerprint decodes many candidate secrets Figure (2-11). To identify which candidate is valid a Cyclic Redundancy Check (CRC) is used. CRC is commonly used in error correction. In proposed system using incorrect minutiae points during decoding will cause an incorrect polynomial reconstruction, resulting in errors. Uludag et al., generate 16-bit CRC data from the secret S . Hence, the chance of a random error being undetected is $2-16$. The 16-bit primitive polynomial,g which is the minimal polynomial of a primitive element of the extension field (Galois field) $GF(pm)$, $g\left(a\right) = a_{16} + a_{15} + a_{12} + 1_{CRC}$ appending CRC bits to the original secret S (128-bits), they construct 144-bit data secure checked (SC). All operations take place in Galois field. System starts with concatenating x and y coordinates of minutiae (8-bits each) as $[x\ y]$ to arrive at the 16 bit locking / unlocking data unit (u). SC is used to find the coefficient of the polynomial p : 144-bit SC can be represented as a polynomial with 9 (144 /16) coefficients in $GF(216)$, with degree $D = 8$.



Si No	X	Y	Theta
0	139	325	90
1	131	326	107
2	135	318	120
3	150	332	258
4	145	318	66
5	90	324	112
6	133	273	185
7	106	254	345
8	138	222	190
9	181	245	44
10	186	210	34
11	135	186	11
12	231	212	44
13	199	131	32
14	110	113	175
15	173	96	5
16	212	89	201
17	77	105	350
18	203	72	11
19	66	57	330
20	89	19	330

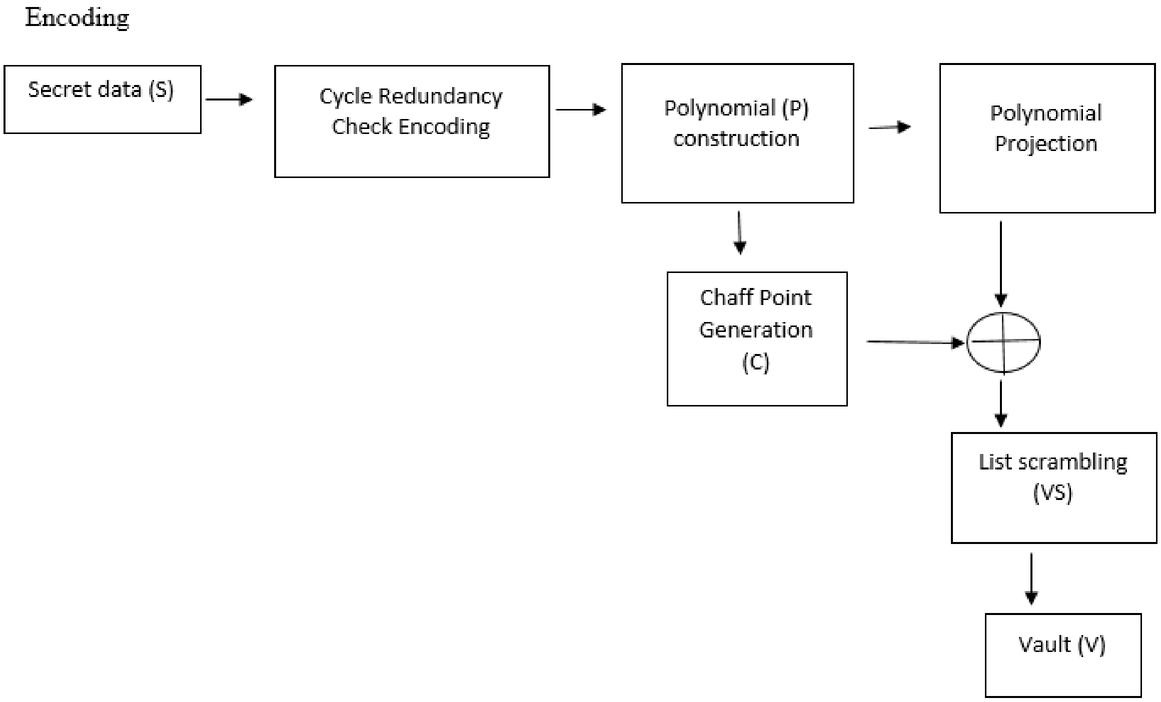
a) Fingerprint minutiae features for image from FVC 2004



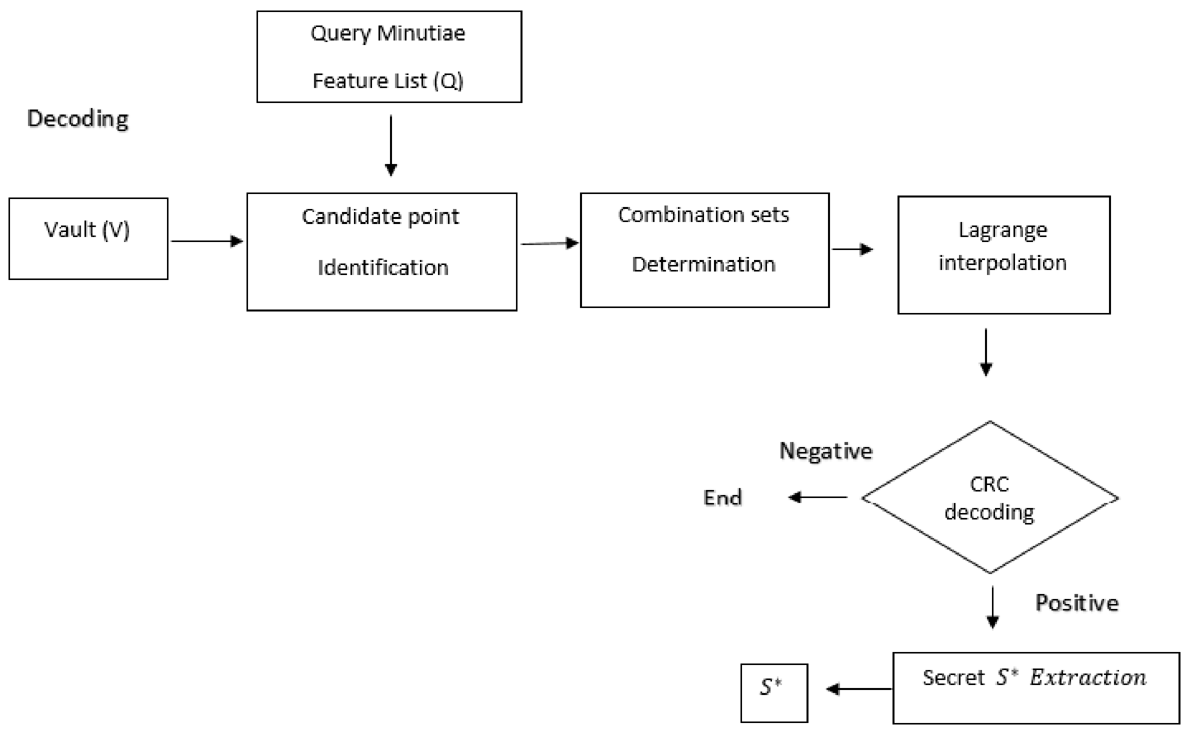
Si No	X	Y	Theta
0	121	247	180
1	95	228	345
2	170	222	52
3	126	196	191
4	177	185	34
5	125	161	6
6	186	106	18
7	98	87	175
8	162	71	0
9	67	79	345
10	193	46	16
11	54	31	330

b) Fingerprint minutiae features for cropped image FVC 2004

Figure 2 -10 Fingerprint minutiae features (x, y,θ) extracted using the Truth tool CUBS, developed at centre for Unified Biometrics and Sensors, University at Buffalo.


Encoding
Secret data (S)
Cycle Redundancy Check Encoding
Polynomial (P) construction
Polynomial Projection
Chaff Point Generation (C)
List scrambling (VS)
Vault (V)

(a)



(b)

Figure 2-5 Fuzzy fingerprint vault : (a) vault encoding, (b) vault decoding

Hence,

$$p(u) = c_8u^8 + c_7u^7 + .. + c_1u^1 + c_0$$

Evaluating $p(u)$ on the template minutiae features (T) to get genuine set$G$, starting with N template minutiae sorted according to ascending u values, u , G founded to be:

G = {(u_1, $p(u_1$)),(u_2 , $p(u_2$)),...(u_N , $p(u_N$))}

While the chaff set C generated randomly by $c_1, c_{2,}c_{3,} \dots \dots , c_M$ as M points in the field $GF(2^{16})$, with the constraint that they do not overlap with the $u_1, u_2, \dots . , u_N$namely $c_j \neq u_i$, j = 1,2,...M, i = 1,2,..., N . Then another set of M random points $d_1, d_{2,} \dots \dots , d_m$, with the constraint that the pairs (c_j,d_j), j = 1,2,...,M don't fall onto the polynomial $p(u)$. Chaff set C is then C = {(c_1, d_1), (c_2, d_2)…… (c_M, d_M)}, where $d_j \neq p(c\ j$), j = 1,2,...M . Union of these two sets, $G \cup C$, is finally passed through a list scrambler which randomizes the list, with the aim of removing any stray information that can be used to separate chaff points from genuine points. This results in vault set VS ,

VS = {(v_1, w_1),(v_2, w_2),,...,(v_{N+M}, w_{N+M})}
Along with *VS* , the polynomial degree *D* forms the final vault *V* . In unlocking part of proposed system the vault *V* using *N* queries minutiae {u_1^*, u_2^* , … . , u_N^*}

*Q = $u_1, u_2, \dots \dots, u_N$. The points to be used in polynomial reconstruction are found by comparing u_i^*,*i* = 1,2,..., *N* with the abscissa values of the vault*V* , namely *vl*, *l* = 1,2,...,(*N* + *M*). If any u_i^* is equal to *vl*, the corresponding vault point (*vl*,*wl*) is added to the list; has *K* points, where *K* ≤ *N* . For decoding a degree *D* polynomial, (*D* +1) unique projections are necessary. All possible combination of (D+1) was founded, among the list with size *K* , resulting in $\frac{K}{D+1}$ combinations. Lagrange interpolating polynomial was constructed for each combination, and it was given for

L={(v_1, w_1),(v_2, w_2),...,(v_{D+1}, w_{D+1})}
where the corresponding polynomial is

$$p^*(u) = \frac{(u-v_2),(u-v_3),......,(u-v_{D+1})}{(v_1-v_2),(v_1-v_3),......,((v_1-v_{D+1})} w_1 \qquad 2\text{-}3$$

This calculation is carried out in the Galois field, *GF*(216) to yield polynomial coefficients. The coefficients are mapped back to the decoded secret. For checking whether there are errors in this secret, a CRC primitive polynomial should be applied. Due to the definition of CRC, if the remainder is not zero, it is certain that there are errors. If the reminder is zero, there are no errors. In general if the query minutiae *Q* overlap with template minutiae *T* in at least (*D* +1) points for some combinations, the correct secret will be decoded, namely, *S** = *S* will be obtained. This denotes the desired outcome when query and template fingerprints are from the same finger. Proposed work suffers from complexity and alignment problems. They claimed that the complexity of attacks that can be launched by impostor users is high. It includes high time complexity due to the need for evaluating multiple point combinations during decoding. In, Uludag and Jain proposed a new biometric cryptosystem designed to overcome the security and privacy problems of previous biometric systems. They proposed to protect the biometric templates as a transformed version of the original template within a cryptographic framework.

Their implementation of fuzzy fingerprint vault used orientation field to derive the helper data which used to allow an alignment between query and template as an automatic solution of fuzzy vault alignment. Utilizing maximum curvature information (invariant to translation and rotation of fingerprints) of orientation field flow curves, the query fingerprint aligned with respect to the template via a variant of Iterative Closest Point (ICP) algorithm. Their alignment routine achieves reasonable accuracy, considering the small amount of data used for alignment.

Further, the helper data does not leak any information about the minutiae-based fingerprint template. The criticism, is that it is not sufficient to handle distortion and deformation of the fingerprint ridge increases as we move away from the centre of the fingerprint area towards the periphery. As well the designed system was dependent on user habituation and cooperation to increase the authentication accuracy. The system was developed for a positive identification scenario where the user is expected to be cooperative (for user convenience); the false rejects will reduce with increased user cooperation. Chung et al[19].proposed a geometric hashing technique to perform alignment in a minutiae-based fingerprint fuzzy vault but still has the problem of limited security. That is, the maximum number of hiding points (chaff points) for hiding the real fingerprint minutiae is limited by the size of the fingerprint sensor meanwhile the size of the fingerprint images captured and the possible degradation of the verification accuracy caused by the added chaff minutiae. All approaches assumed the number of chaff points was 200. Lee et al [20] proposed both the automatic alignment of fingerprint data and higher security by using a 3D geometric hash table. A number of chaff points for the proposed approach were more than in previous approaches by two times, as well as a complexity of cracking the proposed system was very high.

2.3 Summary

Cryptography and biometrics have been identified as two of the most important aspects of digital security environment, for various types of security problems the merging between cryptography and biometrics has led to the development of Bio-Crypto technology. The new technology suffers from several limitations e.g. biometric image based quality, validity, image alignment, cancelability, key revoking and repeatability. Therefore, the literature review is following the merging technology life cycle, it started with quality and validity analysis. This part reviews existing approaches for fingerprint image-quality estimation, including the rationale behind the published measures and visual examples showing their behaviour under different quality conditions. To the best of author’s knowledge, all published works are tackling the validity issue entire quality assessment, they assumed that all images are valid and the need just for quality assessment. Quality assessment was conducted in both field of information, e.g. local and global characteristics. The second part of reviewing according to the bio-crypt life cycle is Bio-crypt development approaches, where literature review divided it into three categories: Key hidden, one way function generator and Fuzzy key generation or on based of merging technique as: (1) loosely-coupled mode (biometric key release), the biometric matching is decupled from the cryptographic part. Biometric matching operates on the traditional biometric template: if they match, cryptographic key release from it is secure location, e.g. a server or smart card. (2) tightly-coupled mode (biometric key generation), biometric and cryptography are merged together at a much deeper level, where matching can effectively take place within cryptographic domain, hence there is no separate matching operation that can be attacked; key extracted from a collected heterogeneous mass (key/bio template) as a result of positive matching. The literature review highlights the remarkable problems and challenges that face the biometric cryptography such as:

- The alignment assumption in previous approaches limits their applicability's.
- Many proposals have failed to consider security engineering aspects, of which the most severe are the irrevocability of biometrics or key diversity and their low level of secrecy.
- No concrete implementation work was reported for the majority of approaches.

CHAPTER 3

FINGERPRINT IMAGE ANALYSIS

3.1 Introduction

Fingerprint is one of the oldest and most widely used biometric traits. A modern scientific fingerprint technology in the acquisition stage of system infrastructure is used due to low cost and simplicity of operation. For this purpose, a wide range of sensors are available commercially to attain a digital fingerprint image which makes it easy to obtain and then accept or reject the fingerprint image for further processing. Clarification of fingerprint image structure is crucial for many fingerprint applications, as well as the performance of built systems which relies on the validity and quality of captured images. Validity check will eliminate invalid images before starting the life cycle of fingerprint metadata enrolling for system processing cycle; therefore the overall benchmarking system accuracy will not be affected by rejecting an invalid image before getting in the system cycle. This chapter explains the basic characteristics of fingerprint images from local and global analysis points of view as well as the relationship between these factors and validity check results. A fingerprint is a group of associated curves. The bright curves are called valleys while the dark curves are called ridges Figure (3.1).

Fingerprint local structure constitutes the main texture like pattern of ridge and valley i.e. detailed pattern around a minutiae point, while valid global structure puts the ridges and valleys into smooth flow or the overall pattern of the ridges and valleys. Ridge to valley structure is analysed to detect image validity values while image quality is justified by its local and global structure. To study the locality and globality of the fingerprint pattern, we first define the fingerprint representation area where we can detect the region of interest (ROI); the image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutiae in the bound region are confusing with those spurious minutiae that are generated when the ridges are out of the sensor. ROI detection and segmentation described in section 3.3. The fingerprint pattern locality and global introduced in section

3.4. A proposed validity check algorithm based on ridge valley statistical weight analysis is discussed in section 3.4. Finally, Section 3.5 provides a summary and discussion of this chapter.

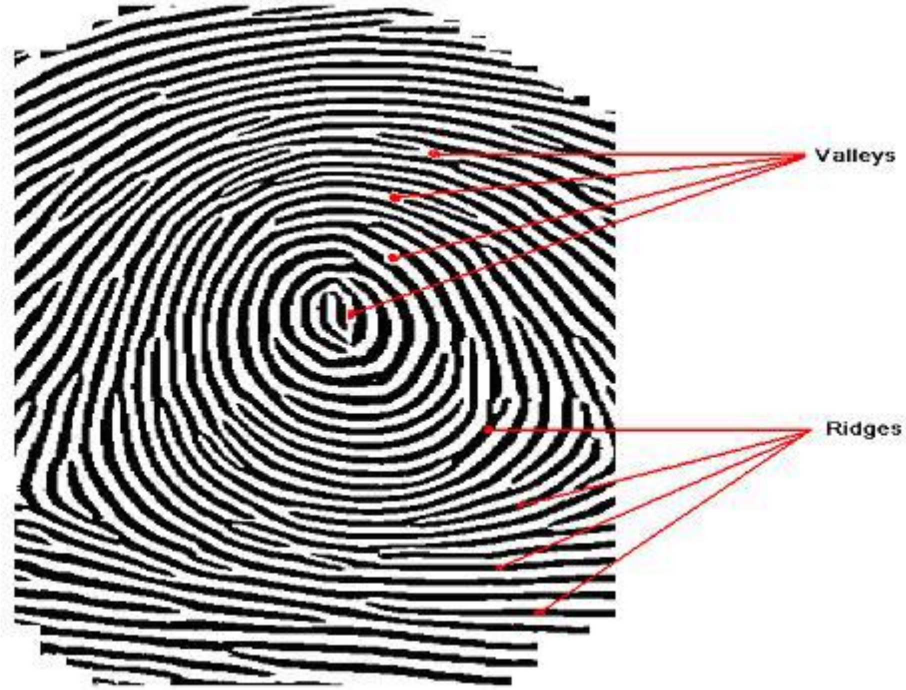


Figure 3-1 Ridges and Valleys of a fingerprint image

3.2 Fingerprint Representation Area

A good fingerprint representation should contain distinctive easily extracted information. Extracted information should be stored in a compact fashion, useful as input for future system models, e.g. verification and identification. Fingerprint image based representation, constituted by raw pixel intensity information, are prevalent among the recognition systems and source of biometric cryptography construction. However, the utility of the systems using such representation may suffer from some factors such as brightness variations, image quality variations, scars, and large global distortions present in the fingerprint image. Therefore, it is extremely difficult to extract robust features from a finger devoid of any ridge structure. Fingerprint ridge structure defined the fingerprint pattern search area. Where search area is a small area of fingerprint in which a feature is searched or where all the macro features are found (e.g. Ridge patterns, Ridge pattern area, Core point, Delta point, Type lines and Ridge count). The accurate search area is the whole perfect ridge pattern area. It is normally defined by diverging ridge flows that form a delta. It is designed to account for detected feature position deviations due to noise, processing variations. Increasing the search area is equivalent to reducing the scanning resolution and reducing the accuracy of detection of the feature position.

3.3 Fingerprint Object Segmentation

It is an essential process of fingerprint recognition to separate the ROI from the undesirable area. The focus of analysis is to the interior part of the fingerprint image. The word of interior is loosely defined as the portion of the image that is not at the boundary of the fingerprint and the blank space. Separation of foreground object from image background is called segmentation processing. Segmentation is the decomposition of an image into its components. A captured fingerprint image usually consists of two components, which are called the foreground and the background.

The foreground is the component that originated from the contact of a fingertip with the sensor. The noisy area at the borders of the image is called the background. The task of the fingerprint segmentation algorithm is to decide which part of the image belongs to the foreground and which part to the background. Accurate segmentation is very important for the validity, quality and reliable extraction of fingerprint features. Several approaches to fingerprint image segmentation were known from literature. In [21] the fingerprint is partitioned into blocks of 16×16 pixels. Then, each block is classified according to the distribution of the gradients in that block. In this method is extended by excluding blocks with a gray-scale variance that is lower than some threshold. In the gray-scale variance in the direction orthogonal to the orientation of the ridges is used to classify each 16×16 block. In the output of a set of Gabor filters is used as input to a clustering algorithm that constructs spatially compact clusters.

In fingerprint images are segmented based on the coherence, while morphology is used to obtain smooth regions. In [22], Yin et al proposed two steps for fingerprint segmentation to exclude the remaining ridge region from the foreground. The non-ridge regions and unrecoverable low quality ridge regions are removed as background in the first step, and then the foreground produced by the first step is further analyzed so as to remove the remaining ridge region. A fingerprint image usually consists of different regions: non-ridge regions, high quality ridge regions, and low quality ridge regions. Fingerprint segmentation is usually able to exclude non-ridge regions and unrecoverable low quality ridge regions as background so as to avoid detecting false features. In ridge regions, including high quality and low quality, there are often some remaining ridges which are the after image of the previously scanned finger and are expected to be excluded as background. However, existing segmentation methods do not take this case into consideration, and often, the remaining ridge regions are falsely taken as foreground. Bazen and Gerez [23] proposed a pixel features based method, where three pixel features, the coherence, the mean and the variance are used to segment fingerprint object. An optimal linear classifier is trained for the classification per pixel, while morphology is applied as post processing to obtain compact clusters and to reduce the number of classification errors. Fingerprint image should be segmented into three areas, clear area of the foreground or object region of interest, background and weak area which can be enhanced in the foreground. Previous literature has shown that a segmentation algorithm that is based on the pixel wise coherence, combined with some morphological operations, is capable of accurately segmenting fingerprints of very bad quality that cannot be processed by the variance-based methods. According to the information used in fingerprint segmentation, the methods can be generally divided into two categories: gray level-based and direction based methods.

3.3.1 Grey Level Segmentation

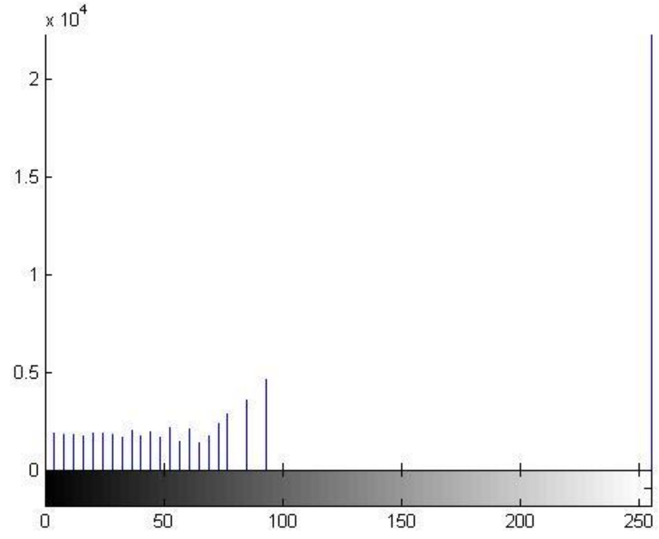
Grey level segmentation or thresholding or binarization is a conversion between a grey level image and a bi level one. This is the first step in several fingerprint image processing applications. Grey level segmentation can be understood as a classification between fingerprint object (ridge valley structure) and background in fingerprint image. The grey value at each pixel can be represented statistically by intensity histogram; therefore, the nature of grey level-based method is how to select an optimal threshold in the histogram to segment the object from background. It is shown that a fingerprint image has the characteristic that the foreground has bigger local contrast than that of the background, i.e., the histogram of local region contrasts must have two pinnacles. It is clear that thresholding is a fundamental tool for segmentation of grey level images when objects and background pixels can be distinguished by their grey level values. Given a digital image I (i, j), of dimension N_x ×N_y , so I (i, j) represents the intensity at location (i, j) with $0 \leq i \leq N_x$ and $0 \leq j \leq N_y$, $0 \leq I\ (i, j) \leq L - 1$. Here, L represents the maximum number of grey levels, and K (L) 2 = log is usually termed as the pixel depth or the number of bits/pixel for the image. Grey-level-based method working on base of quantifying the local contrast histogram into $0 \sim L - 1$ level, with the assumption of the
mean of contrast is T_0 , where T_{i+1} is calculated by:

$$T_{i+1} = \frac{1}{2} \left\{ \frac{\sum_{k=0}^{T_i} k * h_k}{\sum_{k=0}^{T_i} h_k} + \frac{\sum_{k=T_i+1}^{L-1_i} k * h_k}{\sum_{k=T_i+1}^{L-1_i} h_k} \right\} \qquad 3\text{-}1$$

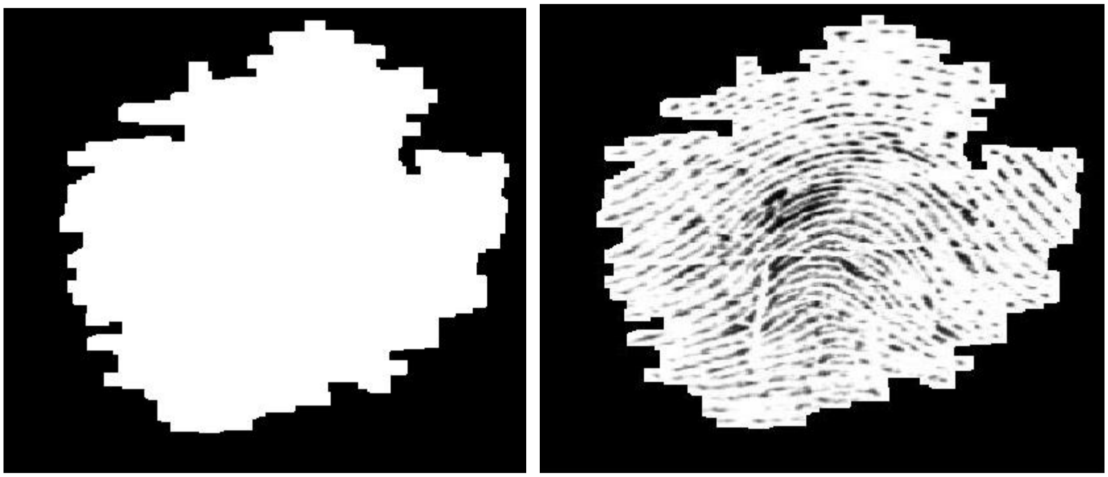
where h_k is the number of pixels whose grey value equal k .

The iteration finishes when $T_{i+1} = T_i$. According to the value when iteration finishes (T_i), get the segmentation threshold kT_i , where the coefficient k can adjust the severe degree of segmentation. When k is bigger, the foreground is smaller. To find the ROI by given method, image partitioned into a number of blocks by a rectangle or square grid. Each interior (fingerprint portion) block is more likely to contain more bright areas than the blocks on the boundary and in the blank regions. As shown in Figure (3-2 (a)) a 2D fingerprint image, where (b) shows the histogram of the gray-scale fingerprint image in (a). Using the Otsu optimum threshold method, a threshold value should be found for the image segmentation. Each pixel of the fingerprint image can be classified into one of two classes: bright or dark. A pixel belongs to bright if its value is greater than the threshold value; otherwise it belongs to the dark class. The thresholded image should be partitioned into the union of disjoint blocks, squaring blocks. A percentage of white area within each block is computed, its value should be compared with a threshold value. If it is greater than the threshold, then all pixels in the block should be set to white, otherwise black.

Fingerprint image.



Histogram of a fingerprint image



(a) (b)

Region of interest (ROI) ROI of a fingerprint image.

(c) (d)

Figure 3-2. (a)Fingerprint image, (b) histogram of fingerprint image, (c) region of interest, (d) ROI of a fingerprint image

In the resulting image, the white region represents the region of interest (ROI), which is shown in Figure (3-2 (c)). Overlaying (c) on (a), the region of the fingerprint image produced for further processing. The result is shown in Figure (3-2 (d)). The obtained result showing that segmentation of the original object from the background starts as expected from the clear separation of modes in the histogram, and it was very effective for all type of fingerprint images, i.e. poor, and good quality. Fingerprint image segmentation based on grey level method is not so easily done in fingerprint images with low contrast. For these cases, image enhancement techniques must be used first to improve the visual appearance of the fingerprint image. Another major problem is the setting of correct threshold value or automated threshold which will classify pixel as object or background.

3.3.2 Directional Segmentation

The main distinction between foreground and background of fingerprint image is the strength of the orientation of the ridge-valley structures Figure (3-3(a)). Therefore, the coherence can be used very well as segmentation criterion. Since a fingerprint mainly consists of parallel line structures, the coherence will be considerably higher in the foreground than in the background.

The coherence in a window [w] centred at (x, y) of intensity image I (x, y) can be computed with a reference of gradient values

{G_x (x y), G_y (x y)} at that intensity pixel (x, y), using gradient values to find the dominant ridge orientation estimation which is mathematically computed by:

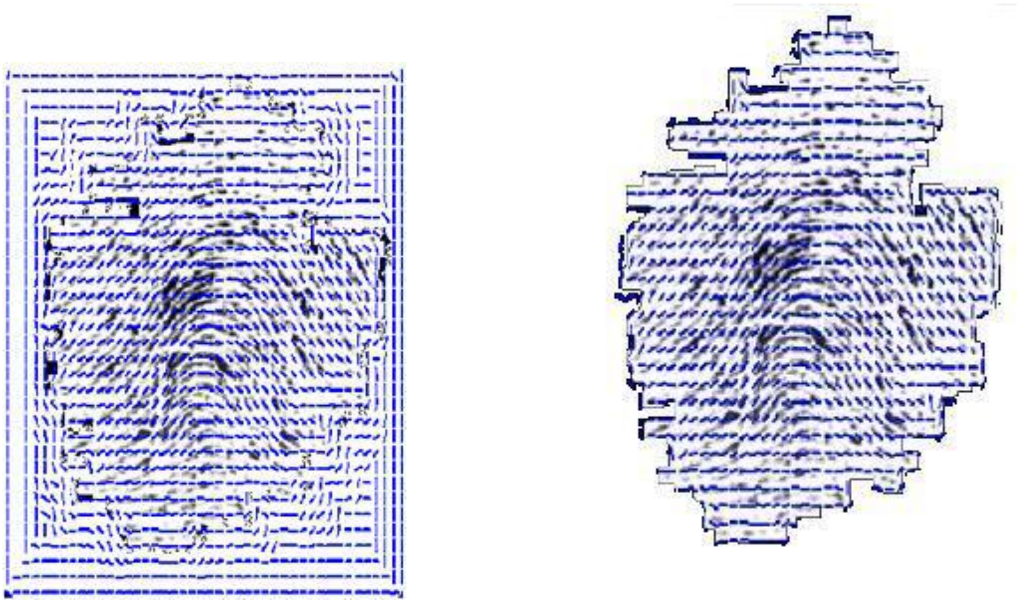
$$O_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} 2 * G_x(u,v) * G_y(u,v) \qquad 3\text{-}2$$

$$O_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (G_x^2(u,v) - G_y^2(u,v)) \qquad 3\text{-}3$$

$$O_E(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (G_x(u,v) - G_y(u,v))^2 \qquad 3\text{-}4$$

$$\text{Coh}=\sqrt{\frac{O_x^2(i,j)+O_y^2(i,j)}{O_E(i,j)*w*w}} \qquad 3\text{-}5$$

So, if the *Coh* is larger than a threshold, the block is considered as foreground, otherwise, it belongs to background. The segmentation result of this method is shown in Figure (3-3(b)). Both previous methods were chosen to segment the fingerprint object because they can correctly segment the fingerprint images whose boundary is distinct. On the other hand, they were sensitive to the quality of image, i.e. good investigators of low quality fingerprint images. Grey level-based method gives an indication of wetness and dryness of fingerprint images, while the direction-based method shows orientation contours of ridge and valley structure, both indication results are very useful in validity estimation as well as in quality benchmarking. Finally, Segmenting an image simplifies it, making it easier to analyse and is therefore a key part of computer vision, image processing, and security generation.



Orientation of fingerprint image (a)

Directional segmentation of (a) (b)

Figure 3-3. (a) Orientation of fingerprint image, (b) Directional segmentation of fingerprint image.

3.4 Fingerprint Pattern Analysis

It was defined in section 1, that fingerprints are the patterns on the inside and the tips of fingers. The ridges of skin, also known as friction ridges, together with the valleys between them form unique patterns on the fingers. Fingerprint pattern analysis from an image anatomy processing point of view is a deconstruction of object patterns, e.g. ridge and valley structure therein form one of a number of different fingerprint patterns used in a fingerprint system. Fingerprint local structure constitutes the main texture-like pattern of ridges and valleys within a local region. The local structure analysis of a ridge output extraction, i.e. minutia, describes a rotation and translation invariant feature of that minutia in its neighbourhood. A valid global structure puts the ridges and valleys into a smooth flow for the entire fingerprint; it reliably determines the uniqueness of a fingerprint. Both local and global structuring analyses determine the quality and validity of a fingerprint image.

3.4.1 Local Analysis

A fingerprint image local representation consists of several components, each component typically derived from a spatially restricted region of the fingerprint. Major representations of the local information in fingerprints are based on finger ridges, pores on the ridges, or salient features derived from the ridges. The most widely used local features are based on minute details called minutiae of the ridges. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending or local discontinuities in the fingerprint pattern. A total of 150 different minutiae types havebeen identified. In practice only *ridge ending* and *ridge bifurcation* minutiae types are used in fingerprint systems[2]. Examples of minutiae are shown in Figure (3-4).

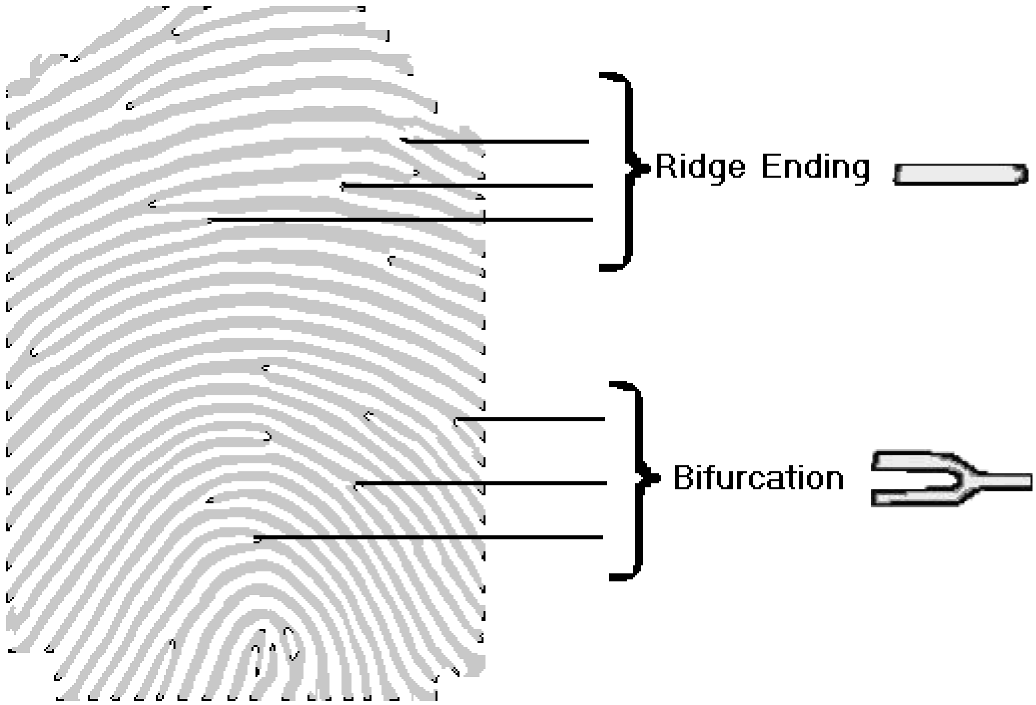


Figure 3-4 Examples of minutiae type

The localization of the minutiae in a fingerprint forms a valid and compact representation of the fingerprint. The validity judgment of fingerprint image is dependent on the following factors: image contrast, graphical representation of fingerprint elements, like ridge and valley clarities and noise infection. The local information of fingerprint image could be obtained by pixel values representation, where pixels indicate the light intensity of the fingerprint image element as well as its grey value representation on grey value map. It is useful for some fingerprint processing techniques, like threshold calculation, segmentation based on grey level, enhancement based on pixel representation and validity check based on enhancement percentages. As local analysis gives contrast information of ridge and valley structure so the goodness, dryness and smudginess of the whole fingerprint can be determined. In this case pixel is a good predictor of image information, for example, the black pixels are dominant if a fingerprint is wet, the average thickness of ridge is larger than one of valley, and vice versa on a dry fingerprint.

A severity of fingerprint image damage can be determined by statistical properties, i.e. standard deviation and mean value in a local blocks division of fingerprint. A valid fingerprint image tends to have a small deviation value for both ridge and valley.

3.4.2 Global Analysis

Global representation is an overall attribute of the finger and a single representation is valid for the entire fingerprint and is typically determined by an examination of the entire finger. The global structure is the overall pattern of the ridges and valleys. Fingerprint images are very rich in information content. The main type of information in the fingerprint image is the overall flow information, which is defined by the pattern of the ridges and valleys in the fingerprint [33]. Fingerprint global structure provides discriminatory information other than traditional widely used minutiae points. Fingerprint global structure such as global ridge structure and singularities is used to dedicate the fingerprint classification. It is beneficial to the alignment of the fingerprints which are either incomplete or poor quality. The global structure analysis is used to certify the localized texture pattern of the fingerprint images while ridge to valley structure is analyzed to detect invalid images. Fingerprint images possess continuity and uniformity as the general characteristic. Continuity is found along the orientation change while uniformity is observed all over the image for its ridge and valley structure, they are considered as a fingerprint global factor. Global uniformity and continuity ensures that the image is valid as a whole. The commonly used global fingerprint structuring features are:

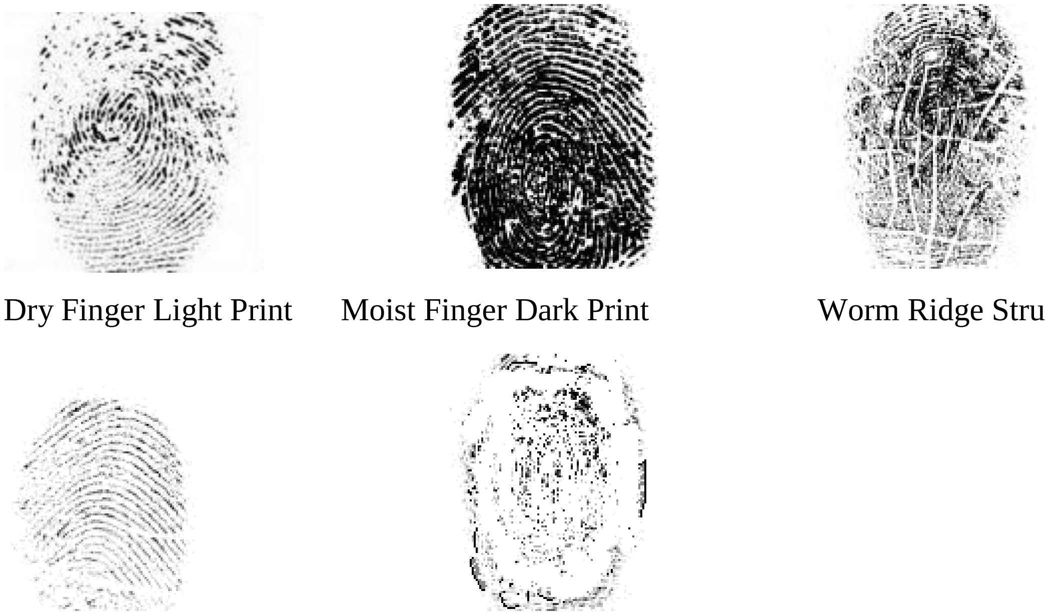
- *Singular points* – discontinuities in the orientation field. There are two types of singular points. A core is the uppermost of the innermost curving ridge [77], and a delta point is the junction point where three ridge flows meet. They are usually used for fingerprint registration and fingerprint classification.

- *Ridge orientation map* – local direction of the ridge-valley structure. It is commonly utilized for classification, image enhancement, and minutia feature verification and filtering.
- *Ridge frequency map* – the reciprocal of the ridge distance in the direction perpendicular to local ridge orientation. It is formally defined and is extensively utilized for contextual filtering of fingerprint images.

This representation is sensitive to the quality of the fingerprint images. However, the discriminative abilities of this representation are limited due to absence of singular points.

3.4.3 Validity Statistical Analysis

Most available fingerprint based systems use global and/or local fingerprint features for enhancement, alignment and matching purposes, therefore feature extraction is very sensitive to validity, integrity, and quality of source images. For instance, false features extracted may appear due to poor and invalid fingerprint factors such as: physiological, e.g. dry fingers, worm, and finer ridge structure, behavioral factor, e.g. uncooperative or nervous subject, environmental factor, e.g. humidity, temperature and ambient light, operational and technological factor, e.g. high throughput, reduced capture time and unclean scanner platen and interaction usage, this is shown in the quality image illustration, Figure (3-5),. Enrolling invalid and missed image features degrades the performance and accuracy benchmarking of system production. A rejection of invalid examined images will reduce system processing time, and increase system reliability. It is therefore essential to design an automatic pre-enrollment step that examines and checks the validity of captured images. There are a number of fingerprint image quality assessment algorithms but none of them tackle the validity factors and total image information within visual quality. A proposed objective validity check approach correlates with perceived quality measurement. To the best of knowledge, the validity factor of fingerprint image is not studied well in any of fingerprint quality estimation method. All reviewed methods concentrate on quality computation based features and classifiers, however these methods as well as reviewed schemes cannot distinguish some invalid images from the valid ones. Validity statistical analysis could act as a prequality step to eliminate invalid images before applying any of quality assessment schemes.



Dry Finger Light Print Moist Finger Dark Print Worm Ridge Structure

Poor Finger Placement None Object Structure

Figure 3-5. Sample images, with different validity and quality

CHAPTER 4
PROPOSED WORK

The biometrics is integrated with cryptography in two ways, namely,
(i) biometric based key release and
(ii) cryptographic key generation from biometric data.

4.1 Biometric Based Key Release

In this scheme, cryptographic key is a secret and biometric data is the authenticator to protect that secret. The cryptographic key is released from the cryptographic construction only when genuine biometric data is provided. Fuzzy vault [24] and fuzzy commitment schemes [25] are the popular cryptographic constructions to bind a key with biometric data. In fuzzy commitment scheme, a binary string (bS'ring) of equal size of cryptographic key (K) is derived from biometric template and the key which is another binary string is XORed with bstring, i.e., bstring XOR Hao et al. [25] proposed a biometric based fuzzy commitment scheme, where randomly generated cryptographic key K is protected by a binary code derived from iris.

In the existing work of key release, fingerprint based fuzzy vault scheme is proposed by many researchers [26]. In literature, coordinate of the minutiae points are used to hide a secret key (K) using a cryptographic construction based on fuzzy vault. The vault releases a cryptographic key for a user who is able to present a query instance of genuine fingerprint to the vault as input. Similarly, Nandakumar et al. proposes a fingerprint based fuzzy vault scheme [24] where (x, y) -coordinates and alignment angle of the minutiae points are used to bind cryptographic key with user's fingerprint data.

4.2 Biometric Based Key Generation

Biometric based cryptographic key generation systems use biometric data, i.e., biometric features to derive a binary string of required length for cryptographic application. In literature, most of the biometric traits, like face [27], fingerprint [28],[29],[30], iris[31], voice[32], signature[33] etc. are used for cryptographic key generation. In most of the fingerprint based key generation approaches, key is generated from the biometric features of user. In fingerprint minutiae points are used to generate cryptographic key using a user defined key generation algorithm. Multi-modal biometrics is also reported in literature to generate cryptographic key. In fingerprint and iris are used to generate a cryptographic key with the help of feature level fusion between two modalities of biometrics. In the literature, key generation depends only on the biometric data of user in most of the existing work. If the biometric data is compromised by the adversary anyway then, the key will be compromised and it results that the biometric becomes useless forever.

4.3 PROPOSED METHODOLOGY

Our proposed approach has three components, namely, template generation, key generation and key regeneration. Each steps are stated in details in the following.

A. Template Generation

Fingerprint features (F^A) are extracted from the fingerprint image (g_A) of user (A) using feature extraction algorithm (f). In this approach, minutiae points are detected as features from the fingerprint image (i.e., m_i = f (g_A) for i = 1, 2,…..,n and m_i € F^A, where n is the total number of minutiae detected from g_A)

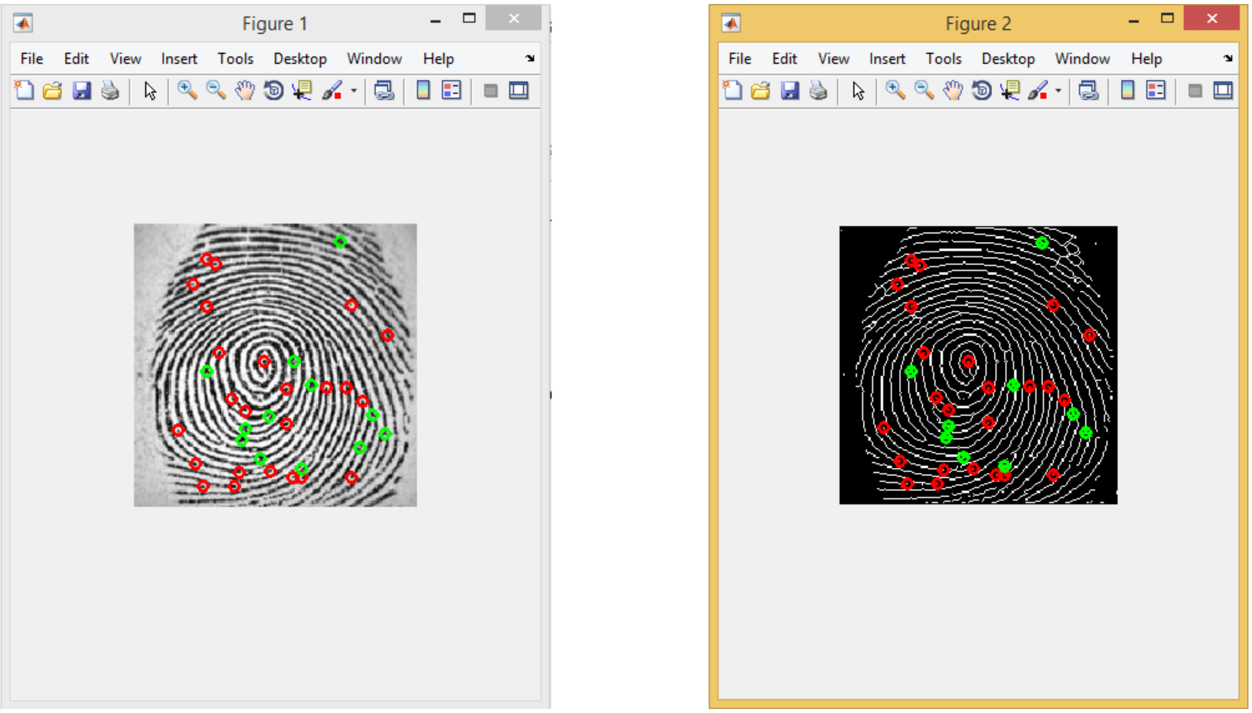


Fig 4.1 Minutiae points extraction

Minutiae points are represented by the triplet of (x_i,y_i, Q_i) where (x_i,y_i) is the coordinate values and Q_i is the alignment angle of minutiae points m_i. In our approach, (x, y) coordinate is used as minutiae points. The fingerprint template (F_{TA})) of user A is generated from the minutiae points F^A. The steps of template generation process are given below.

1. All distances ($d_{i,j}$) between the distinct minutiae points (i.e., m_i and m_j are computed and stored in a matrix D.

$d_{i,j}$= $\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$

D = [$d_{1,1}, d_{1,2}, \ldots \ldots, d_{k,k+1}, d_{k,k+2}, \ldots \ldots, d_{n,n}$]

2. Distances are sorted and only unique distances are stored in vector U_A as follows

U_A = [$u_1, u_2, \ldots \ldots \ldots ., u_q$]

where, i is a distance, $u_1 \leq u_2 \leq u_3 \leq \ldots\ldots \leq u_q$ and there are q numbers of unique distances in the vector U .

3. The unique distances are moved to another vector F_{TA} such a way that the value of u_i, will be stored at a location of that vector where the index value is equal to the u_i ,

. F_{TA} [u_i] = u_k

4. The empty positions of F_{TA} are filed with zero F_{TA} [t] = 0 , where, t ∉ U_A .

In this way, template F_{TA} is generated with zero and non-zero values. The size of the template depends on the maximum distance max(U_A) .This process of template generation is shown in Fig.4.3. In the example, six minutiae points are taken as F^A i.e., F^A = [a,b,c,d,e,f] . The distances are assumed as given in Fig.4.3 (b). There are 6x6 = 36 distances shown in the matrix. The template is shown in Fig.4.3 (d).

4.4 Key generation and message encryption

Fingerprint template is used to generate cryptographic key. In this work, key generation is simple. The template F_{TA} is taken and each element of F_{TA} generates a bit of the key. Overall steps of key generation by the user are shown in Fig 4.2. The steps are described below.

1. User A generates fingerprint template F_{TA} from fingerprint features.

2. User selects an element F_{TA} [i] of template and puts 0 or 1 in the same location of key (i.e., K[i]).

3. User puts 1 in the first location of key vector K (i.e.,K[i] = 1).

4. User puts 0 at K[i] if F_{TA} = 0 (i.e., K[i] = 0) and puts 1 if $F_{TA} \neq 0$ (i.e., K[i] = 1).

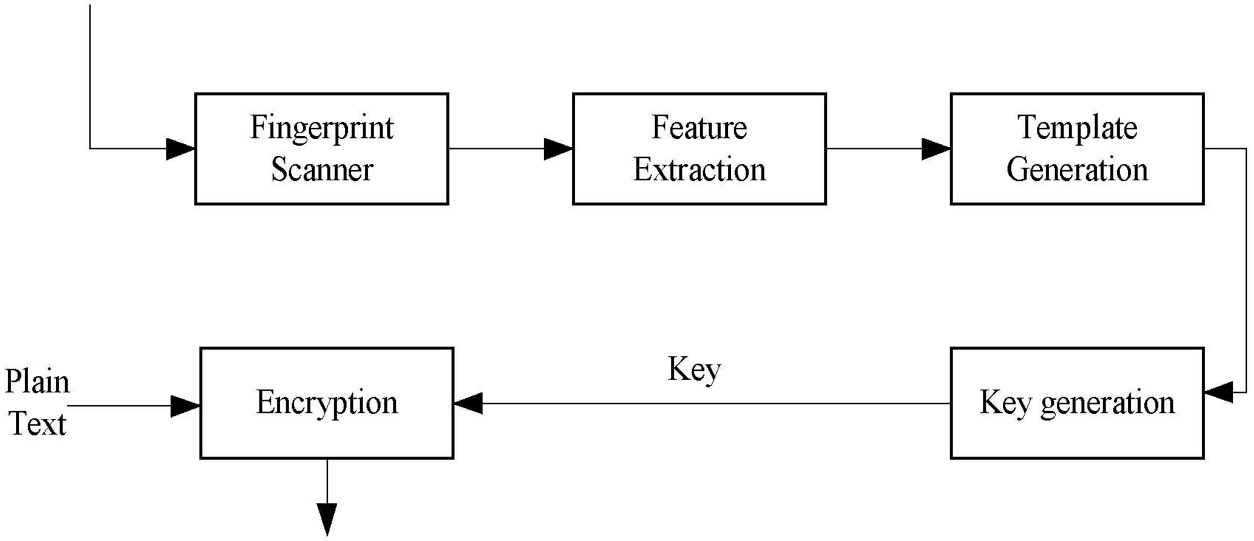
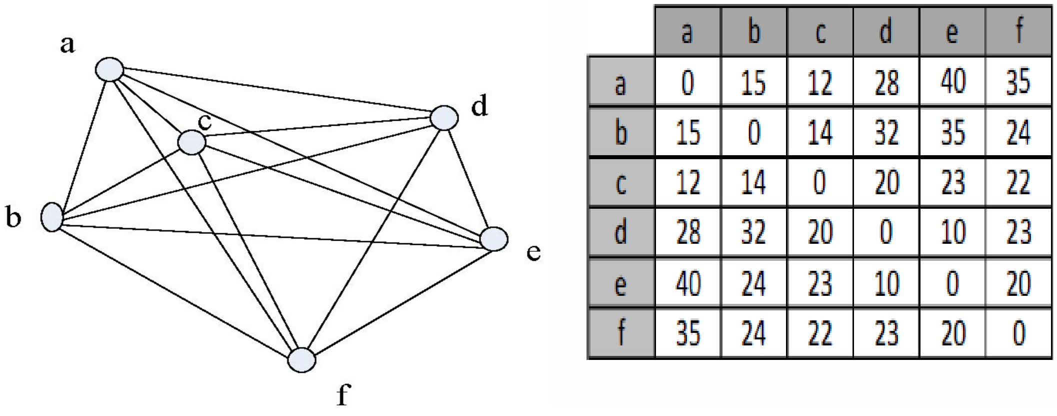


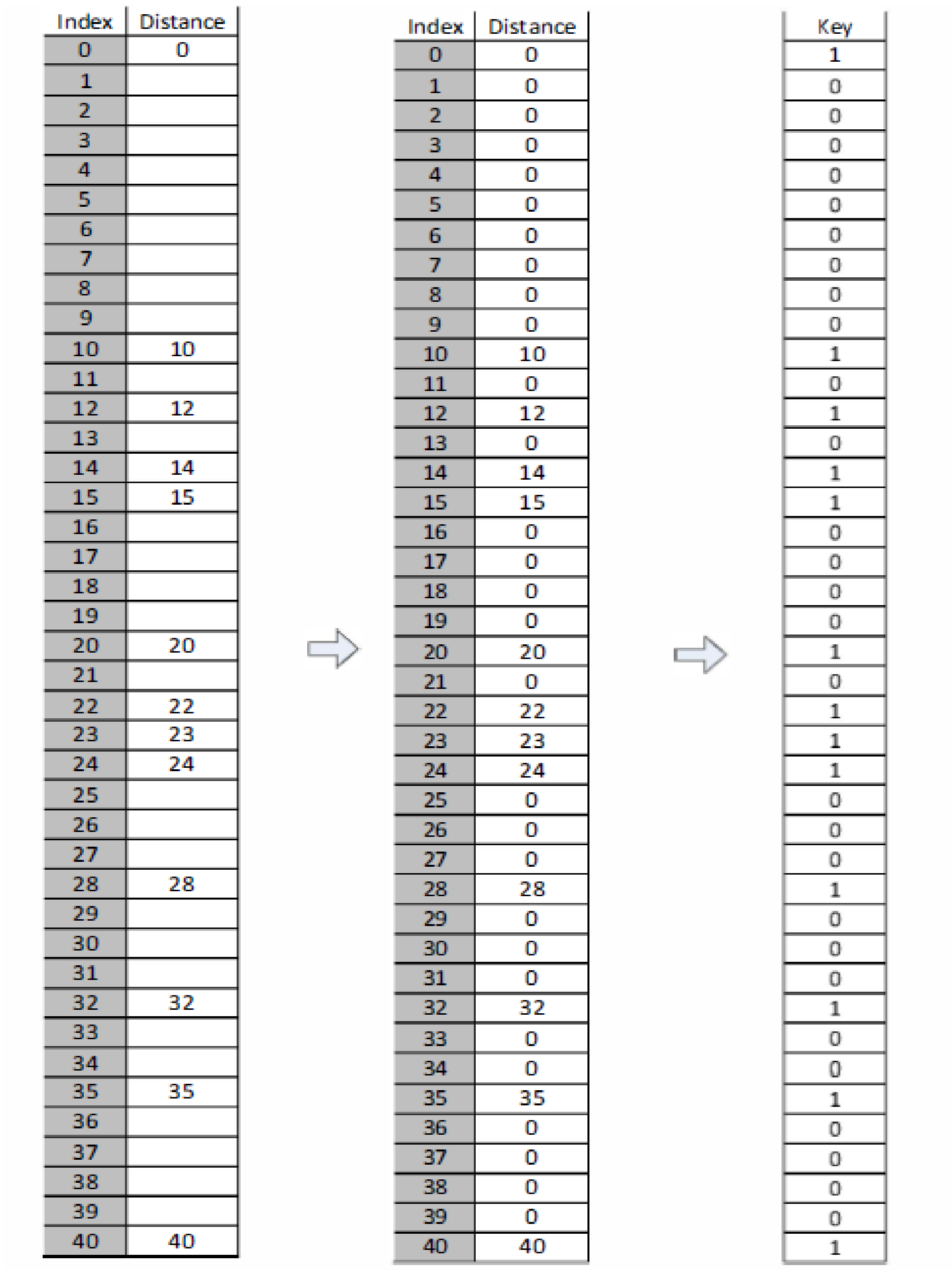
Fig. 4.2. Key generation and message encryption process

This way, cryptographic key K is generated from fingerprint template F_{TA} . The key is used for message encryption and then it is discarded. A sample key is shown in Fig.4.3 (e) which is generated from template F_{TA}.



	a	b	c	d	e	f
a	0	15	12	28	40	35
b	15	0	14	32	35	24
c	12	14	0	20	23	22
d	28	32	20	0	10	23
e	40	24	23	10	0	20
f	35	24	22	23	20	0

(a) (b)



Index	Distance
0	0
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	10
11	
12	12
13	
14	14
15	15
16	
17	
18	
19	
20	20
21	
22	22
23	23
24	24
25	
26	
27	
28	28
29	
30	
31	
32	32
33	
34	
35	35
36	
37	
38	
39	
40	40

(c)

Index	Distance
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	10
11	0
12	12
13	0
14	14
15	15
16	0
17	0
18	0
19	0
20	20
21	0
22	22
23	23
24	24
25	0
26	0
27	0
28	28
29	0
30	0
31	0
32	32
33	0
34	0
35	35
36	0
37	0
38	0
39	0
40	40

(d)

Key
1
0
0
0
0
0
0
0
0
0
1
0
1
0
1
1
0
0
0
0
1
0
1
1
1
0
0
0
1
0
0
0
1
0
0
1
0
0
0
0
1

(e)

Fig 4.3 (a) Minutiae to minutiae distance, (b) Distance matrix, (c) Storing unique distances in a vector of size of maximum distance, (d) Non-existing distances are assumed as zero and blank locations of the vector are filled with zero. This is used as fingerprint template (e) Cryptographic key from template

4.5 Key regeneration and cipher text decryption

The message (plain text P) is encrypted (C = E K (P)) and cipher text (C) is stored in system. The key K is needed to be regenerated from the same fingerprint to decrypt the cipher text. Let us assume, the person A captures another instance of fingerprint of same fingerprint. Let, the instance is g' A and the extracted feature set is FA' (i.e., FA' = f(g'A)) where f is the same minutiae detection algorithm used at the time of key generation for message encryption). The steps are given below.

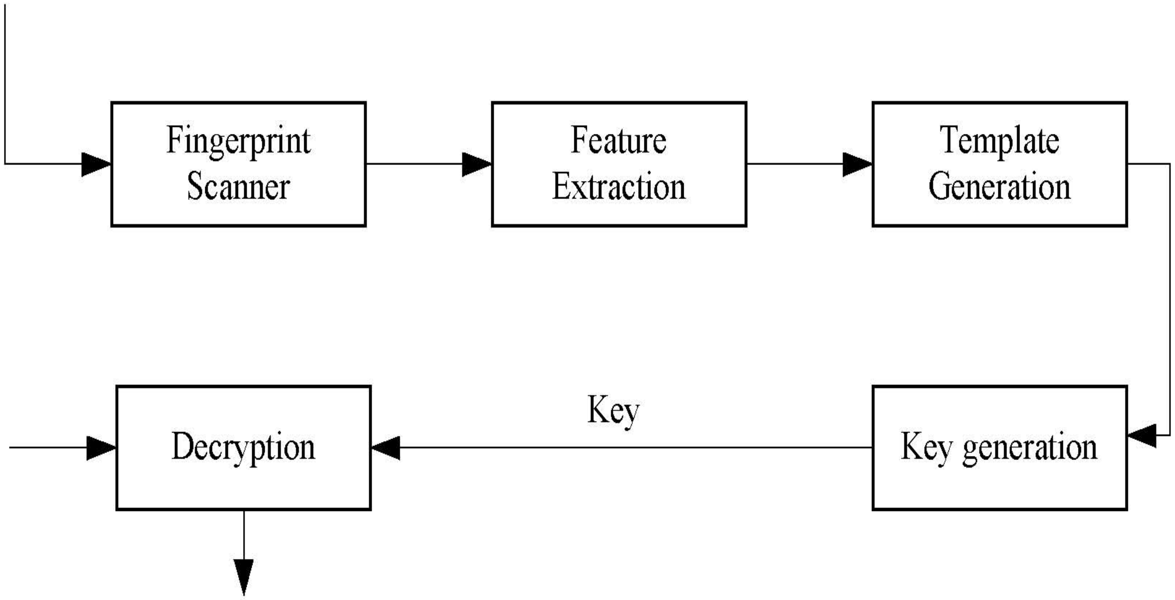


Fig 4.4 Key regeneration and cipher text decryption process

The overall steps of the key regeneration process are shown in the Fig.4.4.

1. User A produces his fingerprint to the fingerprint scanner and fingerprint image (g'_A) is captured.

2. Fingerprint features are extracted from the captured fingerprint image g'_A.

3. Query fingerprint template F'_{TA} is generated from extracted features $F^{A'}$ following the same process.

4. Cryptographic key K' is generated from F'_{TA}.

5. Cipher text (i.e., encrypted message) C is converted in plain text using decryption algorithm (i.e., P = DK' (C)). This way the cryptographic key is regenerated at the time of decryption of cipher text. The key K which is used for encryption and the key K' which is generated to use in decryption process should be exactly same otherwise the exact plain text will not be recovered.

CHAPTER 5

RESULT ANALYSIS

In our approach, fingerprint is used as input biometric trait. The experiment is carried out to generate fingerprint based cryptographic key for encryption and decryption. We observe the similarities between the keys generated from different instances of same fingerprint image. Our experiment also observes the strength of the key with respect to the impostor key which is generated from impostor's fingerprint.

Database

Fingerprint from fingerprint database FVC2004 (Set A) is used as input fingerprint in our experiment. The FVC2004 database consists of four datasets like DBl, DB2,DB3 and DB4. Fingerprints of DB4 dataset are synthetic fingerprint but remaining datasets consist of real fingerprints. Each dataset consists of 800 fingerprints of 100 persons with 8 instances of each person. The DB2 (Set-A) of FVC2004 contains 800 fingerprints and optical sensor "U,are.U 4000" by Digital Persona is used to capture fingerprint image of size 328x 364 at 500 dpi.

Experimental Setup

In our experiment, fingerprint from FVC2004 database (Set DB2A) is used as genuine and impostor fingerprints. To measure the accuracy of fingerprint based cryptographic key, a fingerprint instance of a person is considered to generate encryption key. The remaining instances of that fingerprint of the same person are taken as query fingerprint. The query fingerprint is used to generate test key and it is compared with the encryption key. The similarity between two keys is measured with respect to Hamming distance. If every bits of both keys are similar then the Hamming distance will be zero otherwise the distance will be similar to the total dissimilar bits. This way, the key is also compared with a key which is generated from impostor fingerprint template. Genuine key is generated from an instance of fingerprint and remaining seven instances are used to generate test key. If the keys generated from the instances of similar fingerprints are same then it is a genuine matching otherwise it is false non match. To observe genuine match and false non match ratio, total number of genuine tests is ((8*7) / 2) *100 = 2,800. Similarly, False Acceptance Rate (FAR) is also observed in our experimental result. For FAR (False Acceptance Ratio) or FMR (False Match Ratio) computation, first instance of each person's fingerprint is compared with the first sample of the fingerprint of remaining person's. The total number of false acceptance tests is ((100*99)/2) = 4,950.

In our approach, fingerprint features (i.e., minutiae points) are detected using MATLAB software. In our experiment, (x, y) coordinate values of minutiae points are used to generate template. Euclidean distance between two minutiae points is considered as distance between two minutiae points. The length of cryptographic key is 256 bits in our experiment.

Experimental Result

To measure the similarities and dissimilarities between two fingerprint based cryptographic keys, a predefined threshold value (in bits) is used as the indicator. If the difference between two keys is less than the threshold, then it is counted as a matching. Now if the test key is generated from the set of fingerprint instance of same person then it is a genuine matching. If the key is generated from different set of fingerprint instance of different person then it is taken as false matching. In our experiment, both, false rejection and false matching are investigated. According to the experimental result shown in Fig 5.1 the FRR is the maximum when threshold value is the minimum and FRR is the minimum when the threshold is the maximum. The maximum threshold value results maximum FMR, i.e., maximum threshold value minimizes the inter-person variability.

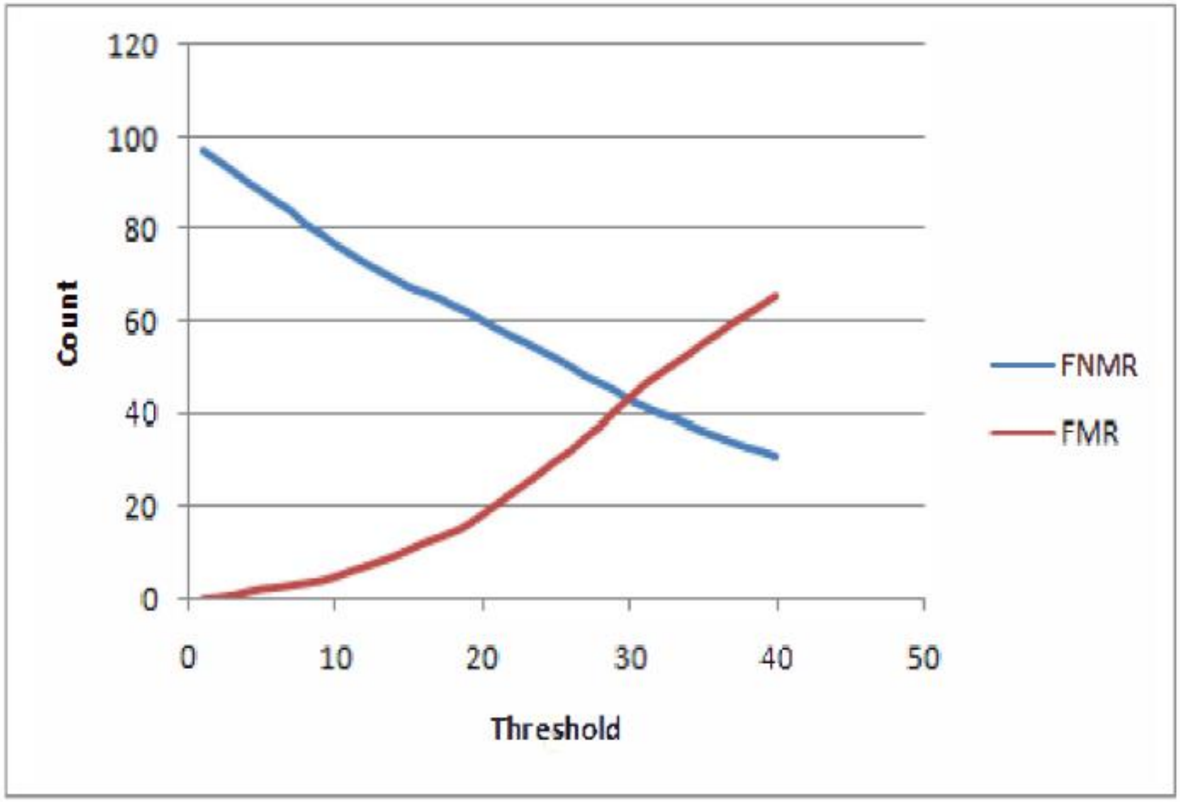


Fig. 5.1. FNMR vs FMR for FVC2004 DB2(A)

Similarly, we have also investigated the FMR vs. GRR (Genuine Rejection Rate) which is shown in Fig.5.2

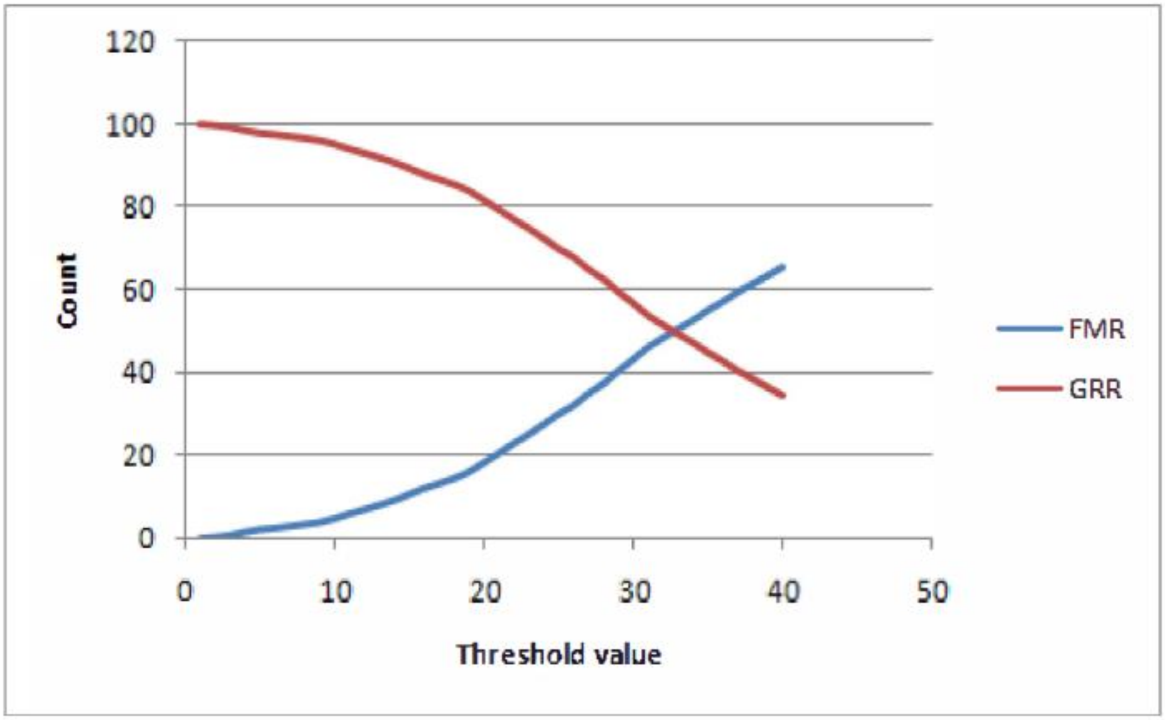


Fig. 5.2 FMR vs GRR for FVC2004 DB2(A)

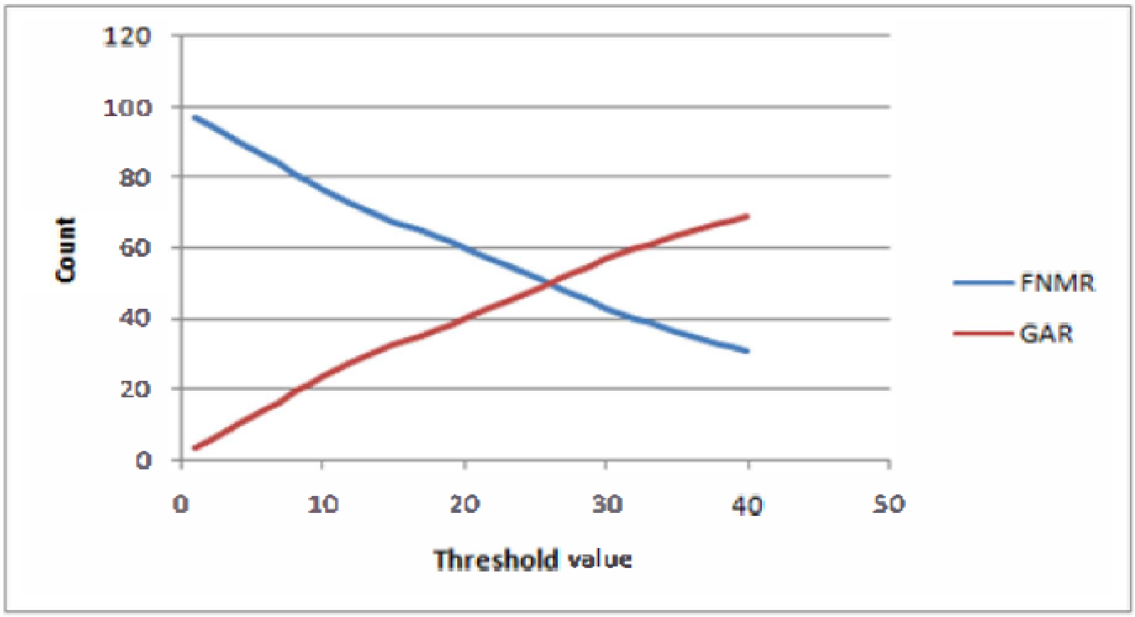


Fig. 5.3 FNMR vs GMR for FVC2004 DB2(A)

The FNMR of the keys is also plotted against genuine match ratio (GMR) which is shown in Fig.5.3.

Security Analysis

Fingerprint based cryptographic key is secured. The attacker does not have any knowledge about biometric of genuine user. The attackers can try to generate a key from his fingerprint. In the experimental result, it is observed that inter-user variation of fingerprint template opposes to generate a genuine key from impostor fingerprint template. The information about fingerprint of genuine user is not recoverable as the key does not leak information about the minutiae points. Moreover, the key can be converted into revocable key by using any shuffling based transformation of the template vector.

CHAPTER 5

CONCLUSION AND FUTURE WORK

Cryptography and biometrics are integrated with each other to improve security of cryptography. In traditional symmetric cryptography, key is generated randomly and user needs to remember the random key. It is really very difficult to memorize a long and random key as the key is not strongly linked with user. In this paper, the key is generated from users fingerprint and the key is linked with user's biometrics which removes the problem of key remembering by users. The proposed approach also provides an option to revoke cryptographic key. The key is secured as the key is generated from fingerprint with the help of a random sequence. The key does not leak any information about the original fingerprint image.

Cryptography is the strongest entity for information and network security whereas; biometric is the most trustworthy in authentication system. The problem of cryptography is with the management of cryptographic key. Biometric is used to address that problem of cryptography. In this approach, we have used fingerprint of user to generate a fingerprint based cryptographic key. There is no need to remember the key as it is generated from user's fingerprint. It also ensures the non-repudiation to information security. This approach also can be implemented using different biometric traits like iris, face, voice etc.

REFERENCES

[1] P. Reid, *Biometrics and Network Security*: Prentice Hall PTR, 2003.

[2] A. Bodo, "Method for producing a digital signature with aid of a biometric feature." Germany: German patent DE 42 43 908 A1, 1994.

[3] P. Janbandhu and M. Siyal, "Novel biometric digital signatures for internet based application," *inf. Manage. Comput. Secur*, vol. 9, pp. 205-212, 2001.

[4] G. J. Tomko, C. Soutar, and G. J. Schmidt, "Fingerprint controlled public key cryptographic system." USA: US Patent 5680460, Oct. 21, 1997.

[5] C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. V. Kumar, "Biometric encryption using image processing," *SPIE, Optical Security and Counterfeit Deterrence Techniques II*, vol. 3314, pp. 178-188., 1998.

[6] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B.V.K. Vijaya Kumar, "Biometric Encryption," in *ICSA Guide to Cryptography*: McGrow-Hill, 1999.

[7] C. R. Costanzo, "Biometric cryptography: Key generation using feature and parametric aggregation," Online Technical Report, 2004.

[8] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," presented at IEEE Symposium on Security and Privacy Proceedings, USA, 1998.

[9] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," presented at Proceedings of the 6th ACM conference on Computer and communications security, 1999.

[10] A. Guven and I. Sogukpinar, "Understanding users' keystroke patterns for computer access security," *Elsevier Science of Computers and Security*, vol. 22,pp. 695-706, 2003.

[11] H. Feng and C. C. Wah, "Private key generation from on-line handwritten signatures," *Information Management & Computer Security*, vol. 10, pp. 159-164,2002.

[12] Y. W. Kuan, A. Goh, D. Ngo, and A. Teoh, "Generation of Replaceable Cryptographic Keys from Dynamic Handwritten Signatures," in *Advances in Biometrics*, 2005, pp. 509 - 515.

[13] Y. W. Kuan, A. Goh, D. Ngo, and A. Teoh, "Cryptographic Keys from Dynamic Hand-Signatures with Biometric Secrecy Preservation and Replaceability," in *Proceedings of the*

Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 2005, pp. 27-32.

[14] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," presented at IEEE International Conference on Multimedia and Expo, 2004.

[15] Y. Dodis, L. Reyzin, and A. Smith., "Fuzzy extractors:How to generate strong keys from biometrics and other noisy data," presented at Int. Conf. Theory and Applications of Crytographic Techniques (EUROCRYPT), 2004.

[16] A. Juels and M. Sudan, "A fuzzy vault scheme," presented at Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on, 2002.

[17] T. Clancy, D. Lin, and N. Kiyavash, "Secure Smartcard-Based Fingerprint Authentication," presented at ACM SIGMM Workshop on Biometric Methods and Applications, Berkley, USA, 2003.

[18] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy Vault for Fingerprints," presented at Fifth International Conference on Audio- and Video-based Biometric Person Authentication, Rye Twon, USA, 2005.

[19] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault," presented at Information Security and Cryptology, Beijing, China, 2005.

[20] S. Lee, D. Moon, S. Jung, and Y. Chung, " Protecting Secret Keys with Fuzzy Fingerprint Vault Based on a 3D Geometric Hash Table," presented at ICANNGA 2007, Warsaw, Poland, 2007.

[21] B. M. Mehtre, N. N. Murthy, S. Kapoor, and B. Chatterjee, "Segmentation of fingerprint images using the directional image," *Pattern Recogn.*, vol. 20, pp. 429- 435, 1987.

[22] J. Yin, E. Zhu, X. Yang, G. Zhang, and C. Hu, "Two steps for fingerprint segmentation," *Image Vision Comput.*, vol. 25, pp. 1391-1403, 2007.

[23] A. M. Bazen and S. H. Gerez, "Segmentation of Fingerprint Images," presented at Workshop on Circuits Systems and Signal Processing, 2001.

[24] K. Nandakumar, A. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance"IEEE Trans. on Information Forensics and Security,vol. 2, no. 4, pp. 744-757,2007

[25] Feng Hao, Ross Anderson, and John Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081- 1088,2006.

[26] Yang, Shenglin, and Ingrid Verbauwhede. "Automatic secure fingerprint verification system based on fuzzy vault scheme."Proceedings (ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol. 5. IEEE, 2005.

[27] Chen, B.; Chandran, V., "Biometric Based Cryptographic Key Generation from Faces," In Proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital image Computing Techniques and Applications, vol., no., pp.394-401, 2007.

[28] S. V. K. Gaddam and M. Lal, "Efficient Cancellable Biometric Key Generation Scheme for Cryptography," international Journal of Network Security," vol.ll, no.2, pp.57 -65, sep.20 I O.

[29] N. Lalithamani and K.P. Soman, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme," European Journal of Scientific Research, vol.3l, no.3, pp.372-387, 2009.

[30] A. Jagadeesan, K. Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Le vel Fusion of Fingerprint and Iris," international Journal of Computer Science and information Security, vol. 7, no. 2, pp.28-37, February 2010.

[31] Rathgeb, Christian, and Andreas Uhl. "Context-based biometric key generation for Iris," iET computer vision. vol. 5, no. 6, pp. 389-397, 2011.

[32] Monrose, F., Reiter, M. K., Li, Q., and Wetzel, S. "Cryptographic key generation from voice. " In Proceedings of IEEE Symposium on Security and Privacy, 2001, pp. 202-213

[33]Feng, H., and Wah, C. C. "Private key generation from on-line handwritten signatures." Information Management & Computer Security, vol. 10, no. 4, pp. 159-164,2002.