FINGERPRINT IMAGE PROCESSING FOR GENERATING SECURITY AND CRYPTOGRAPHY KEYS

Thesis · August 2008

CITATIONS
0

READS
317

1 author:

Mokhled Altarawneh
Mu'tah University
31 PUBLICATIONS **159** CITATIONS

SEE PROFILE

FINGERPRINT IMAGE PROCESSING FOR GENERATING SECURE CRYPTOGRAPHIC KEY

Al Tarawneh Mokhled

BSc, Baku, Azerbaijan, 1990

MEng, University of the Ryukyus. Japan, 2001

School of Electrical, Electronic and Computer Engineering

Faculty of Science, Agriculture and Engineering

Newcastle University

U.K.

Thesis submitted to Newcastle University for the degree of

Doctor of Philosophy

January 2008

Dedication

To my father, and mother souls, May Allah Almighty

accept them with his mercy.

To my beloved wife Amal. None of this would
be possible without your love and support

To my children, Zaid, Saba , Banan and Duaa who are the reason
to try and make the world a safer place.

Abstract

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 crypt technology. The new technology suffers from several limitations and this thesis, addresses the biometric information quality and the security weakness of cryptography. In many applications fingerprint has been chosen as a core of bio crypt combined technology due to it's maturity in terms of availability, uniqueness, permanence, feasibility, ease of use and acceptance. Fingerprint has been studied from the point of view of information strength to suitability to the cryptographic requirement. The factors relating to generating and constructing combined bio crypt key such as biometric image validity, quality assessment and distinct feature extraction are studied to avoid corruptness of the source biometric images. A number of contributions are made in this work, firstly, the analysis of the validity and quality robustness of fingerprint images is undertaken, and a novel algorithm is realised for circumventing these limitations. Secondly, new algorithms for increasing the management security of image based biometric keys is described, via shielding bio crypto information as another line of defence against serious attack. Finally, fingerprint feature vector is proposed to replace minutiae based fuzzy vault to output high entropy keys. This allows the concealment of the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is open to an attacker.

Acknowledgments

﴿ يرفعِ اللَّهُ الذينَ ءامنوا منكم و الذين أوتوا العلم درجات﴾

[*Allah* raises the ranks of those among you who believe and those who were granted the knowledge.] *Qur'an*

I would like to express my profound gratitude to Professor S. S. Dlay for his supervision, his unlimited help, wise guidance, patience, and support during all stages of the dissertation and preparation of this thesis. Thanks for making this research possible and for navigating it along the thin line between practice and theory. I am indebted to him more than he knows. His red pen ink must have gold cost.

I would also like to express my sincere thanks to Dr. W.L. Woo for his supervision, courteous, kindness. His helpful comments, constructive criticism and invaluable suggestions made this work successful.

Thanks are also due to my colleague in Biometrics research group at Newcastle University and my friends for their help, patience and understanding.

Thanks also have to go to my friend Lloyd Palmer for his valuable time in proofreading earlier draft of the thesis.

I would like to take this opportunity to express my inexpressible gratitude to Mutah University for providing the financial support for this work.

Mokhled S. AlTarawneh

List of Publications

[1] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "Crypto key generation using contour graph algorithm" in *Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition ,and applications* Innsbruck, Austria ACTA Press, 2006, pp. 95-98 .

[2] M. S. Altarawneh, W.L.Woo, and S. S. Dlay, "BIOMETRICS AND FUTURE SECURITY," in *Proceedings of MU International Conference on Security, Democracy and Human Rights*, Mutah, Jordan, 10-12 July 2006.

[3] M. S. Altarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "CRYPTO KEY GENERATION USING SLICING WINDOW ALGORITHM," *In Proceedings of 6th International Symp. On Communication Systems, Networks and Digital Signal Processing (CSNDSP' 06)*, Patras, Greece, 19-21, July, 2006, pp. 366-370

[4] M. S. ALTARAWNEH, L.C.KHOR, W.L.WOO, and S.S DLAY, "A NON Reference Fingerprint Image Validity Check," in *Proceedings of The International Conference on Digital Communications and Computer Applications (DCCA 2007)*, Jordan, Irbid, March, 2007, pp. 776-780

[5] M. S. ALTARAWNEH, W.L.WOO, and S.S DLAY, "OBJECTIVE FINGERPRINT IMAGE QUALITY ASSESSMENT USING GABOR SPECTRUM APPROACH," in *Proceedings of the15th International Conference on Digital Signal Processing (DSP 2007),* Wales, UK, July, 2007, pp. 248-251

[6] M.S. ALTARAWNEH, W.L. WOO, and S.S. DLAY, "A Hybrid Method for Fingerprint Image Validity and Quality Computation," accepted in The 7th WSEAS International Conference on SIGNAL PROCESSING, ROBOTICS and AUTOMATION (ISPRA '08), Cambridge, UK, February 20-22, 2008

[7] M.S. ALTARAWNEH, W.L. WOO, and S.S. DLAY, "Biometric Key Capsulation Technique Based on Fingerprint Vault: Analysis and attack," accepted in the 3rd

IEEE INTERNATIONAL CONFERENCE ON INFORMATION & COMMUNICATION TECHNOLOGIES: FROM THEORY TO APPLICATIONS, ICTTA08, Umayyad Palace, Damascus, Syria, April 7 - 11, 2008.

[8] M.S. ALTARAWNEH, W.L. WOO, and S.S. DLAY, "Fuzzy Vault Crypto Biometric Key Based on Fingerprint Vector Features", accepted in the 6th Symposium on Communication Systems, Networks and Digital Signal Processing, Graz University of Technology, Graz.

[9] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "A NON Reference Fingerprint Image Validity via Statistical Weight Calculation," *Digital Information Management*, vol. 5, pp. 220-224, August, 2007.

Abbreviations

AFAS	Automatic Fingerprint Authentication System
AFIS	Automatic Fingerprint Identification System
BE	Biometric Encryption
BKC	Biometric Key Capsulation
BS	Background Subtract
BW	Berlekamp Welch
CA	Certificate Authority
CBCG	Contour Based Construction Graph
CN	Crossing Number
CP	Chaff Point
CRC	Cyclic Redundancy Check
CSF	Contrast Sensitivity Functions
DB	Data Base
DC	Directional Contrast
DFT	Discrete Fourier Transform
DT	Determine Threshold
EER	Equal Error Rate
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

FR	Full Reference
FRR	False Reject Rate
FVC	Fingerprint Verification Competition
FVS	Fuzzy Vault Scheme
GAR	Genuine Accept Rate
GF	Gabor Feature
GF	Galois Field
GS	Gabor Spectrum
GSM	Gabor Spectral Method
HLK	Header Locker Key
HVS	Human Visual System
ICP	Iterative Closest Point
IQA	Image Quality Assessment
IQF	Image Quality of Fingerprint
IQS	Image Quality Survey
IT	Information Technology
ITU	International Telecommunication Union
MINDTCT	Minutiae Detection
MOS	Mean Opinion Score
MLP	Multi Layer Perceptron
MSE	Mean Squared Error
MR	Matrices Regenerator
NFIQ	Fingerprint Image Quality
NIST	National Institute of Standards and Technology
NN	Neural Network
NR	No Reference
OAS	Object Area Segmentation
OCL	Orientation Certainty Level

OF	Orientation Field
PCA	Principle Component Analysis
PET	Privacy Enhancing Technology
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PLCC	Pearson Linear Correlation Coefficient
PPI	Pixel Per Inch
PR	Polynomial Reconstruction
PS	Power Spectrum
PSNR	Peak Signal-to-noise Ratio
PWC	Pixels Weight Calculation
QA	Quality Assessment
QI	Quality Index
ROC	Receiver Operating Characteristic
ROI	Region Of Interest
RP	Reference Point
RR	Reduced Reference
RS	Reed-Solomon
SKC	Secret Key Cryptography
SP	Singular Point
SROCC	Spearman Rank Order Correlation Coefficient
SSIM	Structural Similarity
SWA	Slicing Window Algorithm
SW	Slicing Window
TAR	True Acceptance Rate
TM	Transformed Matrix
TR	True Rate
TRR	Threshold Ratio

w.r.t	With respect to
VCA	Validity Check Algorithm
VHG	Vector Header Generator
VS	Vault Set
WSQ	Wavelet Scalar Quantization

Table of Contents:

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background

Technology brings a new dimension to biometrics in this information society era, while biometrics brings a new dimension to individual identity verification. It provides a guaranteed level of accuracy and consistency over traditional methods. Biometrics means "The statistical analysis of biological observations and phenomena". It refers to the use of distinctive physical (e.g., fingerprints, face, retina, iris, hand geometry, palm) and behavioural (e.g., gait, signature, speech) characteristics for automatically recognizing individuals [1, 2]. Biometric based identification relies on "something that you are", or "something that you do", and hence it differentiate between an authorized person and an impostor [3]. Any physiological or behavioural human characteristic can be used as a biometric as long as it satisfies the following requirements [4]:

- *Universality*, every person should have the characteristic.
- *Uniqueness*, no two persons should be the same in terms of the characteristic.
- *Permanence or Immutability*, the characteristic should be invariant in time.
- *Collectability*, the characteristic can be measured quantitatively. In addition, application related requirements are also of utmost importance in practice:
- *Circumvention*, refers to how easy it is to fool the system by fraudulent techniques;
- *Performance*, refers to the achievable identification accuracies; the resource requirements for acceptable identification accuracy, and the working environmental factors that affects the identification accuracy;
- *Acceptability*, refers to what extent people are willing to accept the biometric system.

Biometric characteristics provide a unique natural signature of a person and it is widely accepted. While some of the requirements described above like universality, and collectability are relatively easy to verify for certain human characteristics, others like immutability, and uniqueness require extensive tests on a large number of samples in order to be verified. Each biometric technique has its advantage and disadvantage. The applicability of a specific biometric technique depends heavily on the application domain. No single biometric can meet the entire requirement (e.g. accuracy, cost, practicality) which means no biometric is "optimal" [5]. Fingerprints have been used as a biometric characteristic because they could offer unique advantages over other biometrics in terms of acquisition ease, relative temporal invariance, and uniqueness among different subjects [6]. A brief comparison of biometric techniques based on seven factors is provided in Table1-1. 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.

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)

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 [2]. 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.

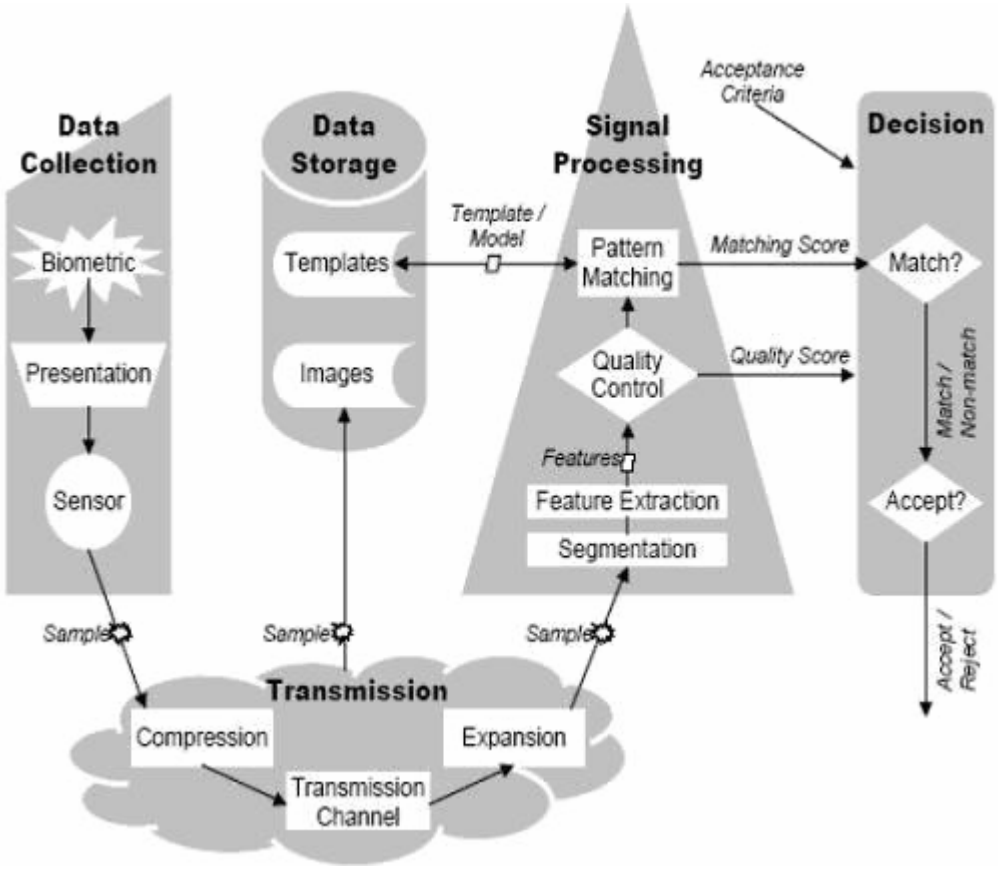


Figure 1-1 Block diagram of a generic biometric system [7]

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 [8]. 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.

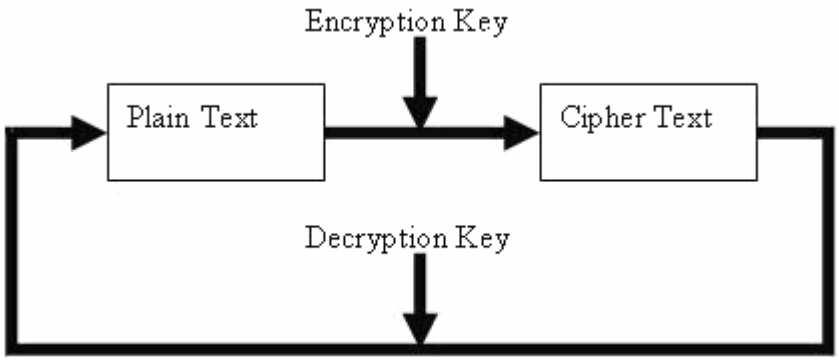
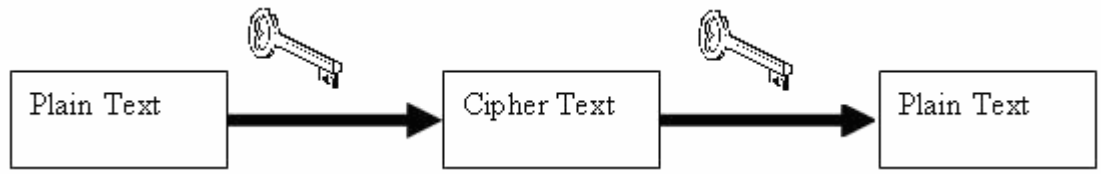


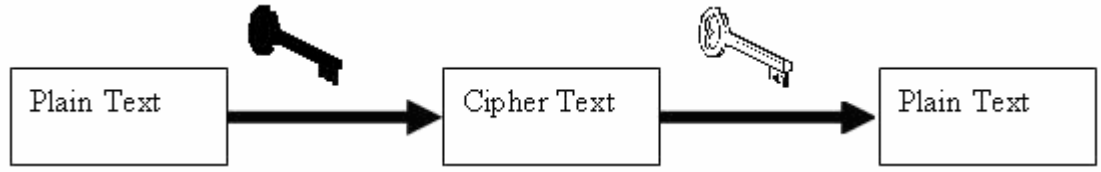
Figure 1-2 Block diagram of a generic cryptography

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 ciphertext, which will in

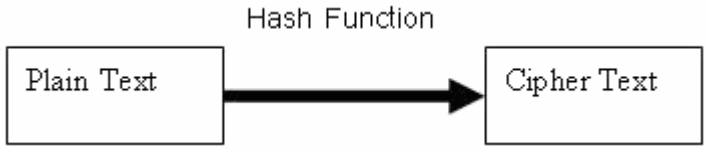
turn (usually) be decrypted into usable plaintext [9]. A single key is used for both encryption and decryption in secret key cryptography; two keys are used in public key cryptography. Hash function uses a fixed-length value computed from the plaintext that makes it impossible for either the contents 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 [10]. 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 [11]. 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 [11]. 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 [12]. Using data derived directly from a biometric fingerprint image is another method. In this manner fingerprint templates are used as a cryptographic key [13, 14]. However, sensitivities due to environmental, physiological factors and compromising of the cryptographic keys stand as a big obstacle [15]. 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 [16]. 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.

1.5 Aims 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:

- To 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.

1.6 Original Contributions

The original contributions resulting from the PhD research can be grouped in the following methods: fingerprint image validity check, quality assessment, crypto key generation and capsulation.

1. Novel algorithm for benchmarking the validity of fingerprint images based on statistical weight checking. It is a blind based or no-reference algorithm, which

means it has access only to the tested image. It is applied to the base image element because it describes an image object with the contrast, brightness, clarity and noising attributes. Developed algorithm is a good predictor of image quality estimation and total image information within visual quality. This is described in chapter 3 and the work has been presented at [17], and published in [18].

2. A new algorithm for fingerprint image quality assessment which enhances the overall performance of fingerprint based systems. The developed algorithm is derived from power spectra of two dimensional Gabor features. It benefits from the use of both Gabor and Fourier power spectrum methods, such as frequency and orientation representations. Developed algorithm can effectively guide the template selection at the enrolment stage and fingerprint image quality classification for automatic parameters selection in fingerprint image pre-processing. This work has been presented at [19], [20].

3. Novel Algorithm for crypto key generation based on a technique known as contour graph and slicing window. This algorithm is developed to overcome the key diversity problem. It avoids instability and inconstancy of biometric features by constructed contour graph and sliced windows and their adjacency matrix representation. This work has been presented at [13] and [14].

4. A new capsulation technique for fingerprint fuzzy vault key management. The developed technique is used to secure both the secret key and the biometric template by binding and shielding them within a cryptographic framework. The technique used capsulation process to solve the problems of key management and to distribute the level of security on the shields structure. Keys entropy depends on level of shielding and polynomial degree of shielded secret key, while encryption key depend on constructed vault entropy, and it is slightly more efficient in terms of encryption/decryption speed because it used a heading capsulation technique on covering the ciphertexts.

1.7 Thesis Outline

Chapter 2 surveys the development stages of bio crypt technique from validity check, quality assessment to quality of service of keys construction. Chapter 3 provides a detailed methodology of how to build aimed validity check approach for fingerprint image benchmarking. This thesis has conducted experiments on a VTC2000DB1_B, TIMA databases [21] & [22]. It also briefly reviews segmentation method as a fundamental infrastructure for validity check approach. The characteristics of this approach have been highlighted. Chapter 4 describes image quality measures, methods, proposed Gabor spectrum approach for fingerprint image quality assessment. The proposed algorithm is tested subjectively, objectively and reliably. Results are fully discussed and a detailed summary is given in this chapter. Chapter 5 describes fingerprint bio keys methods "releasing, generating and binding", in this chapter a minutiae based generating approaches are proposed and investigated to address the problems of direct key generation. Chapter 6 analyses a binding technique on base of fuzzy vault construct. It shows a technique weakness and it discusses how to overcome these problems. A key capsulation technique is also proposed to solve key management problems. Chapter 7 concludes the thesis, by summarizing the results obtained and indicating future development.

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 Validity Check and Quality Assessment

With the advent of various bio crypt standards and a proliferation of image encryption products that are starting to appear in the marketplace, it has become increasingly important to devise biometric image validity and quality assessment algorithms that will standardize the assessment of biometric image validity in the first round and quality in the total rank. The subjective assessment of Mean Opinion Score (MOS) is very tedious,

expensive and cannot be conducted in real time but it could be a basic judgment reference of devised objective measurement algorithms. A recent trend incorporates validity and quality metrics into the biometric system based to make the new systems more accurate, efficient, and more reliable. Lim et al. [23, 24] studied the local structure of the fingerprint image by partitioning the image into blocks of size 32×32 pixels, they computed the following features in each block: orientation certainty level (OCL), ridge frequency, ridge thickness and ridge-to-valley thickness ratio. Blocks are then labelled as "good", "undetermined", "bad" or "blank" by thresholding the four local features. A local quality score S_L is computed based on the total number of "good", "undetermined" and "bad" quality image blocks. They used the ratio of the eigen-values of the gradient vectors to estimate the local ridge orientation certainty. As fingerprint image sub-blocks generally consists of dark ridge lines separated by white valley lines along a same orientation, the consistent ridge orientation is therefore the one of the distinguishable local characteristics of the fingerprint image. The covariance matrix C of the gradient vector for an N points image block is given by:

$$C = E\left\{\begin{bmatrix} dx \\ dy \end{bmatrix}\begin{bmatrix} dx & dy \end{bmatrix}\right\} = \begin{bmatrix} a & c \\ c & b \end{bmatrix}. \qquad 2 - 1$$

where $E\{\bullet\} \equiv \frac{1}{N}\sum_{N} \bullet$

For the covariance matrix in (2-1), eigenvalues λ are found to be:

$$\lambda_{\max} = \frac{(a+b) + \sqrt{(a-b)^2 + 4c^2}}{2} \qquad 2 - 2$$

$$\lambda_{\min} = \frac{(a+b) - \sqrt{(a-b)^2 + 4c^2}}{2} \qquad 2 - 3$$

For a fingerprint image block; the ratio between $\lambda_{\min}$ and $\lambda_{\max}$ gives an orientation certainty level, Equation (2-4). OCL gives an indication of how strong the energy is concentrated along the ridge-valley orientation on certainty level. The lower the value the

stronger it is. It is obvious that OCL is between 0 and 1 as a, b>0. It is used to estimate the orientation field and localize the region of interest (ROI) within the input fingerprint image.

$$ocl = \frac{\lambda_{\min}}{\lambda_{\max}} = \frac{(a+b) - \sqrt{(a-b)^2 + 4c^2}}{(a+b) + \sqrt{(a-b)^2 + 4c^2}} \qquad 2\text{-}4$$

The certainty level of the orientation field in a block quantifies the extent to which the pixel gradient orientations agree with the block gradient orientation. For each block, if its certainty level of the orientation field is below a threshold, then all the pixels in this block are marked as background pixels. As the computation of certainty level is a by-product of the local ridge orientation estimation, it is a computationally efficient segmentation approach. Performing the principal component analysis (PCA) approach can effectively indicate the directional strength possessed by an image sub-block. However, it does not guarantee any periodic layout of ridges and valleys. OCL is a good indicator of quality of a fingerprint sample, it is still not sufficient. Therefore, there is a need to further examine the ridge-valley structure of the fingerprint sample. Ridge valley structure analysis performed on image blocks. Inside each block, an orientation line, which is perpendicular to the ridge direction, is computed. At the centre of the block along the ridge direction, a 2-D vector V_1 (slanted square in fingerprint orientation pattern) Figure (2-1), with size 32×13 pixels is extracted and transformed to a vertical aligned 2-D vector V_2. By using equation (2-5), a 1-D vector V_3, that is the average profile of V_2, can be calculated.

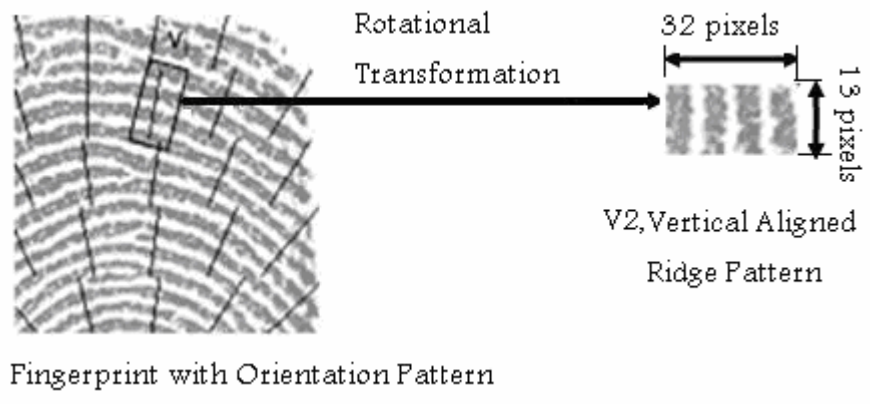


Figure 2-1 Extraction of a local region and transformation to vertical aligned pattern

$$V_3(i) = \frac{\sum_{j=1}^{m} V_2(i,j)}{m},\ i = 1,..32 \qquad 2 - 5$$

where m is the block height (13 pixels) and i is the horizontal index.

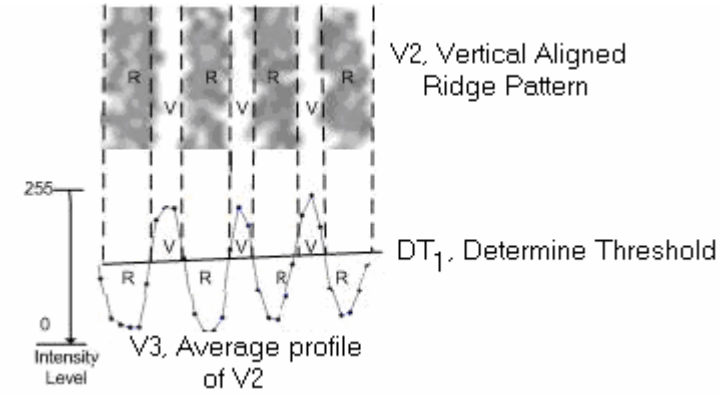


Figure 2-2 V2 region segmentation

Once V_3 has been calculated, linear regression is then applied on V_3 to find the Determine Threshold (DT_1) which is a local threshold for the block. DT_1 is the line positioned at the centre of the Vector V_3, and is used to segment the image block into the ridge or valley region. Regions with grey level intensity lower than DT_1 are classified as ridges; else they are classified as valleys. The process of segmenting the fingerprint region into ridge and valley using DT_1 is shown in Figure (2-2). From the one-dimensional signal in Figure (2-2), several useful parameters are computed, such as

valley thickness and ridge thickness. Since good finger images cannot have ridges that are too close or too far apart, thus the nominal ridge and valley thickness can be used as a measure of the quality of the finger image captured. Similarly, ridges that are unreasonably thick or thin indicate that the finger image may not be captured properly or is a residual sample.

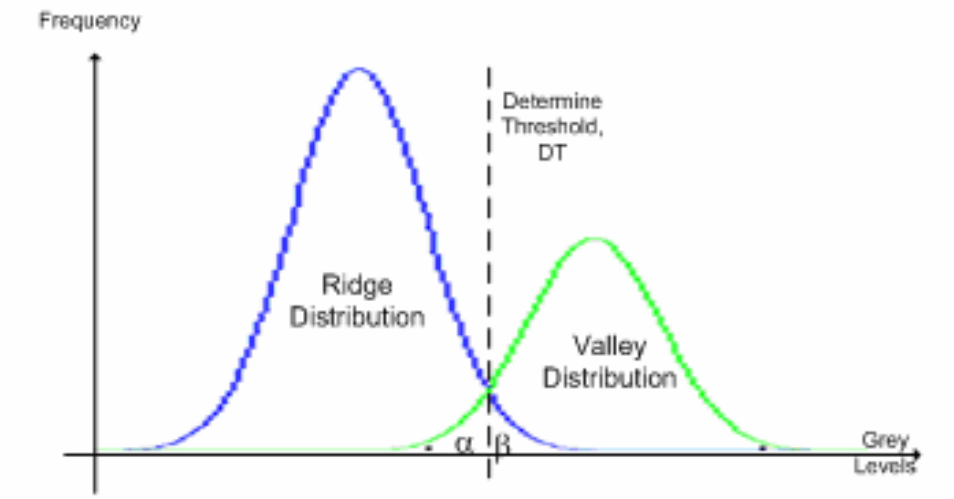


Figure 2-3 Ridge and Valley distribution

Thus, the finger image quality can be determined by comparing the ridge and valley thickness to each of their nominal range of values. Any value out of the nominal range may imply a bad quality ridge pattern. Figure (2-3) shows the grey level distribution of the segmented ridge and valley. The overlapping area is the region of potential misclassification since in this region, whether a pixel belongs to ridge or valley cannot be accurately determined using DT_1. Hence, the area of the overlapping region can be an indicator of the clarity of ridge and valley, subject to the ridge and valley thicknesses being within the acceptable range. Shen et al. [25] divided the fingerprint image into $N(blocks)$ and applied Gabor filtering to image sub-blocks. Gabor features of each block are computed first, and then the standard deviation of the Gabor features is used to determine the quality of this block. They conclude that a good quality block with clear repetition of ridge and valley pattern can be identified by the output of a Gabor filter bank. The mathematical conclusion of the previous method is as follows:

The general form of a 2D Gabor filter is defined by

$$h(x, y, \theta_k, f, \sigma_x, \sigma_y) = \exp\left[-\frac{1}{2}\left(\frac{x_{\theta_k}{}^2}{\sigma_x{}^2} + \frac{y_{\theta_k}{}^2}{\sigma_y{}^2}\right)\right] \times \exp\left(i 2\pi f x_{\theta_k}\right), \quad 2 - 6$$

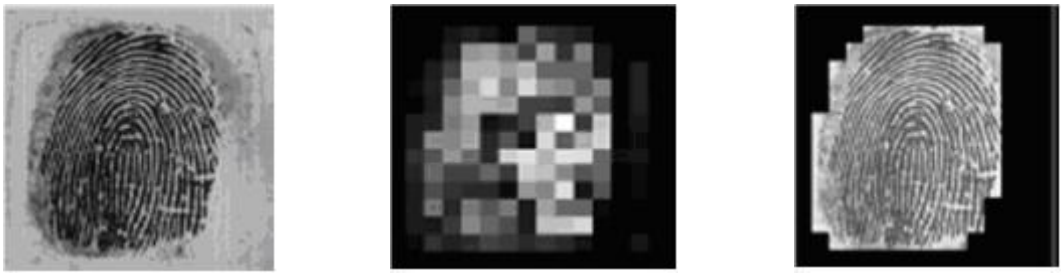
$k = 1, ..., m$

Where $x_{\theta_k} = x\cos\theta_k + \quad y\sin\theta_k$ and $y_{\theta_k} = -x\sin\theta_k + \quad y\cos\theta_k$, f is the frequency of the sinusoidal plane wave, m denotes the number of orientations, θ_k is the k^{th} orientation of the Gabor filter, σ_x and σ_y are the standard deviations of the Gaussian envelope along the x and y axes, respectively. After obtaining m Gabor features, g_{θ_k}, of the block, the standard deviation value G is computed as follows:

$$G = \left(\frac{1}{m-1}\sum_{k=1}^{m}\left(g_{\theta_k} - \bar{g}_\theta\right)^2\right)^2, \ \bar{g}_\theta = \frac{1}{m}\sum_{k=1}^{m} g_{\theta_k} \quad 2 - 7$$

where $\theta_k = \pi(k-1)/m, \quad k = 1, \quad ...., \quad m$

They compute the value of G for each block. If G is less than a block threshold value (T_b), the block is marked as a background block, otherwise the block is marked as a foreground block. The quality field for the fingerprint image in Figure (2-4 (a)) is shown in Figure (2-4(b)). The segmented image is shown in Figure (2-4(c)).



(a) (b) (c)

Figure 2-4 Foreground/background segmentation: (a) origin image; (b) quality field (Standard deviation of m Gabor features); (c) segmented image

The quality field value for a foreground block is defined to have one of the following values: “good” and “poor”. A block is marked as a “poor” quality block if its G value is

less than a preset quality threshold (T_q), otherwise it is marked as a "good" quality block. QI (Quality Index) is defined to quantify the quality of a fingerprint image, where

$$QI = 1 - \frac{Numberof"poor"ForegroundBlocks}{NumberofForegroundBlocks} \qquad 2 - 8$$

A fingerprint image is marked as a "good" quality image if the QI value is bigger than a threshold T_Q, otherwise it's marked as a "poor" quality image. The choice of T_q, and T_Q were determined experimentally. Shen et al. [25], Qi et al. [26] categorized the poor quality fingerprint images into smudge and dry images according to smudginess and dryness indices, (SI, DI), where SI, DI are used to determine whether this image consists of a large number of dry or smudged blocks. The idea is that for a smudged block, most ridges are connected with each other, so that the mean value of the block is small. While for a dry block, some of ridges are disjointed and the mean value of the block will be larger. A poor block is marked as a smudged block if it's mean value is less than a preset smudged threshold T_S, while a poor block is marked as a dry block if its mean value is larger than the preset dry threshold T_d. Both T_S and T_d are determined by the mean value of the foreground blocks of the image.

$$SI = \frac{Numberof"poor"\&"smudged"ForegroundBlocks}{NumberofForegroundBlocks} \qquad 2 - 9$$

$$DI = \frac{Numberof"poor"\&"dry"ForegroundBlocks}{NumberofForegroundBlocks} \qquad 2 - 10$$

Two thresholds T_S and T_D were chosen empirically to determine the type of a poor quality fingerprint image. If $SI \geq T_S$ and $DI \geq T_D$, the image is marked as others. If $SI \geq T_S$ and $DI < T_D$, the image is marked as smudged. If $SI < T_S$ and $DI \geq T_D$, the image is marked as dry. Shen et al in their proposed method used fingerprint local orientation information for image segmentation and quality specification. Qi et al. [26] combined

quality calculation of both local and global features of a fingerprint image. Their hybrid method combined the quality indices of local information (e.g. Gabor feature, smudginess and dryness) and global information (e.g. foreground area, central position of foreground index; minutiae count index and singular point index). The seven quality indices are mathematically calculated as follows:

1. The Gabor feature quality index Q_1 is calculated by averaging the standard deviation of all image sub-blocks Equation (2-7). If the average is greater than or equal to the threshold value T_{ave}, the quality will be 1.

$$Q_1 = \frac{\min\left(\sum_{i=1}^{N_{FA}} G(i) \Big/ N_{FA}, T_{ave}\right)}{T_{ave}} \qquad 2\text{-}11$$

where N_{FA} is the number of foreground blocks

2. The smudginess and dryness indices are calculated by Equations (2-9), (2-10) respectively where the quality of smudginess Q_2 and quality of dryness Q_3 are computed by:

$$\mathrm{Q}_2 = 1 - \mathrm{SI} \qquad 2\text{-}12$$

where $SI = \frac{N_{FS}}{N_{FA}}$, N_{FS} is the number of smudgy foreground sub blocks whose mean value is less than a smudginess threshold value T_s .

$$Q_3 = 1 - DI \qquad 2\text{-}13$$

where $DI = \frac{N_{FD}}{N_{FA}}$, N_{FD} is the number of dry foreground sub blocks whose mean value is larger than a dryness threshold value T_d .

3. Foreground area quality index is computed by:

$$Q_4 = \frac{N_{FA}}{N} \tag{2-14}$$

where N_{FA} is the number of foreground blocks which counted according to the rules given in [25] and N is total blocks.

4. Central position of foreground index is calculated with reference to centroid coordinates (x_c, y_c) of sub-blocks in foreground area.

$$Q_5^x = 1 - \frac{\left| x_c - width/2 \right|}{width/2} \tag{2-15}$$

$$Q_5^y = 1 - \frac{\left| y_c - height/2 \right|}{height/2} \tag{2-16}$$

5. Minutiae count index which depends on the quantified relation between really extracted minutiae n_{mc} count and expected minutiae count E_{mc} where

$$Q_6 = \frac{\min(n_{mc}, E_{mc})}{E_{mc}} \tag{2-17}$$

6. Singular point (SP) index quality calculated according to the following rules

$$Q_7 = \begin{cases} 1 & core \quad exsit \\ 0 & core \quad not \ exsit \end{cases} \tag{2-18}$$

7. Finally, the overall image quality is the combining value of seven quality indices Equation (2-19).

$$Q\sum_{i=1}^{7}\varpi_i Q_i \qquad \text{2-19}$$

where ϖ_i is the weight of each quality index Q_i.

Nill et al. [27] proposed an objective image quality assessment based on the digital image power of normally acquires scenes. Their system is designed to compute image quality based on the two dimensional, spatial frequency power spectrum of the digital image. The power spectrum, which is the square of the magnitude of the Fourier transform of the image, contains information on the sharpness, contrast, and detail rendition of the image and these are the components of visual image quality, i.e. image global information. Their approach was implemented on fingerprint images as Image Quality of Fingerprint (IQF) [28]. In IQF, the power spectrum is normalized by image contrast, average gray level (brightness), and image size; a visual response function filter is applied, and the pixels per inch (PPI) resolution scale of the fingerprint image is taken into account. The fundamental output of IQF is a single-number image quality value which is the sum of the filtered, scaled, weighted power spectrum values. The power spectrum normalizations allow valid inter-comparisons between disparate fingerprint images. IQF processing steps start with acquisitioned live scan or inked image, i.e. raw format image then locating the approximate vertical and horizontal edges of the fingerprint image to identify the ROI of fingerprint image, define a set of overlapping windows that covering entire fingerprint area into sub images, weed out a low structure windows and finally a computing process of image quality, i.e. window power spectrum computation, normalization, incorporation with human visual system (HVS) by applying a HVS filter, and image quality weighting and scaling by pixel per inch. A major benefit of an image quality measure based on image power spectrum is that it is applied to the naturally imaged scene. It does not require use of designed quality assessment targets or re-imaging the same scene for comparison purposes; it requires only a selection of an image area containing some structure, i.e. it is blind image quality assessment method. Chen et al [29] analyzed fingerprint Global structure by computing its 2D Discrete Fourier Transform (DFT). For

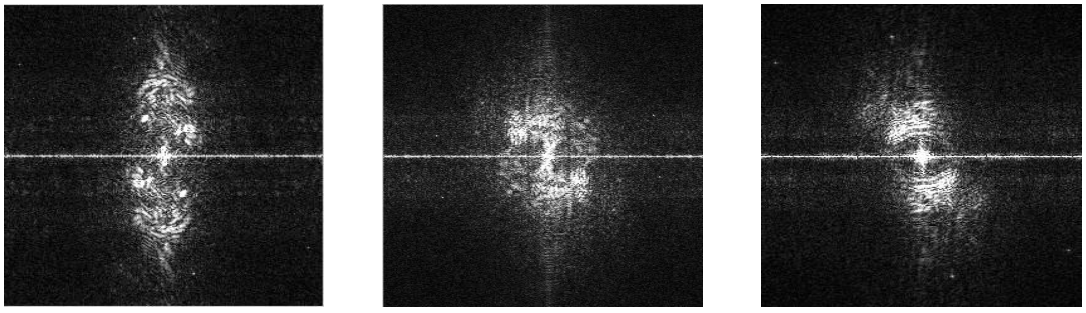
a fingerprint image, the ridge frequency value lies within a certain range. ROI of the spectrum is defined as an annular region with radius ranging between the minimum and maximum typical ridge frequency values Figures(2-5, 2-6), images from [22]. As fingerprint image quality increases, the energy will be more concentrated in ring patterns within the ROI. The global quality was measured by the energy concentration in ring-shaped regions of the ROI therefore a set of constructed bandpass filters to compute the amount of energy in ring-shaped bands. Good quality images will have the energy concentrated in few bands. Chen et al. [29] used the power spectrum method which represent the magnitude of various frequency components of a 2D fingerprint image that has been transformed with the Fast Fourier Transform from the spatial domain into the frequency domain. Different frequencies in the power spectrum are located at different distances and directions from the origin, i.e. the centre of power spectrum. Higher frequency components of the image will be located at greater distances from the origin. Different directions from the origin will represent different orientations of features in the image. The power at each location in the power spectrum is an indication of the frequency and orientation of a particular feature in the image. The power spectrum $S_f(u,v)$ of a $M \times M$ point digital image $f[x,y]$ can be computed as the magnitude squared of the discrete Fourier transform:

$$S_f(u,v) = \left| \sum_{x=0}^{M-1} \sum_{y=0}^{M-1} f[x,y] e^{-2\pi (ux+vy)/M} \right|^2 \qquad 2\text{-}20$$

where $u,v = -\frac{M}{2} \ldots \frac{M}{2}$

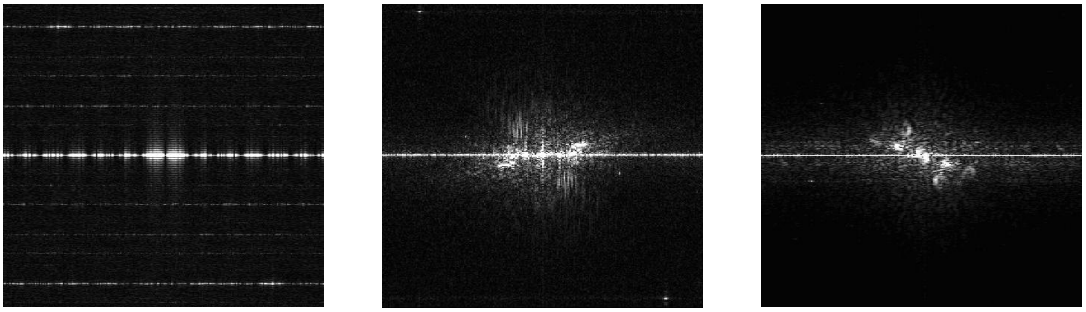
Evaluating the power spectrum is an excellent way to isolate periodic structural features or noise in the image [27]. Since the power can vary by orders of magnitude in an image, the power spectrum is usually represented on a log scale Figures (2-5, 2-6). The power spectrum approach does not depend on imaging designed targets, does not require detection and isolation of naturally occurring targets, and does not require re-imaging the same scene for comparison purposes. This approach is useful for distinguishing the total

direction and the consistency of the fingerprint ridges and valleys because it is based on the use of the frequency characteristics [30]. A ring in Fourier spectrum is the indicating factor of the quality of image itself, incase of good quality images it is clearly appearing around the origin. In contrast, bad quality images do not produce a ring in Fourier spectrum. This is due to the fact that bad quality images generally have less uniform and less periodic ridge-valley structure than good fingerprint images.



PS (Nik_index1.tif) PS (1_ben_index2.tif) PS (7_nik_aurircu1.tif)

Figure 2-5 Power spectrum of good fingerprint images



PS (No_contact_pb4.tif) PS (cut6.tif) PS (strange9.tif)

Figure 2-6 Power spectrum of bad fingerprint images

Lee et al. [30] and Joun et al. [31] used local contrast measurement in terms of contrast of the gray values between the ridges and valleys along the orientation of the ridge flow. The idea behind their approach is that, high directional contrast shows good quality orientation while low contrast shows bad quality. Mathematically, this approach is represented as the following equations:

$$S_i(x,y) = \sum_{j=1}^{8} G(P_{ij}) \qquad 2\text{-}21$$

where $i = 1,...8$

$G(P_{ij})$ denotes the gray value of the pixel corresponding to a position P_{ij} in an 8 directional window that is used to compute the directional contrast. For each 8×8 block, the local gray value θ_i is calculated using equation (2-22), and the biggest value $\theta_{\max}, \theta_{\max} = \max(\theta_i)$, will be used in quality measurement calculations.

$$\theta_i = \sum_{x=1}^{8}\sum_{y=1}^{8} S_i(x,y) \qquad 2\text{-}22$$

The directional contrast D_k will be obtained from the difference between $\theta_{\max}$ and θ_i at the K^{th} block, equation 2-23.

$$D_k = \left|\theta_{\max} - \theta'\right|_k \text{ for } k = 1,...N \qquad 2\text{-}23$$

where N is the number of blocks, θ_i is the direction perpendicular to $\theta_{\max}$. Finally quality measure Q_{DC} of the whole fingerprint image is calculated by normalizing the sum of D_k, equation 2-24.

$$D_k = \frac{1}{c}\sum_{x=1}^{N} D_k \qquad 2\text{-}24$$

where c is certain normalization factor so that the final result is in [0, 1].

Ratha et al. [32] present a method of quality estimation from wavelet compressed fingerprint images. However, it's not a desirable approach for uncompressed fingerprint image databases since the wavelet transform consumes much computation. They observe that a significant fraction of the normalized cumulative spectral energy is within the first few sub bands of a wavelet scale quantization (WSQ) compressed good quality fingerprint image. Accordingly, they design rotation invariant criteria to distinguish smudged and blurred fingerprint images. Ratha et al. [33] described a pixel intensity

method of fingerprint image quality computation. Pixel intensity method classifies image blocks into directional and non-directional as follows. The sum of intensity differences $D_d(i,j)$ between a pixel (i,j) and l pixels selected along a line segment of orientation d centred around (i,j) is computed for n different orientations.

$$D_d(i,j) = \sum_{(i',j')} \left| f(i,j) - f_d\left(i',j'\right) \right| \qquad 2\text{-}25$$

where $d = 0, \pi/n, ..., \pi$ and where $f(i,j)$ is the intensity of pixel (i,j) and $f_d\left(i',j'\right)$ are the intensities of the neighbours of pixel (i,j) along direction d. For each different orientation d, the histogram of $D_d(i,j)$ values is obtained for all pixels within a given foreground block. If only one of the n histograms has a maximum value greater than a prominent threshold, the block is marked as "directional". Otherwise, the block is marked as "non-directional" [34]. The overall quality of the fingerprint image is computed from directional blocks by assigning a relative weight w_i for foreground block i at location x_i, given by:

$$w_i = e - \frac{\|x_i - x_c\|^2}{2q^2} \qquad 2\text{-}26$$

where x_c is the centroid of foreground, and q is a normalization constant.

An overall quality score Q of a fingerprint image is obtained by computing the ratio of total weights of directional blocks to the total weights for each of the blocks in foreground Equation (2-27)

$$Q = \sum_D w_i \Big/ \sum_F w_i \qquad 2\text{-}27$$

where D is the set of directional blocks and F is the set of foreground blocks.

The quality Q is used as a measure of how much reliable directional information is available in a fingerprint image. If the computed Q is less than the quality threshold, the

image is considered to be of poor quality. Tabassi et al. [35, 36] used a classifier method to define the quality measures as a degree of separation between the match and non-match distribution of a given fingerprint. This can be seen as a prediction of the matcher performance. Their method was implemented on neural network based and released by The National Institute of Standards and Technology as Fingerprint Image Quality package (NFIQ) [37], where a novel strategy for estimating fingerprint image quality presented. Image quality map is generated by minutiae detection (MINDTCT) for quality measurement of localized regions in the image by determining the directional flow of ridges and detecting regions of low contrast, low ridge flow, and high curvature. Image quality map formulated based on feature extraction which compute fingerprint image fidelity characteristics and results in an 11-diemensional feature vector, as shown in Table 2-1.

	Name	**Description**
1	foreground	number of blocks that are quality 1 or better; i.e. $foreground = \sum_{i=1} U_i$ where U_i is number of blocks with quality i
2	total of minutia	number of total minutiae found in the fingerprint
3	min05	number of minutiae that have quality 0.5 or better
4	min06	number of minutiae that have quality 0.6 or better
5	min075	number of minutiae that have quality 0.75 or better
6	min08	number of minutiae that have quality 0.8 or better
7	min09	number of minutiae that have quality 0.9 or better
8	quality zone 1	% of the foreground blocks of quality map with quality =1
9	quality zone 2	% of the foreground blocks of quality map with quality =2
10	quality zone 3	% of the foreground blocks of quality map with quality =3
11	quality zone 4	% of the foreground blocks of quality map with quality =4

Table 2-1 Feature vector description

Neural network block that classifies feature vectors into five classes of quality based on various quantities of normalized match score distribution Figure (2-7). The final general

map contains an integer value between 1(highest) and 5 (poorest). The quality measure can be seen as a prediction of matcher performance. This approach uses both local and global features to estimate the quality of a fingerprint images. Zhu et al. [38] proposed a neural network based fingerprint image quality estimation, which estimates the correctness of ridge orientation of each local image block using neural network and then computes the global image quality based on the local orientation correctness.

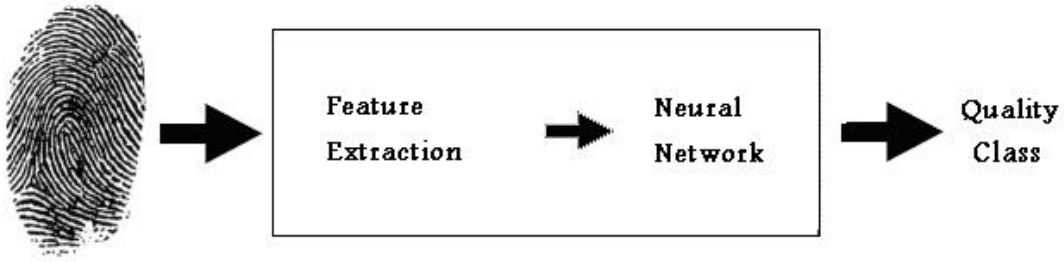


Figure 2-7 NIST Fingerprint Image Quality Block Diagram [36]

2.3 Cryptography and Bio Keys

Cryptography is an important feature of computer and network security [11]. 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 [39] proposed that data derived from the template be used directly as a cryptographic key, Bodo's work was supported by [40, 41]. 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. [42] 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. [12] 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. [15] 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 [12, 15] 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 $f_1(x)$ obtained during verification and $f_0(x)$ obtained during an enrolment is formally defined as

$$c(x) = \int_{-\infty}^{\infty} f_1(v) f_0^*(x+v) dv \qquad 2\text{-}28$$

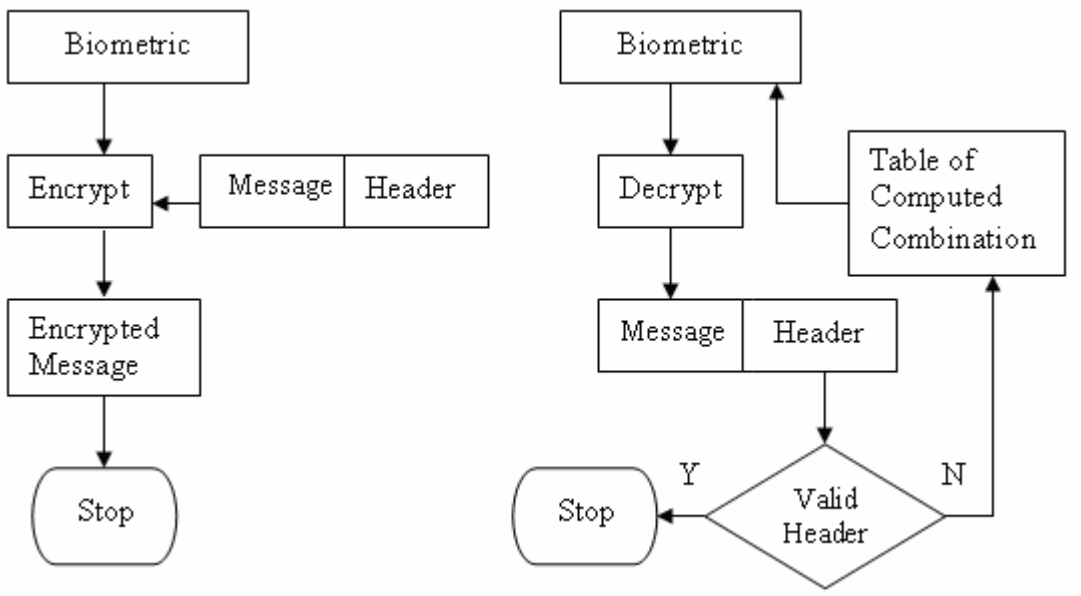
where * denotes the complex conjugate.

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

$$c(x) = FT^{-1}\{F_1(u) F_0^*(u)\} \qquad 2\text{-}29$$

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 [43]. 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 [44],[45] 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 [46] 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 [12]. 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 [47] 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 (2-8), the encryption process begins with the acquisition of the required biometric samples.



Encryption Process Decryption Process

Figure 2-8 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 [47], 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 the non-repudiation problems. However, to be robust this scheme needs several biometrics. Davida et al. [44], [48] proposed an algorithm based on the iris biometric. They considered binary representation of iris texture, called Iris Code [49], 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 [44], [48] 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 [50] 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. [51] 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 [8]; 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 [52], 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 [53]. Keystroke rhythms are a method that tries to understand individual's behaviour. In [53], 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 [53] 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 [52, 54]. In [55], 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. [56, 57] 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 [52]. Chang et al. [58] 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 [52] and [58] did not address the issue of setting the thresholds for distinguishable features, this issue was tackled by Zhang et al.'s work in [59], 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. [60] 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). For three distance metrics (Hamming distance, set difference and edit distance), Dodis et al. calculated the information revealed by (P), and elaborated on the existence of possible algorithms for FE construction. They also proposed a modification of the Juels and Sudan's fuzzy vault scheme [45]: instead of adding chaff points to the projections of the polynomial (p), Dodis et al. [60] proposed to use a polynomial $(p)'$ (of degree higher than (p)) which overlaps with (p) only for the points from the genuine set (A). This new polynomial $(p)'$ replaces the final point set (R) of Juels and Sudan's scheme [45]. Juels and Sudan's fuzzy vault scheme [45] is an improvement upon the previous work by Juels and Wattenberg [61]. In [45], Alice can place a secret (k) (e.g., secret encryption key) in a vault and lock (secure) it using an unordered set (A). Here, unordered set means that the

relative positions of set elements do not change the characteristics of the set: e.g., the set $\{-2,-1,3\}$ conveys the same information as $\{3,-1,-2\}$. Bob, using an unordered set (B), can unlock the vault (access (k)) only if (B) overlaps with (A) to a great extent. The procedure for constructing the fuzzy vault is as follows: First, Alice selects a polynomial (p) of variable (x) that encodes (k) (e.g., by fixing the coefficients of p according to (k)). She computes the polynomial projections, $p(A)$ for the elements of (A). She adds some randomly generated chaff points that do not lie on (p), to arrive at the final point set (R). When Bob tries to learn (k) (i.e., find (p)), he uses his own unordered set (B). If (B) and (A) substantially overlaps, he will be able to locate many points in (R) that lie on (p). Using error-correction coding (e.g., Reed- Solomon [62]), it is assumed that he can reconstruct (p) (and hence (k)). As example, assume Alice selects the polynomial $p(x) = x^2 - 2x + 2$, where the coefficients $(1,-2,2)$ encode her secret (k). If her unordered set is $A = \{-1,-2,-3,3,2,1\}$, she will obtain the polynomial projections as $\{(A, p(A))\} = \{(-1,5),(-2,10),(-3,17),(3,5),(2,2),(1,1)\}$ to this set; she adds two chaff points $C = \{(0,2),(1,0)\}$ that do not lie on (p) , to find the final point set $R = \{(-1,5),(-2,10),(-3,17),(3,5),(2,2),(1,1),(0,2),(1,0)\}$. Now, if Bob can separate at least 3 points from (R) that lie on (p), he can reconstruct (p), hence decode the secret represented as the polynomial coefficients $(1,-2,2)$. Otherwise, he will end up with incorrect (p), and he will not be able to access the secret (k). The security of this scheme is based on the infeasibility of the polynomial reconstruction problem. The scheme can tolerate some differences between the entities (unordered sets (A) and (B)) that lock and unlock the vault. 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 threshold) is not present. Based on the fuzzy vault scheme, Clancy et al. [63] proposed 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. [63] 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 $2^{-69} \approx 1.7 * 10^{-21}$ 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 [64] 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. [65] 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).

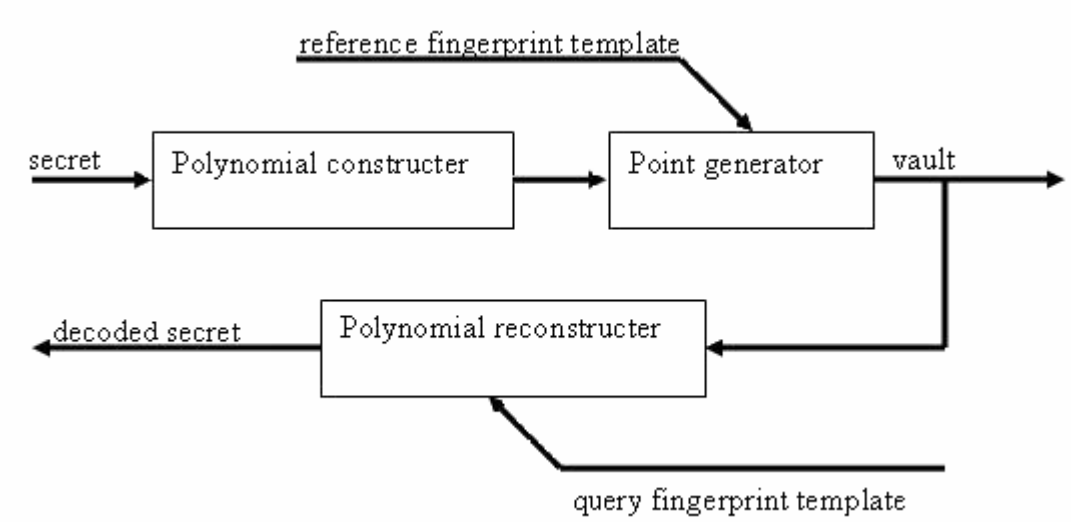
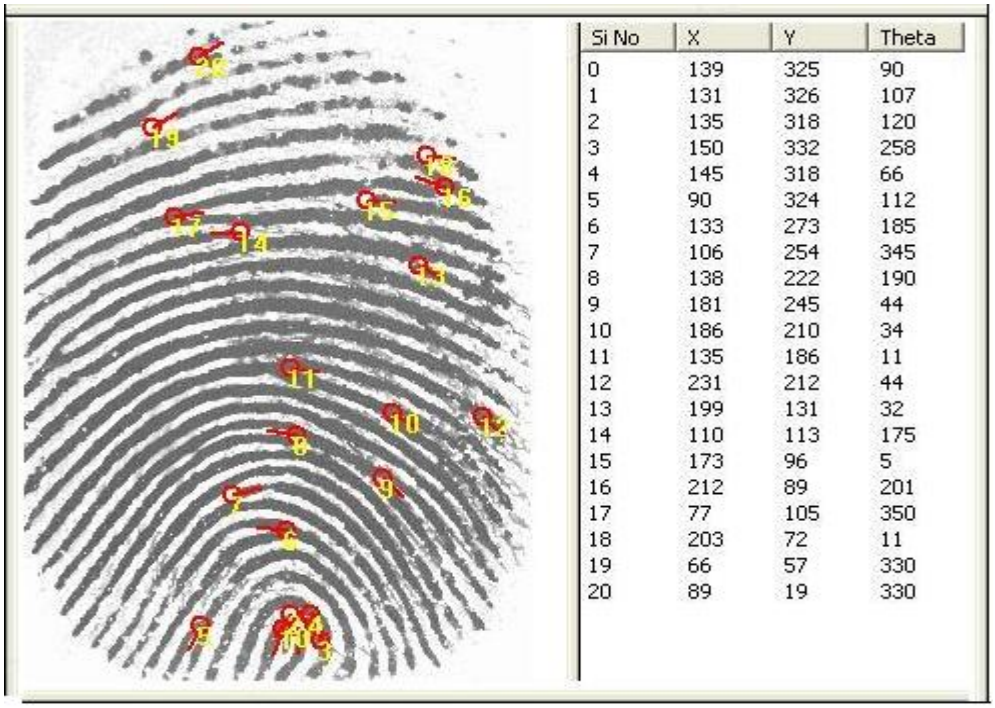


Figure 2-9 Fuzzy vault system block diagram.

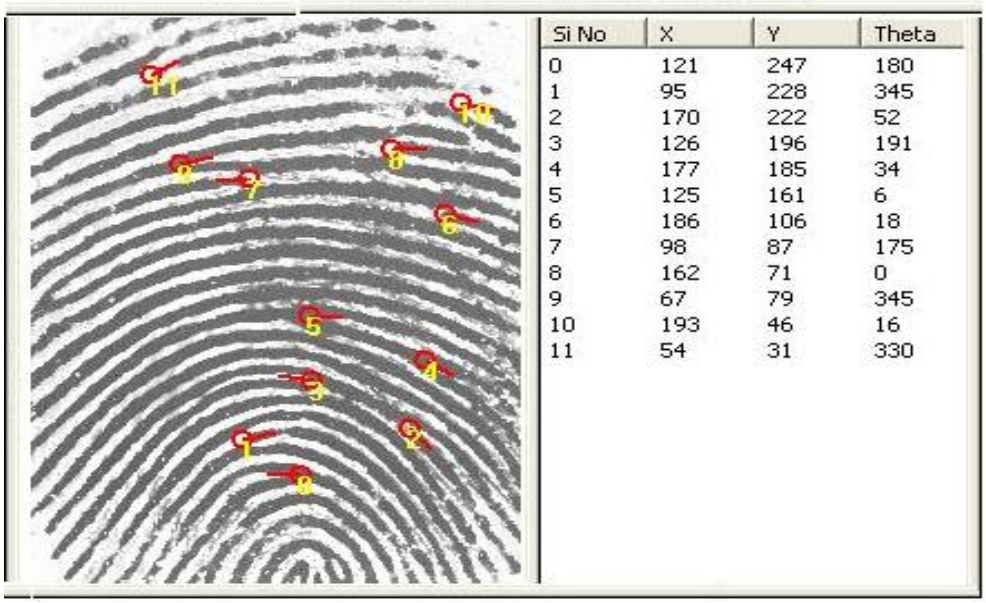
They extend [64] into [65] where chaff points generated according to minutiae points and protected secret, which is clear in secret check block (cyclic redundancy check encoding), and chaff generation block. [65] differ from [45] work's in decoding implementation does not include any correction scheme, 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. in [65], 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, which is the minimal polynomial of a primitive element of the extension field (Galois field) $GF\left(p^m\right)$, $g_{CRC}(a) = a^{16} + a^{15} + a^{12} + 1$ 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 $GF(2^{16})$, 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

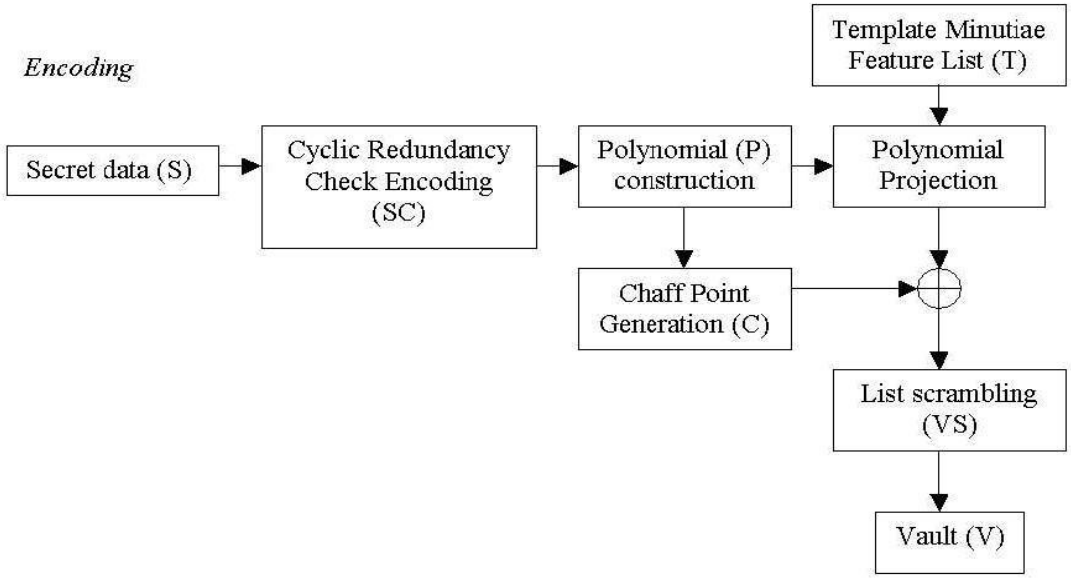
a) Fingerprint minutiae features for image from FVC 2004



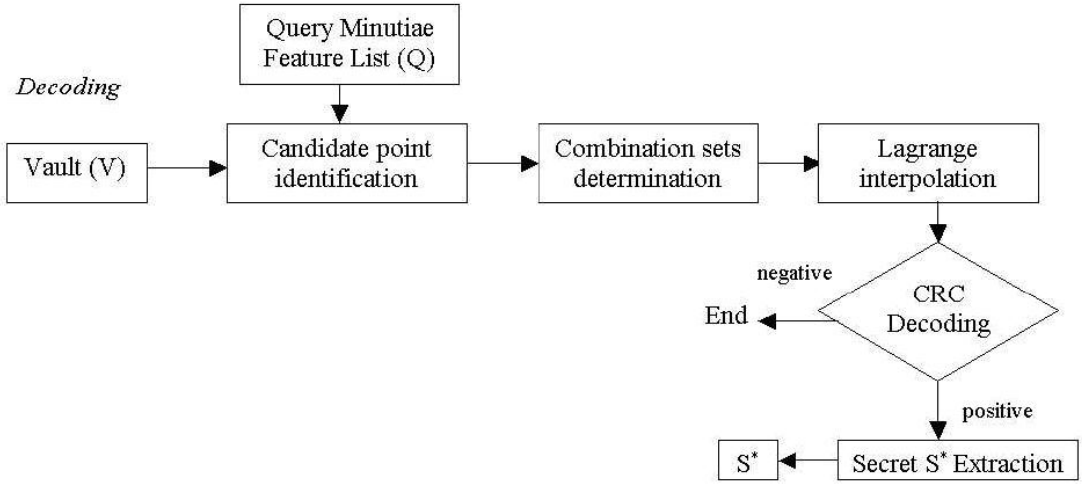
Si No	X	Y	Theta
0	121	247	180
1	95	228	345
2	170	222	52
3	126	196	191
4	177	185	34
5	125	161	6
6	186	106	18
7	98	87	175
8	162	71	0
9	67	79	345
10	193	46	16
11	54	31	330

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.



(a)



(b)

Figure 2-11 Fuzzy fingerprint vault : (a) vault encoding, (b) vault decoding [65]

Hence,

$$p(u) = c_8 u^8 + c_7 u^7 + \ldots + c_1 u^1 + c_0 \qquad 2\text{-}30$$

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, $u_1, u_2, ..., u_N$, G founded to be:

$$G = \{(u_1, p(u_1)), (u_2, p(u_2)), ...(u_N, p(u_N))\} \quad 2\text{-}31$$

While the chaff set C generated randomly by $c_1, c_2, ..., c_M$ as M points in the field $GF(2^{16})$, with the constraint that they do not overlap with the $u_1, u_2, ..., u_N$, namely $c_j \neq u_i, j = 1,2,...M, i = 1,2,..., N$. Then another set of M random points $d_1, d_2, ..., d_M$, 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,

$$VS = \{(v_1, w_1), (v_2, w_2), ..., (v_{N+M}, w_{N+M})\} \quad 2\text{-}32$$

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 $Q = \{u_1^*, u_2^*, ..., u_N^*\}$. 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 $K \leq N$. 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 $\binom{K}{D+1}$ combinations. Lagrange interpolating polynomial was constructed for each combination, and it was given for

$$L=\{(v_1,w_1),(v_2,w_2),\ldots\{v_{D+1},w_{D+1}\}\} \quad \text{2-33}$$

where the corresponding polynomial is

$$p^*(u)=\frac{(u-v_2)(u-v_3)\ldots(u-v_{D+1})}{(v_1-v_2)(v_1-v_3)\ldots(v_1-v_{D+1})}w_1\ldots \quad \text{2-34}$$
$$+\frac{(u-v_1)(u-v_2)\ldots(u-v_{D+1})}{(v_{D+1}-v_1)(v_{D+1}-v_2)\ldots(v_{D+1}-v_D)}w_{D+1}$$

This calculation is carried out in the Galois field, $GF(2^{16})$ 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 in [65] 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 [66], 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 of [66], 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. [67] 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 in [63, 64, 67] assumed the number of chaff points was 200. Lee et al [68] 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.

2.4 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 [2]. 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 [69], 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 [70], this method is extended by excluding blocks with a gray-scale variance that is lower than some threshold. In [71] the gray-scale variance in the direction orthogonal to the orientation of the ridges is used to classify each 16×16 block. In [72], the output of a set of Gabor filters is used as input to a clustering algorithm that constructs spatially compact clusters. In [73], fingerprint images are segmented based on the coherence, while morphology is used to obtain smooth regions. In [74], 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 in [75] 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 $N_x \times N_y$, so $I(i,j)$ represents the intensity at location (i,j) with $0 \le i \le N_x$ and $0 \le j \le N_y$, $0 \le I(i,j) \le L-1$. Here, L represents the maximum number of grey levels, and $K = \log_2(L)$ 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:

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

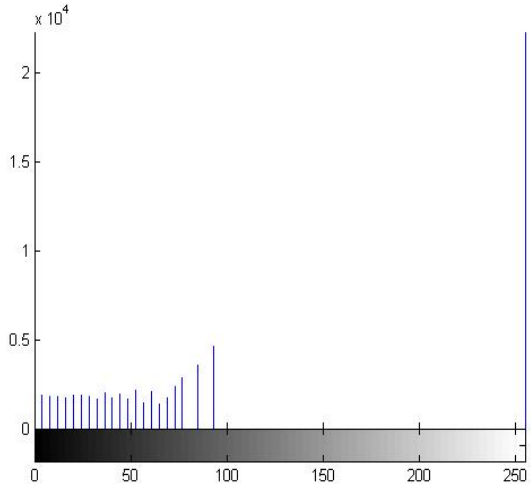
where h_k is the number of pixels whose grey value equal k.

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 [76], 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.

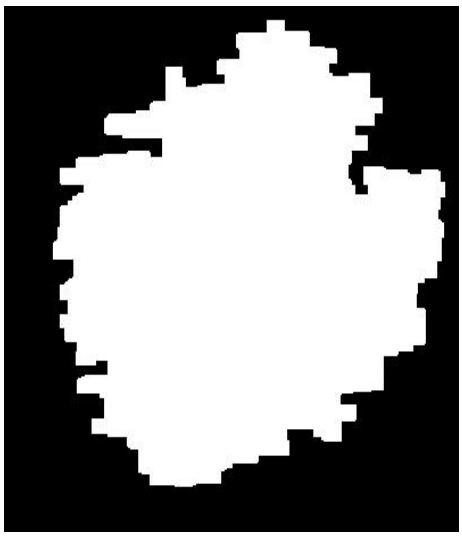
Fingerprint image.

(a)



Histogram of a fingerprint image.

(b)



Region of interest (ROI)

(c)

ROI of a fingerprint image.

(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:

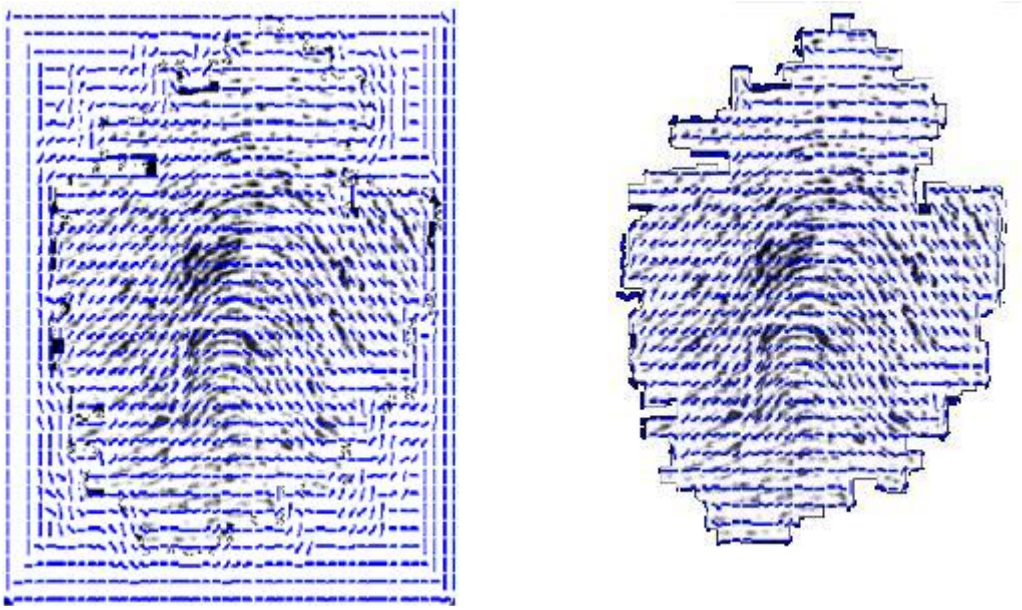
$$O_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} 2G_x(u,v)G_y(u,v) \qquad 3\text{-}2$$

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

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

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

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 have been 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).

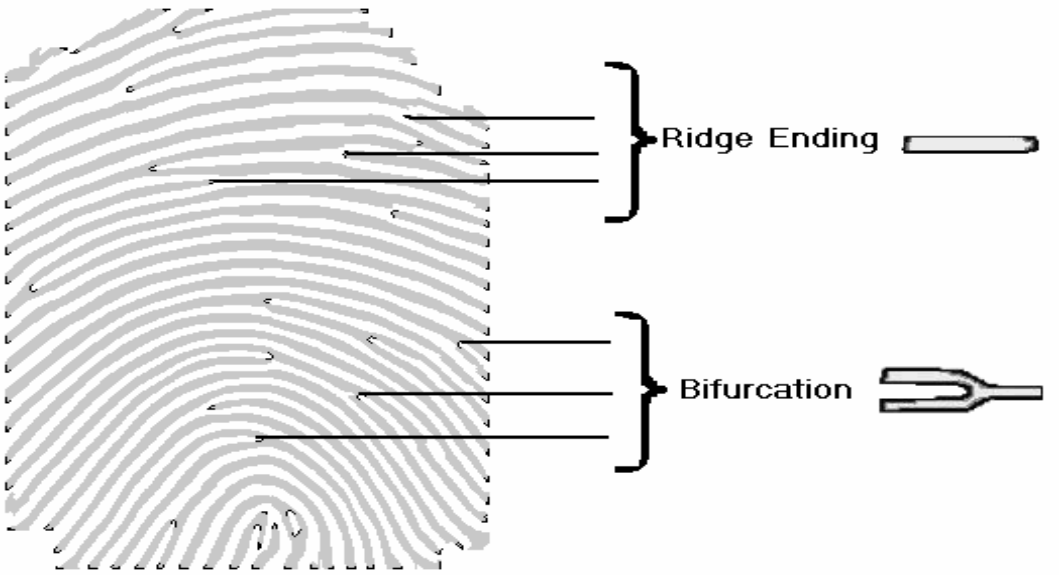


Figure 3-4 Examples of minutiae type

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 in [33] and is extensively utilized for contextual filtering of fingerprint images.

This representation is sensitive to the quality of the fingerprint images [6]. 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), [36]. 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 [78] cannot distinguish some invalid images from the valid ones. Validity statistical analysis could act as a pre-quality step to eliminate invalid images before applying any of quality assessment schemes [17, 18].

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

3.5 Validity Check Algorithm

The major novelties of validity check algorithm (VCA) consist of blind validity check and simple computational models. VCA is consists of two processing blocks, Figure3-6. Firstly, Object Area Segmentation (OAS) which performs a background subtraction (BS), and Pixels Weight Calculations (PWC). Secondly, the Image Validity is judged by threshold ratio (TRR) which experimentally obtains the base of good fingerprint images. TRR is defined to be judging values between 0.5 and 1; therefore the values out of this range indicate invalidity of tested images. TRR is used to train our approach for validity check to achieve a computational performance as well as principle core of image quality measures. VCA is applied to the base image element statistical weight calculation because the image element (pixel) describes an image object with the contrast, brightness, clarity and noising attributes.

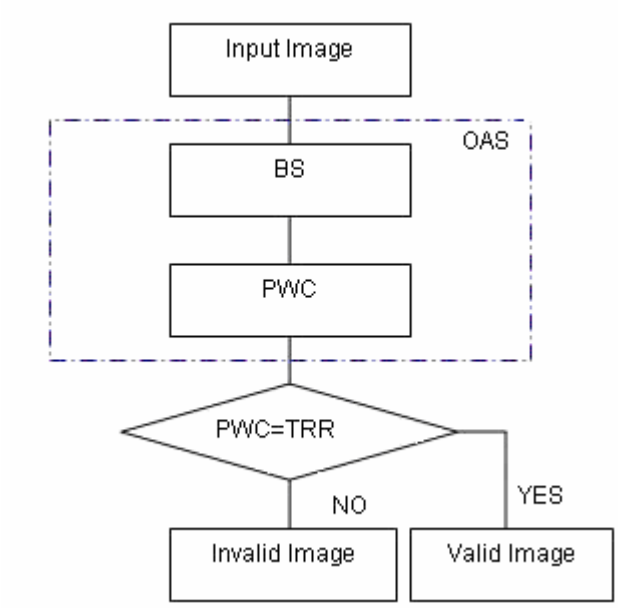


Figure 3-6 VCA flowchart

The VCA algorithm depends on fingerprint object segmentation, background subtraction, total image thresholding and pixel weight calculation. A none reference VCA signifies that the statistical weight calculation is relative to absolute pixel value after object background subtraction [18]. It works on a fact that no knowledge of the original image, and it doesn't make any assumptions on the type of invalidity factors. VCA found to be able to assign indicating quality assessment predictor.

3.5.1Objective Area Segmentation

This procedural block will segment the object region from the background based on morphological operations of global image threshold using Otsu method implementation Figure (3-6), [76]. Otsu method was chosen for its computational efficiency, where the image is a 2D grayscale intensity function and contains N pixels with gray levels from 1 to L. The pixels are classified into two classes based on a comparison of their intensity values with the threshold $T \in [0,255]$, class C_1 with gray levels $[1,...,t]$ and C_2 with gray levels $[t+1,...,L]$. Then, the grey level probability distributions for two classes are:

C_1 : $p_1 / \omega_1(t), \ldots p_t / \omega_t(t)$, and

C_2 : $p_{t+1}/\omega_2(t), p_{t+2}/\omega_2(t),..., p_L/\omega_2(t)$, where

$$\omega_{1(t)} = \sum_{i=1}^{t} p_i \qquad 3\text{-}6$$

and

$$\omega_{2(t)} = \sum_{i=t+1}^{L} p_i \qquad 3\text{-}7$$

also the means for classes C_1 and C_2 are

$$\mu_1 = \sum_{i=1}^{t} ip_i/\omega_1(t) \qquad 3\text{-}8$$

and

$$\mu_2 = \sum_{i=t+1}^{L} ip_i/\omega_2(t) \qquad 3\text{-}9$$

The mean intensity for the whole image μ_T will be

$$\omega_1\mu_1 + \omega_2\mu_2 = \mu_T \qquad 3\text{-}10$$

$$\omega_1 + \omega_2 = 1 \qquad 3\text{-}11$$

The between-class variance of the thresholded image was defined using discriminant analysis [9].

$$\sigma_B^2 = \omega_1(\mu_1 - \mu_T)^2 + \omega_2(\mu_2 - \mu_T)^2 \qquad 3\text{-}12$$

The optimal threshold (ot) is chosen so that the between-class variance σ_B^2 is maximized:

$$ot = MAX\{\sigma_B^2(t)\} \qquad 3\text{-}13$$

The object region segment from the background morphologically is defined by:

if $I(x,y) \rangle T$, then $I(x,y) \in$ object

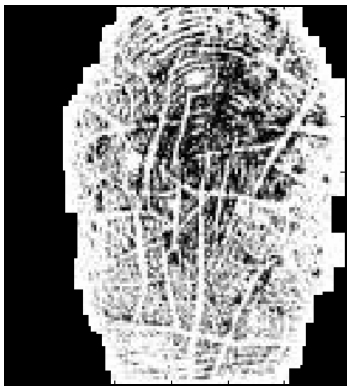
else

if $I(x,y) \leq T$, then $I(x,y) \in$ background

The background is subtracted to work over pure segmented, threshold image and binarized based on threshold level black and white image for the next block usage.

Dry Finger Light Print

Moist Finger Dark Print

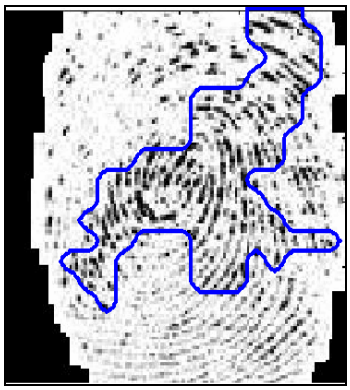


Worm Ridge Structure

Poor Finger Placement

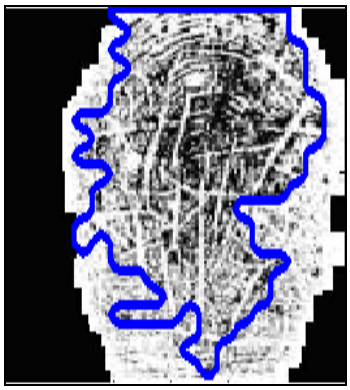
None Object Structure

(a)



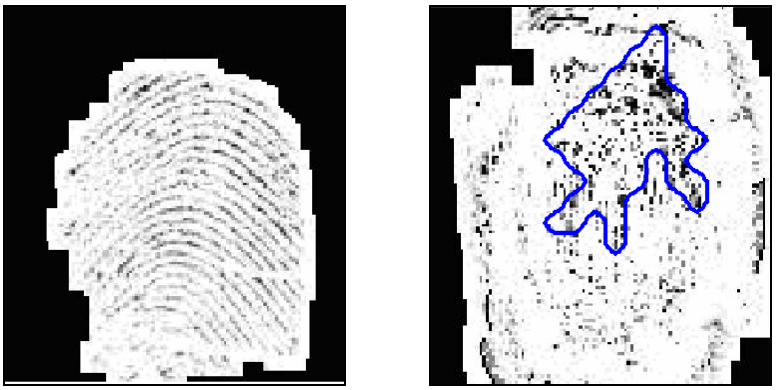
Dry Finger Light Print

Moist Finger Dark Print



Worm Ridge Structure

(b)



Poor Finger Placement None Object Structure

(b')

Figure 3-7 (a) Objects segmented areas, (b-b') object weighted areas

3.5.2 Pixels Weight Calculation

In this block, pixels will be counted into two groups, black group which is supposed to have a ridge structure of our fingerprint tested images, and a white group which belongs to the valley structure, ratio of black and white counts will indicate the validity contrast as well as hints of validity check of the whole image as result of image validity which is judged by threshold ratio. The valid result must be in the range between 0.5 and 1; therefore the values out of this range indicate invalidity of tested images.

3.6 Experimental Analysis

The proposed algorithm is extensively tested on DB1, FVC2000, FVC2004 databases, and TIMA MSN database [22]. Fingerprint images (TIFF, WSQ, JPG, BMP, format, different sizes, and resolutions). VCA was compared with the results of subjective quality survey as well as with results of NFIQ, NIST Fingerprint Image Quality.

3.6.1 Subjective Test

The subjective experiment was done as an image quality survey (IQS) based on visual assessment (subjective measurement). It was conducted on different image qualities, and validity taken from the previous databases. The validity factors were taken as image contrast, ridge clarity, valley clarity, image noise, and image content quality [informative

of image object, percentage of finger image]. The validity factors are selected between [0 and 100], 0 for no factor satisfaction, 100 for excellent presence of factor. For more refined assessments of image validity IQS was passed to 15 subjects working in the field of image processing and biometrics, since they are familiar with images and their directions. The 15 scores of each image were averaged to a final validity MOS, Table 3-1.

3.6.2 NIST Fingerprint Image Quality Test

Images were converted to the Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image format and tested under NFIQ software which generating image quality map by MINDTCT to measure the quality of localized regions in the image including determining the directional flow of ridges and detecting regions of low contrast, low ridge flow, and high curvature. The information in these maps is integrated into one general map, and contains 5 levels of quality (4 being the highest quality and 0 being the lowest). The background has a score of 0, a score of 4 means a very good region of fingerprint. The quality assigned to a specific block is determined based on its proximity to blocks flagged in the above-mentioned maps. The result in table 3-1 for NFIQ was the activation score of quality of images.

3.6.3 VCA Test

VCA was implemented in Matlab, and applied extensively on the same test source images as well as on the whole databases with the respect of human visual eye trace. This is because the human visual perception has a remarkable ability to detect invalid objects in visual image. Figure (3-8) shows the scatter relation between three tested approaches, where VCA is more close to human visual perception survey. Table 3-1 demonstrates how much each measurement approach coincides with human visual measure, while Table 3-2 shows the correlation relationship among tested approaches. All tests show that VCA can be added to the NFIQ factors to enhance its validity result. Also it could be part of a blind quality assessment for fingerprint images as a function of monitoring and controlling image enrollment for the sake of increasing the efficiency of the whole system, i.e. verification, identification and over above crypto key generation systems.

Image	Validity MOS	NFIQ	VCA
Image 1	0.5025	0.49	0.52
Image 2	0.363	0.34	0.32
Image3	0.524	0.47	0.52
Image 4	0.297	0.3	0.26
Image 5	0.3095	0.31	0.25
Image 6	0.348	0.36	0.26
Image 8	0.307	0.33	0.21

Table 3-1 Part of validity IQS, NFIQ and VCA results

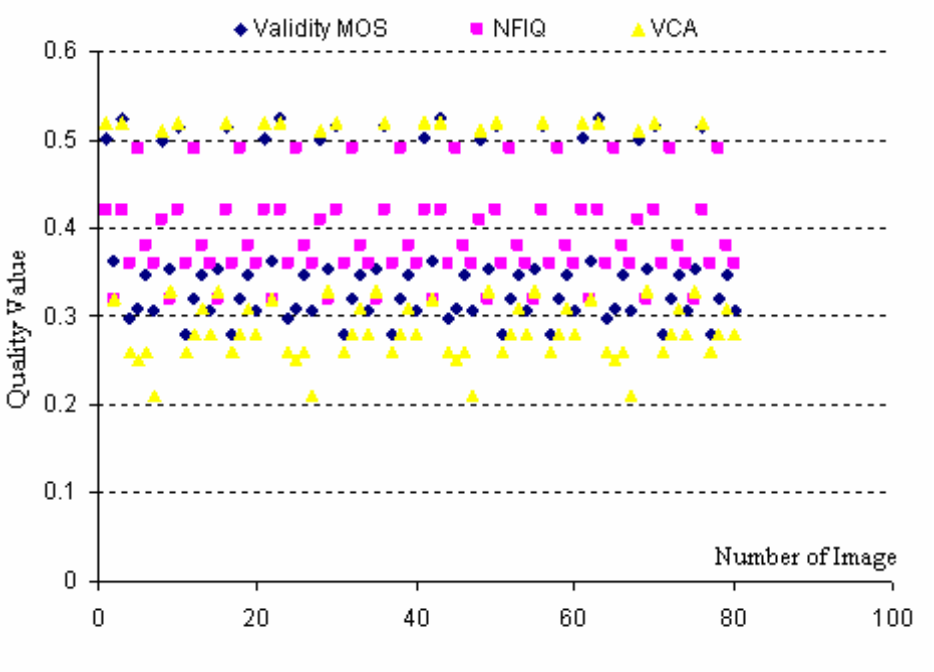


Figure 3-8 Approaches scattering relation

	Correlation Relation		
	Validity MOS	NFIQ	VCA
Validity MOS	1	0.977984	0.981753
NFIQ	0.977984	1	0.948127
VCA	0.981753	0.948127	1

Table 3-2 Correlation relation results of image validity measures

Correlation results indicate that the proposed algorithm is feasible in detecting low quality as well as non-fingerprint images.

3.7 Summary

In this chapter, a novel approach for image validity checks is presented, it is computationally efficient, since no complicated processes are computed and it is using system pre processing blocks such as segmentation and subtraction. Results show that the proposed approach is competitive with the state of the art method NFIQ and it could be a complementary factor in the image quality assessment process. Studying the characteristics structure of other biometric objects such as IRIS, FACE, we could say that implemented approach could be used. With the development of acquiring devices, and combination of NFIQ or any image quality estimation method and the VCA algorithm, acquiring devices such as scanners will enter into a new era - smart detection technology and checking of capturing sources. The following summarized remarks are useful for fingerprint image study:

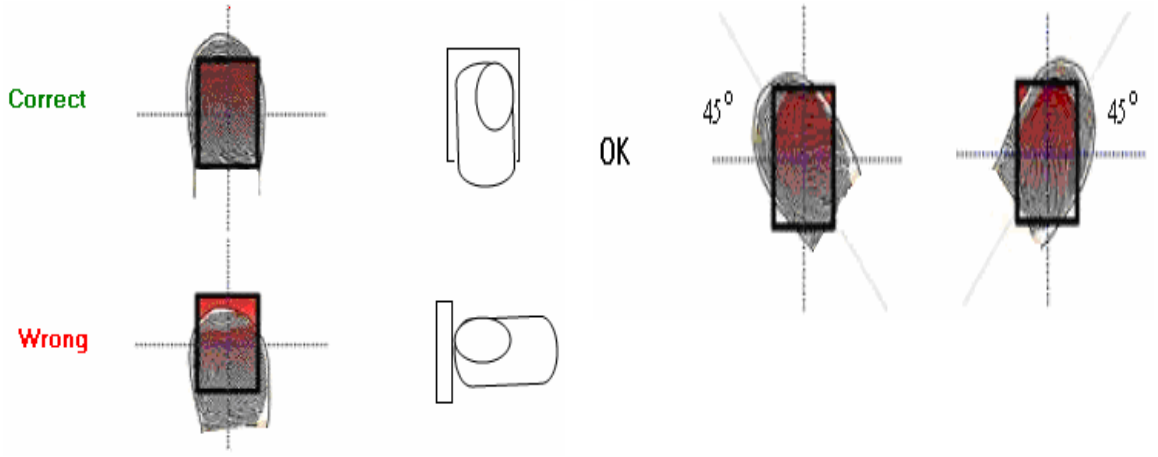
- Reliable extraction of fingerprint feature relies on image validity, quality and accurate image segmentation.
- Images with low contrast are difficult to segment.
- Image enhancement must be used to improve the visual appearance of fingerprint images.
- Validity check is a good predictor of image quality estimation.

Chapter 4 Fingerprint Image Quality Assessment

4.1 Introduction

Fingerprint images are subject to a wide variety of distortions during acquisition, analysis, processing, compression, storage, transmission and reproduction, any of which may cause a degradation of its visual quality. The most fundamental problem of the error visibility framework is image quality definition. In particular, it is not clear that error visibility should be equated with image quality degradation, since some types of distortions may be clearly visible but not perceptual. Images may be corrupted by sources of degradation, which could be raised during acquisition, transmission, processing and reproduction [79]. To maintain, control, and enhance the quality of images, it is important for image life cycle systems, e.g. acquisition, management, communication, and processing to be able to identify and quantify image quality degradations [80]. The development of real-time fingerprint image quality assessment can greatly improve the accuracy of fingerprint image based systems, it is utilized to evaluate the system performance [23, 25, 81, 82], assess enrolment acceptability [83], evaluate the performances of fingerprint sensors and improve the quality of fingerprint databases [84]. The idea is to classify fingerprint images based on their quality, where, it is desirable to assess the quality of a fingerprint image in real time as a quality control procedure. This allows poor image acquisition to be corrected through recapture and facilitates the capture of best possible image within the capture time window configured in the system and image capture system will be calibrated and controlled to satisfy the image quality parameters. Therefore, it is appropriate to select minor or major image pre-processing techniques. The essential factors for fingerprint image quality metrics are: captured image size, captured image position and placement Figure (4-1(a)), image orientation Figure (4-1(b)), ridge clearness Figure (4-2), matching features quantity Figure (4-3), and distortion of image Figure (4-4)

which is difficult to assess without actual matching. Good quality images require minor pre-processing and enhancement, while bad quality should be rejected. Processing parameters for dry images (low quality) and wet images (low quality) should be automatically determined. These results can be improved by capturing more good quality fingerprint images to increase the system identification accuracy and the integrity of fingerprint database. In this chapter, we aim to develop a scheme which allows the quantitative deterministic assessment of fingerprint image quality. The scheme assesses the percentage or size of the given image that may contain an actual fingerprint and how reliable the ridge flow could be detected from the located fingerprint area. This assessment should agree as closely as possible with that pre obtained subjective analysis test. It should be noted that exact correlation will never be achieved due to natural variations in the subjective assessment. The most meaningful image quality measures are based on visual assessment (subjective measurement). Subjective tests have shown that the eye tends to concentrate upon those areas of a scene or image where there is a high concentration of contours, i.e. fingerprint images ridges and valleys. In this chapter, we will describe the construction of image quality measurements, the performance evaluation of image quality assessment techniques. A new quality assessment technique based on assurance quality of services will be proposed. As a conclusion comparison results will be discussed.



(a) (b)

Figure 4-1 (a) Fingerprint image capturing position and placement , (b) Orientation field

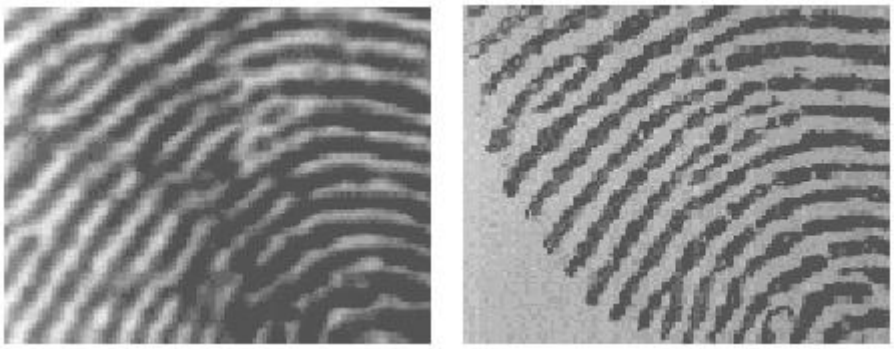


Figure 4-2 Ridge clearness images

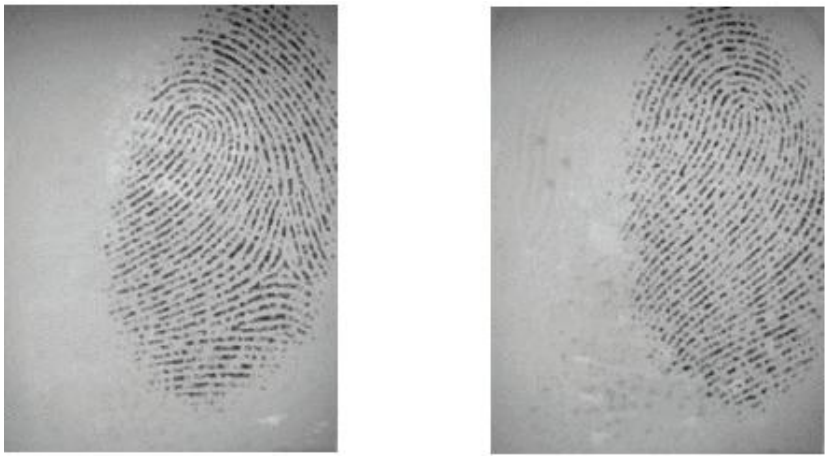


Figure 4-3 Very few minutiae for images from FVC2002

Figure 4-4 Distorted fingerprint images from FVC2004

4.2 Image Quality Measures

Image quality assessment and comparison metrics play an important role in various graphics orientated applications. They can be used to monitor image quality for further processing systems, they can be employed to benchmark image processing algorithms, and they can be embedded into the rendering algorithms to optimize their performances and parameter settings. Fingerprint images may undergo distortions during preliminary acquisition process, compression, restoration, communication or final database enrolment. Hence image quality measurement plays a significant role in several image-processing applications. Image quality, for scientific, forensic, and security purposes, can be defined in terms of how well desired information can be extracted from the source image. An image is said to have acceptable quality if it shows satisfactory usefulness, which means discrimination of image content, extractability of its features, and satisfactory clearness, which means identification of fingerprint image content, i.e. ridges, valleys. Image quality metrics are important performance variables for digital imaging database systems, and are used to measure the visual quality of processing images [85]. There are three major types of quality measurements: subjective, objective and perceptual measurement. In this thesis; it is investigated how to find the coefficient correlation between proposed objective quality assessment algorithm and subjective opinion score. It is obvious to know that measuring the quality of the fingerprint images is required. Hence, quality measurement is one of the pre-processing stages of cryptography key generation models. We can acquire a higher quality image by taking the quality of the image in the post-processing stage of the authentication and matching process. Also, by rejecting a low quality image and making user to input the correct fingerprint Figure (4-1(a)), we can guarantee better image quality. The bifurcation and the ridges become unclear if there is too much or less pressure on the finger in the input process. If the quality of fingerprints is poor (bad), we can find out three cases: false minutiae finding, omission of minutiae, and error occurrence in the position of minutiae. In order to solve these problems, the enrolment stage must have a measure to select the good quality of fingerprint images. Quality measurement is increasingly deployed in all biometric based systems to predict the performance fact of given systems, i.e. evaluation criteria for assessing the

performance of image enhancement, feature extraction and matching with respect to the quality indices.

4.2.1 Subjective Quality Measurement

Generally, the image quality assessment (IQA) has been performed subjectively using human observers based on their satisfaction, where subjective experiments are used to be the benchmark for any kind of visual quality assessment. Since human beings are the ultimate receivers in most image processing applications, the most reliable way of assessing the quality of an image is by subjective evaluation. A subjective quality measure requires the services of a number of human observers, the MOS is based on the results of human observers' assessments. Their assessments depend on the type, size, range of images, observer's background and motivation and experimental conditions like lighting, display quality etc. The observer viewpoint concentrations in case of fingerprint image are: clear ridges, low noise, and good contrast, then they might reasonably say it is good quality. A human judgment is really on how perfect is their human visual system (HVS) as a core of subjective and perceptual quality assessment. The HVS, reviewed in a number of literatures, e.g. [85, 86] is viewed as an information processing system and its major psychophysical features were modelled, e.g. contrast sensitivity function (CSF), light adaptation, and contrast masking. The contrast sensitivity function is the first feature of HVS; it models the sensitivity of the HVS as a function of the spatial frequency content in visual stimuli. The second feature of HVS is the light adaptation or luminance masking perception obeys Weber's law, which can be expressed as

$$\frac{\sigma I}{I} = K \qquad 4\text{-}1$$

Where I is the background luminance, and σI is the just noticeable incremental luminance over the background by the HVS, and K is a constant called Weber function. Weber's law is maintained over a wide range of background luminance's and breaks only at very little low or high light conditions. Light adaptation allows the HVS to encode the contrast of the visual stimulus instead of light intensity. The fourth feature of HVS is contrast masking where it is referring to the reduction of visibility of one image component due to the presence of masker. Masker strength is measured by the variation

of signal visibility within presence or absence of masker. The HVS is enormously complex with optical, synaptic, photochemical and electrical phenomena. HVS modelled for objective representation while it is a core results of subjective assessment, i.e. a sight basement of observers opinion score and it is reliability affecting the mean results score, observers decisions are limited arranging in standard values defined by the International Telecommunication Union (ITU), ITU suggest standard viewing conditions, criteria for the selection of observers and test material, assessment procedures, and data analysis methods. The ITU has recommended a 5-point scale using the adjectives bad, poor, fair, good and excellent [87]. The ITU scale was used in all subjective based tests, as well as a basic scale for MOS [19]. The MOS is generated by averaging the results of a set of subjective tests, where a number of subjects are asked to watch the test images and to rate their quality. Subjective tests may measure impairment scores as well as quality scores; or they can be asked to rate the degree of distortion, the amount of defects or the strength of artefacts. Subjective quality measurement techniques provide numerical values that quantify viewer's satisfaction; however, subjective experiments require careful setup and are time consuming because observers response may vary, hence expensive and often impractical. Furthermore, for many applications such as online quality monitoring and control subjective experiments cannot be used at all. They provide no constructive methods for performance improvement and are difficult to use as a part of design process. It is used to predict the successfulness of objective proposing methods within correlated relation.

4.2.2 Perceptual Quality Measurement

The perceptual quality measurement techniques are based on models of human visual perception like image discrimination models and task performance based models. Ideally, they should be able to characterize spatial variations in quality across an image. The several perceptual image discrimination quality metrics have been proposed as alternatives to objective metrics; for example, methods which incorporate luminance adaptation and contrast sensitivity functions, metrics which incorporate observer performances for supra threshold artefacts, and threshold perceptual metrics. The perceptual models are based on properties of the visual system and measurements of the

eye characteristics, e.g. CSF, light adaptation, and masking [88]. The perceptual metrics can provide a more consistent estimation of image quality than objective metrics when artefacts are near the visual threshold. Image discrimination models used in perceptual quality assessment, however, have been developed for measuring general quality degradation introduced by compression processes. The implementation of these metrics is also often complex, and time-consuming subjective psychophysical testing is required for validation [89]. While task-based model observers have been designed to predict human visual detection of signals embedded in noisy backgrounds, the effect of quality degradations on the performance of detecting analysis features for fingerprint image requires further investigation. This kind of measurement could be used in refining fingerprint images for the purpose of updating database sources. Fingerprint image database refining is based on image fidelity, which is the subset of overall image quality that specifically addresses the visual equivalence of two images. It is used to determine the difference between two images that are visible to the human visual system. Usually one of the images is the reference which is considered to be original, perfect or uncorrupted. The second image has been modified or distorted in some sense. It is very difficult to evaluate the quality of an image without a reference. Thus, a more appropriate term would be image fidelity or integrity, or alternatively, image distortion. In addition to the tow digital images, an image fidelity based on perceptual metric requires a few other parameters, e.g. viewing distance, image size, display parameters. The output is a number that represents the probability that a human eye can detect a difference in the two images or a number that quantifies the perceptual dissimilarity between the two images. Alternatively, the output of an image perceptual metric could be a map of detection probabilities or perceptual dissimilarity values. The most common stages that are included in the perceptual model are:

Calibration, it is the conversion of input image values to physical luminance's before they enter the HVS model.

Registration, i.e. the point by point correspondence between two images, is necessary for any quality metric to make any sense. Otherwise, the value of a metric could be

arbitrarily modified by shifting one of the images. The shift does not change the images but changes the value of the metric.

Display model, i.e. an accurate model of the display device is an essential part of any image quality metric, as the HVS can only see what the display can reproduce. Display model effects are incorporated in the perceptual model, therefore, when the display changes, a new set of the perceptual model must be obtained.

4.2.3 Objective Quality Measurement

Objective image quality measures play important roles in various image processing applications. It seeks to measure the quality of target images algorithmically. A good objective measure reflects the distortion on image due to blurring, noise, compression and sensor inadequacy. One expects that such measures could be instrumental in predicting the performance of vision based algorithms such as extraction, image based measurements, detection, segmentation, etc., tasks. Objective analysis involves use of image quality/distortion metrics to automatically perceive image quality; Peak Signal-to-noise Ratio (PSNR) and Mean Squared Error (MSE) are the most common objective criterion [87, 90]. These methods provide mathematical deviations between original and processed images. Mathematical metrics measure quality in terms of relative simple mathematical functions, usually with pixel-by-pixel weighted differences between the reference R and the distorted image D. MSE and PSNR defined as:

$$MSE = \frac{1}{I}\sum_{i=1}^{I}(R_i - D_i)^2 \qquad 4\text{-}2$$

$$PSNR = 10 \cdot \log_{10}\frac{R_M^2}{MSE} \qquad 4\text{-}3$$

where I is the total number of pixels in the image and R_M is the maximum possible reference intensity value. The analysis depends on the number of images used in the measurement and the nature or type of measurement using the pixel elements of digitized images. However, these simple measures operate solely on the basis of pixel-wise differences and neglect the important influence of region of interest image content and viewing conditions on the actual visibility of artefacts. Therefore, they cannot be

expected to be reliable predictors of perceived quality. Metrics have been defined either in the spatial or frequency domain. These measurement techniques are easy to calculate, however they do not consider human visual sensitivities. They do not adequately predict distortion visibility and visual quality for images with large luminance variations or with varying content. An objective quality assessment classified into graphical and numerical classes, histogram criteria is an example of the graphical class and MSE is a numerical example. It is believed that a combination of numerical and graphical measures may prove useful in judging image quality. Objective image quality metrics can be classified according to the availability of an original (distortion-free) image, with which the distorted image is to be compared. Most existing approaches are known as *full-reference*, meaning that a complete reference image is assumed to be known. In many practical applications, however, the reference image is not available, and a *no-reference* or "blind" quality assessment approach is desirable. In a third type of methods, the reference image is only partially available, in the form of a set of extracted features made available as side information to help evaluate the quality of the distorted image. This is referred to as *reduced-reference* quality assessment. This thesis focuses on non-reference image quality assessment for the sake of automatic acceptance and rejection of target fingerprint image. Thus, the term quality assessment is not used here to refer to the fidelity of the tested sample, but instead to the utility of the sample to an automated system. It is a difficult task to objectively weight the clearness of fingerprint ridges, low noise, and image good contrast. A blind quality assessment is a good indicator for validity check while validity benchmark is good quality estimator and vice versa [91]. Both validity and quality estimators are used to be matching performance predictive of biometric systems. The main goal of objective quality assessment is to design algorithms whose quality prediction is in good agreement with subjective scores from human observers. There are different attributes that characterize an objective quality approach in terms of its prediction performance with respect to MOS [56]. The most important one is its accuracy. Where accuracy is the ability of a metric to predict subjective ratings with minimum average error and can be determined by means of the *Pearson* linear correlation coefficient (PLCC). For a set of D data pairs (x_i, y_i), it is defined as follow

$$Pearson = \frac{\sum_{i=1}^{N}\left(x_i - \bar{x}\right)\left(y_i - \bar{y}\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i - \bar{x}\right)^2}\sqrt{\sum_{i=1}^{N}\left(y_i - \bar{y}\right)^2}} \qquad 4\text{-}4$$

where $\bar{x}$ and $\bar{y}$ are the means of the respectively objective and subjective data.

This assumes a linear relation between the data sets, which may not be the case. Therefore, in this thesis correlation will be used to obtain relative comparisons between subjective and objective data, as well as to investigate the performance of the proposed objective metrics. The objective metrics developed in this thesis will be used in different stages of bio crypto image processing based and analysis systems as monitoring, optimization, and benchmarking, and will be compared to the state of the art objective metrics currently in use.

4.3 Objective Image Quality Methods

One of the important goals of quality assessment research is to design algorithms for objective evaluation of quality in a way that is consistent with subjective human evaluation. By "consistent" we mean that the algorithm's assessments of quality should be in close agreement with human judgements, regardless of the type of distortion corrupting the image, the content of the image, or strength of the distortion. Depending on how much prior information is available and on how a perfect candidate image should look like, objective image quality algorithms can be classified as "Full-reference" or bi-variant, in which the algorithm has access to the perfect image, "No-reference" or uni-variant, in which the algorithm has access only to the distorted image and "Reduced-reference", in which the algorithm has partial information regarding the perfect image. All algorithms try to map the reconstructed image to some quantity that is positive and zero only when original and modified images are identical and also increases monotonically as the modified image looks worse. It is very useful to be able to automatically assess the quality of images when the number of images to be evaluated is large. The currently available quality measurement methods are in general restricted due to the fact that actually only very limited and isolated models for the determination of perception based image attributes exist. As a result, objective image quality measurement

methods are in most cases easy to apply, but only in a few cases can their results be generalised. Fingerprint image quality assessment is a difficult yet very important task in the evaluation of any fingerprint imaging applications. Fingerprint image quality affects the performance and interoperability of fingerprint based application, e.g. identification, authentication, and built on based crypto systems. The basic premises of fingerprint image quality assessment are based on extractable information as a task of quality assessment information, e.g. ridges and valleys, how this information will be extracted, how it will be correlated to the extracting observation and finally the statistical analysis between image and object according to the noise measurement. Blind quality assessment is desirable in finger crypto key generation, where the reference image is unavailable and assessment will be taken according to the available image information and or extraction based features availability.

4.3.1 Full Reference Method

Full reference (FR) image quality assessment (QA) algorithms generally interpret image quality as fidelity or similarity with a “reference” or “perfect” image in some perceptual space Figure (4-5). Such “full-reference” QA methods attempt to achieve consistency in quality prediction by modelling salient physiological and psycho visual features of the HVS, or by signal fidelity measures. FR methods approach the image QA problem as an information fidelity problem [80, 92]. FR quality assessment method is completely dependent on a referenced image, so the analysis and investigation of a target image refereed by a used factor during the design or evaluation of a FR system. The reference signal is typically processed to yield a distorted (test) visual data, which can then be compared to the reference using full reference methods. Typically, this comparison involves measuring the “distance” between the two signals in a perceptually meaningful way. This can be achieved by studying, characterizing and deriving the perceptual impact of the distorted signal to human viewers by means of subjective experiments. The full reference metric is convenient for image coding scheme comparison [93]. The full-reference measures can be used to estimate a spectrum of distortions that range from blurriness and blockiness to several types of noise; this could be noticed in case of image transmission over noisy channels. Fingerprint images may be a subject of transmission

for database renewing where it requires the entire reference content to be available, usually in uncompressed form, which is quite an important restriction on the usability of such metrics. In general, full reference assessment considers structural similarity (SSIM) and peak signal to noise ratio (PSNR) as image quality assessors.

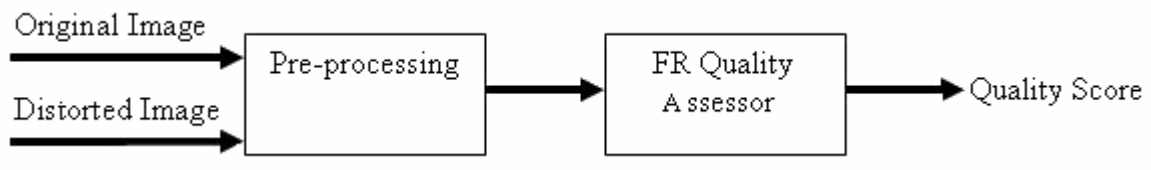


Figure 4-5 Diagram of a full reference image quality assessment system

Both the SSIM and PSNR are related to the human visual system, noting that people evaluate image quality based on structural information rather than pixel intensities themselves. The principle idea underlying the structural similarity approach is that the HVS is highly adapted to extract structural information from visual scenes, and therefore, a measurement of structural similarity (or distortion) should provide a good approximation to perceptual image quality. A full reference method can be used also in evaluation and comparative study of fingerprint image quality estimation and benchmarking approaches.

4.3.2 Reduced Reference Method

Reduced-reference (RR) image quality measures aim to predict the visual quality of distorted images with only partial information about the reference images. Reduced-reference measures are between full-reference and no-reference measures; RR approaches were clearly introduced in video, audio transmission and still images applications while it is still an open research issue in a fingerprint image based systems. Applying RR method on fingerprint images is a hard task since a high-quality reference image of the same individual is usually not available, i.e. the link to the individual cannot be established in advance. A representative extracting feature is the basic fundamental of a RR quality assessment evaluator. Figure (4-6) shows how an RR quality assessment method may be deployed in still images real applications.

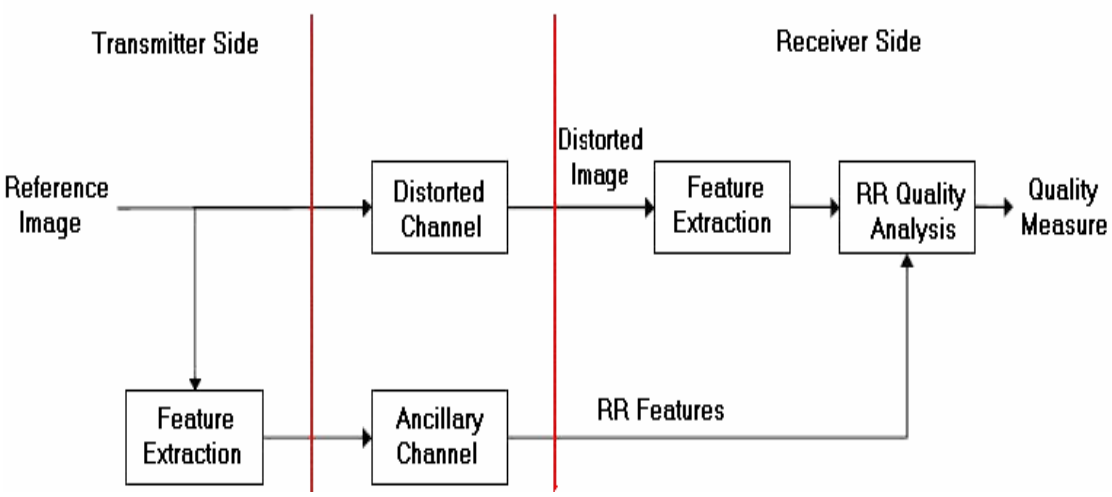


Figure 4-6 Block diagram of conventional reduced reference image quality methods.

At the sender side, a feature extraction process is applied to the original image, and then the extracted features are transmitted to the receiver as side information through an ancillary channel. Although it is usually assumed that the ancillary channel is error free. Another choice is to send the RR features in the same channel as the image being transmitted. In that case stronger protection of the RR features relative to the image data is usually needed. When the distorted image is transmitted to the receiver through a regular communication channel with distortions, feature extraction is also applied at the receiver side. This could be exactly the same process as in the sender side, but it might be adjusted according to the side information, which is available at the receiver side. In the final stage of RR quality assessment method, the features that were extracted from both the reference and distorted images are employed to yield a scalar quality score that describe the quality of the distorted image. RR features should provide efficient summary of the reference image, they should be sensitive to a variety of image distortion and they should have good perceptual relevance. In most cases, RR features are simply a set of randomly selected image pixels. When these pixels are transmitted to the receiver, they are compared with corresponding pixels in the distorted image. The MSE or PSNR value between the reference and distorted images can then be estimated. This method is used for assessing the quality of fingerprint images by extracting informative features. Fronthaler, et al. [94] exploited the orientation tensor which holds edge and texture information to assess the quality of fingerprint images. Their method decomposes the

orientation tensor of an image into symmetry representations, where the included symmetries are related to the particular definition of quality and encode a priori content-knowledge about the application (e.g. fingerprints).

4.3.3 Non Reference Method

No-reference (NR) image quality measures or blind image quality assessment is the most difficult problem in the field of image analysis [95]. In case of blind quality assessment an objective model must evaluate the quality of any real image, without referring to an original high quality image. Blind image quality assessment is useful to many fingerprint image based applications. In all image based applications, the original high resolution image is often not available as the ground truth; therefore blind assessment of the quality acquisitioned, enrolled, registered, and further processed fingerprint images become necessary. All previous fingerprint image quality assessment techniques were based on non reference method principles: absent of reference image, entire information usage to compute the total image quality score. Several assessment techniques have been described in the literature (reviewed in chapter 2), and they were divided into: 1) those that use local features of the image; 2) those that use global features of the image; and 3) those that address the problem of quality assessment as a classification problem [96]. But they are reclassified into two main classes' Figure (4-7). Structural and intelligent representation approaches.

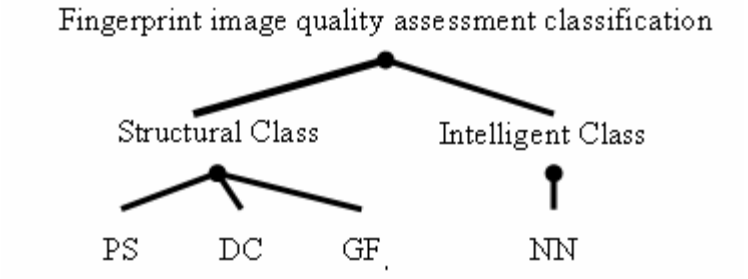
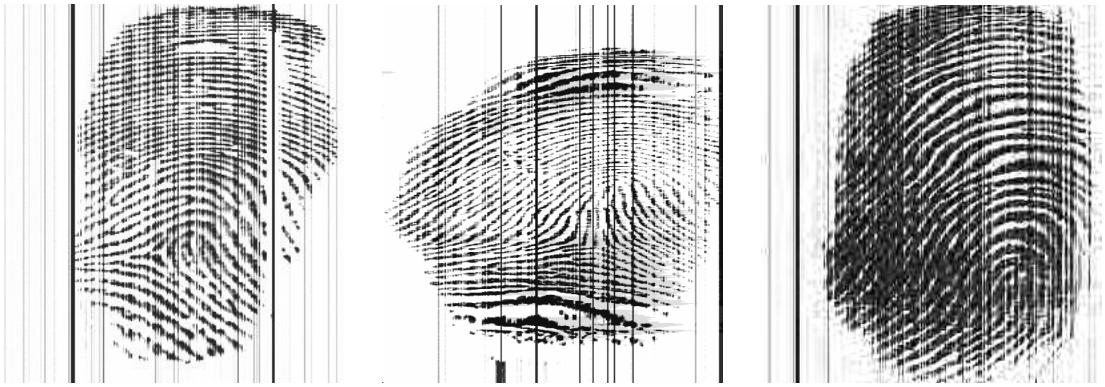


Figure 4-7 Fingerprint image quality assessment classification, where PS is Power spectrum, DC is Directional contrast, GF is Gabor feature and NN is Neural network.

Methods that rely on image features either global or local are tied on structural representation [23, 29, 97, 98] and they are divided into three types: Power Spectrum, Orientation flow, and Gabor feature based, while second class was proposed in [36] as intelligent neural network fingerprint image quality estimator, these types of methods rely on computing a feature vector using the quality image "map" and minutiae quality statistics produced by the minutiae detection algorithm. The feature vector is then used as inputs to a Multi-Layer Perceptron (MLP) neural network classifier, and the output activation level of the neural network is used to determine the fingerprint's image quality value.

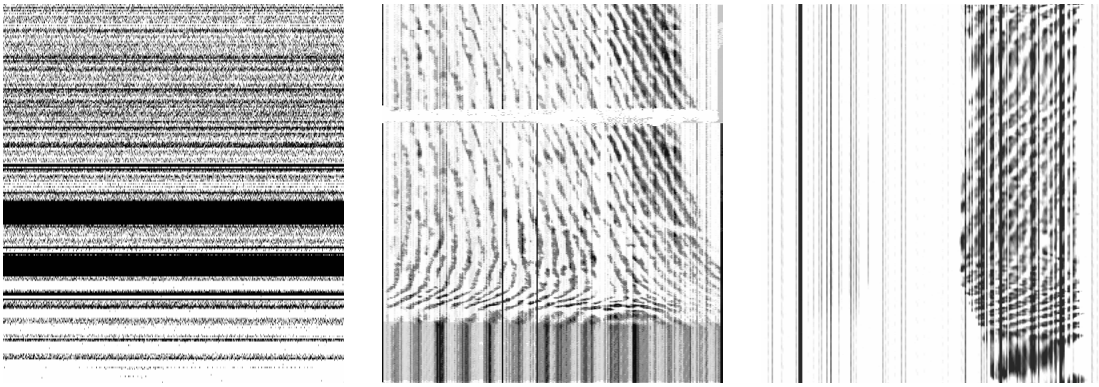
4.4 Gabor Spectrum Approach for Fingerprint Image Quality Assessment

Fingerprint images are subject to poor and invalid acquisition 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), while Figures (4-8 & 4-9) show examples of good and bad quality images of TIMA fingerprint database. Fingerprint image quality is usually defined as a measure of structural feature representation, i.e. ridge and valley clarity and their end extraction points, i.e. minutiae, core and delta points. The performance of fingerprint systems is affected by fingerprint image quality and most available systems use global and/or local fingerprint features for matching based or security systems, therefore feature extraction is very sensitive to validity, integrity, and quality of source images.



Nik_index1.tif 1_ben_index2.tif 7_nik_auricu1.tif

Figure 4-8 Good Fingerprint Images



No_contact_pb4.tif cut6.tif Strange9.tif

Figure 4-9 Bad and non Fingerprint Images

For instance, false extracted features may appear due to previous poor and invalid fingerprint factors. Quality assurance of stored template at the enrollment of automatic recognition system, quality ware fusion, and image region variety check for enhancement guidance reasons are the benefits of blind fingerprint image quality assessment[94]. Therefore, it is desirable to assess the quality of image to improve the overall performance of biometric systems, but it is a difficult task due to blind automatic prediction of perceived image quality. We used Gabor and Fourier power spectrum methods to get a novel Gabor spectrum (GS) approach [19], and quantitatively compare the implantation results of GS with respect to an existing two classes, as well as, manually human image quality survey (IQS) which assigned quality estimation values on the TIMA database [22].

4.4.1Gabor Features

The characteristics of Gabor filter, especially the frequency and orientation representations, are correlated with perceptual image and similar to those of the human visual system. Therefore, Gabor features were used for computation of foreground-background segmentation, degree of smudginess and dryness of fingerprint images. The 2D Gabor function is represented as a Gaussian function modulated by a complex sinusoidal signal and it is adopted for feature extraction, Equation (2-6). Since most local ridge structures of fingerprints can be modelled as oriented sinusoids along a direction normal to the local ridge orientation [97], the Gabor parameters are set to the following values: frequency of the sinusoidal plane wave; $f = 0.125$ (corresponds to inter-ridge distance of 8), standard deviations of the Gaussian envelope along x, y axes; $\sigma_x = \sigma_y = 4$, and $\theta = \{0^\circ, 22.5^\circ, 45^\circ, 67.5^\circ, 90^\circ, 112.5^\circ, 135^\circ, 157.5^\circ\}$, resulting in eight Gabor filter, Figures (4-10), (4-11). These values were set to be used for databases quality analyses. Gabor feature extraction is performed by convolving the input image with the set of Gabor filters, Equation (4-5). It is used to determine the quality of fingerprint images [23, 98]. An image is divided into blocks of size w centred at (X, Y), the magnitude Gabor feature at that sampling point can be defined as follows:

$$g(X, Y, \theta_k, f, \sigma_x, \sigma_y) = \left| \sum_{x=-w/2}^{(w/2)-1} \sum_{y=-w/2}^{(w/2)-1} I(X+x, Y+y) h(x, y, \theta_k, f, \sigma_x, \sigma_y) \right|, \quad 4\text{-}5$$

where $k = 1,...m$, $I(x, y)$ denotes the gray-level value of the pixel (x, y), and w is the size of the blocks in divided image. m Gabor matrices are obtained according to the Gabor parameters set. Then, each block is sampled by these matrices and m Gabor features are obtained. A $(w \times w)$ block is then compressed to m meaningful Gabor features. Finally, the standard deviation value of each block is computed by Equation (2-7).

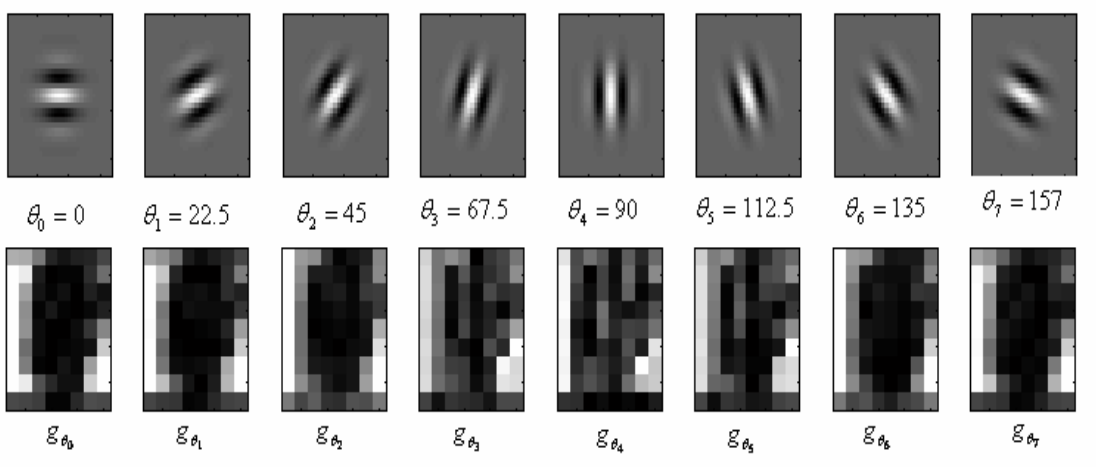


Figure 4-10 Gabor features of (Nik_index1.tif) fingerprint images

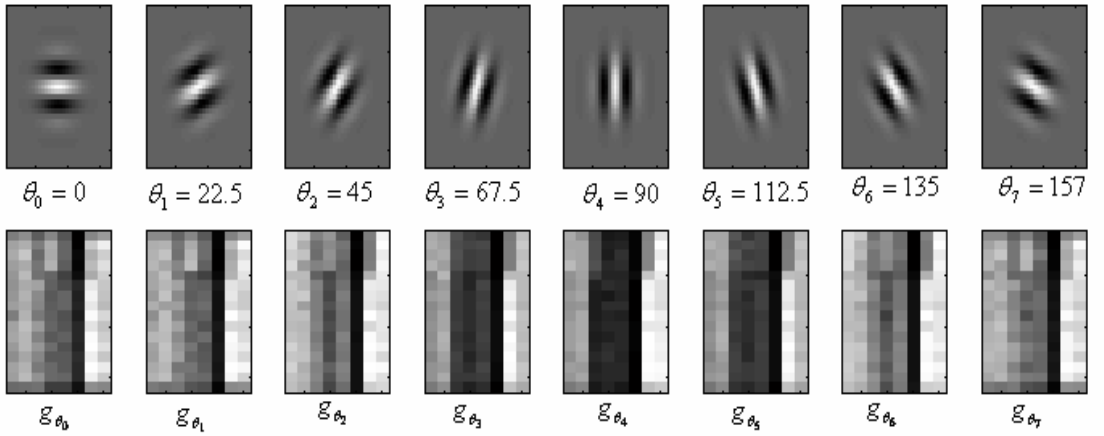


Figure 4-11 Gabor features of (No_contact_pb4.tif) fingerprint images

The standard deviation value is used for both image quality estimation and fingerprint image segmentation. Fingerprint area (foreground) is segmented depending on the standard deviation value, if it is less than the block threshold value, the block is counted as background; otherwise the block is counted as a foreground block. The quality field for a foreground block is counted to be good quality if it is more than the preset quality threshold; otherwise it is counted as a bad block. The total quality of the fingerprint image is calculated according to the quantities of foreground blocks, Equation (2-8). In this case, the fingerprint image is counted as good quality if total quality value is bigger than a pre determined threshold; otherwise it's counted as a poor quality image.

4.4.2 Gabor Spectral Method

Gabor spectral method (GSM) used benefit of both Gabor and Fourier power spectrum methods, such as frequency and orientation representations. GSM is based on spectrum analysis of Gabor features banks within orientations: [0: pi/8: 7pi/8] for all non overlap fingerprint image blocks. Method flowchart is shown in Figure (4-12). GSM performs fingerprint image resizing into (256x256) for the reason of using same size images, then a (32x32) non-overlapping block is used to find block quality estimation, after that GSM procedure is started with calculating the spectrum of Gabor feature banks within given orientations, section (4.4.3). The standard deviation of calculated feature is used to determine the quality of under process block, and then the total quality of image is calculated by averaging blocks determined quality. Final quality will be measured in range [0, 1] after applying a chosen normalization factor on averaged determined quality.

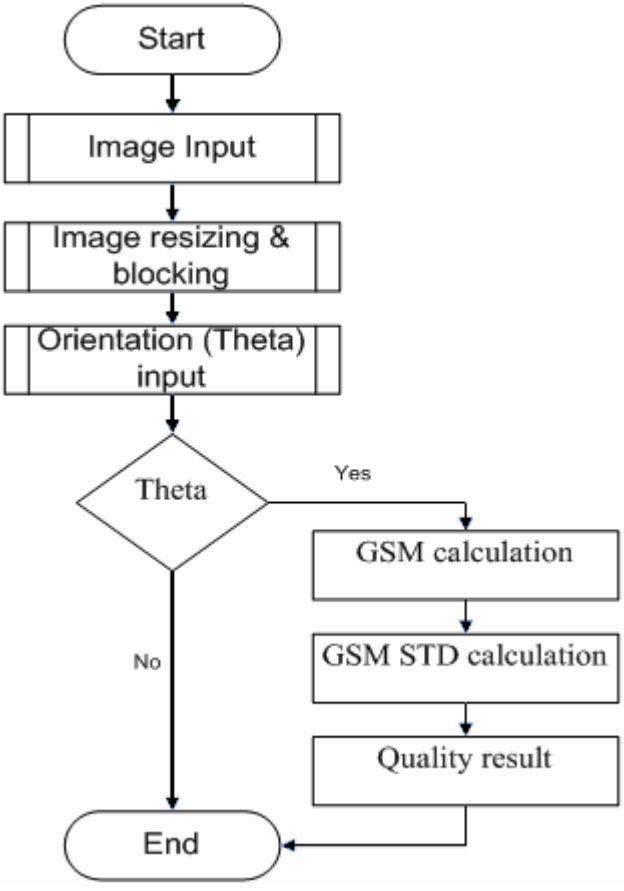


Figure 4-12 Gabor spectrum method block diagram.

4.4.3 GSM Mathematical Background Analysis

An even value of Gabor function represents the characteristics of function filtration for frequency and orientation similarities of the human visual system [99]. The Gabor features spectrum will be found by Fourier Transform of 2-d even symmetric Gabor function, where the 2-d even symmetric Gabor function is defined as:

$$g(x,y) = e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}} \cdot \cos(2\pi f x') \qquad 4\text{-}6$$

where $x' = (x\cos\theta + y\sin\theta), y' = (-x\sin\theta + y\cos\theta)$ are rotated coordinates,

Thus $g(x,y) = e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}} \cdot \cos(2\pi f(x\cos\theta + y\sin\theta))$

$$= e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}} \cdot \cos(2\pi fx\cos\theta + 2\pi fy\sin\theta)),$$

where $\theta_1 = 2\pi fx\cos\theta$, and $\theta_2 = 2\pi fy\sin\theta$; So

$g(x,y) = e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}} \cdot \cos(\theta_1 + \theta_2)$, Using trigonometric identity (Euler's formula) $\cos(\theta_1 + \theta_2) = \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2$, Then

$$g(x,y) = e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}} \cdot (\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2)$$

Thus

$$g(x,y) = e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}} \cdot \cos\theta_1\cos\theta_2 - e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}} \sin\theta_1\sin\theta_2 \qquad 4\text{-}7$$

The Fourier Transform of Equation (4-7), 2-d symmetrical Gabor function is

$$F(g(x,y))(u,v)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}g(x,y)\cdot e^{-2j\pi(ux+vy)}dxdy \qquad 4\text{-}8$$

Using equation (4-6) into (4-7)

$$F(u,v)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}}\cdot\cos\theta_1\cos\theta_2\cdot e^{-2j\pi(ux+vy)}dxdy$$
$$-\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}}\cdot\sin\theta_1\sin\theta_2\cdot e^{-2j\pi(ux+vy)}dxdy$$

where $\cos(\theta)=\frac{1}{2}(e^{j\theta}+e^{-j\theta})$, $\sin(\theta)=\frac{1}{2j}(e^{j\theta}-e^{-j\theta})$, thus

$$F(u,v)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}}\cdot\frac{1}{2}[e^{j\theta_1}+e^{-j\theta_1}]\cdot\frac{1}{2}[e^{j\theta_2}+e^{-j\theta_2}]\cdot e^{-2j\pi(ux+vy)}dxdy$$
$$-\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}}\cdot\frac{1}{2j}[e^{j\theta_1}-e^{-j\theta_1}]\cdot\frac{1}{2j}[e^{j\theta_2}-e^{-j\theta_2}]\cdot e^{-2j\pi(ux+vy)}dxdy$$

$$=\frac{1}{4}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}}\cdot[e^{j(\theta_1+\theta_2)}+e^{j(-\theta_1+\theta_2)}+e^{j(\theta_1-\theta_2)}+e^{j(-\theta_1-\theta_2)}]\cdot e^{-2j\pi(ux+vy)}dxdy$$
$$-(-\frac{1}{4})\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-\frac{1}{2}\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\}}\cdot[e^{j(\theta_1+\theta_2)}-e^{j(-\theta_1+\theta_2)}-e^{j(\theta_1-\theta_2)}+e^{j(-\theta_1-\theta_2)}]\cdot e^{-2j\pi(ux+vy)}dxdy$$

$$=\frac{1}{2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-\frac{1}{2}\{\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\}}\cdot[e^{j(\theta_1+\theta_2)}+e^{j(-\theta_1-\theta_2)}]\cdot e^{-2j\pi(ux+vy)}dxdy$$

$$= \frac{1}{2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\frac{1}{2}\{\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\}} \cdot e^{j(\theta_1+\theta_2)} \cdot e^{-j2\pi(ux+vy)} dxdy$$

$$+ \frac{1}{2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\frac{1}{2}\{\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\}} \cdot e^{j(-\theta_1-\theta_2)} \cdot e^{-2j\pi(ux+vy)} dxdy$$

Solving each part of equation (4-9) thus,

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\frac{1}{2}\{\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\}} \cdot e^{j(\theta_1+\theta_2)} \cdot e^{-j2\pi(ux+vy)} dxdy$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\frac{x^2}{2\sigma_x^2}} \cdot e^{2j\pi fx\cos\theta} \cdot e^{-2j\pi ux} \cdot e^{-\frac{y^2}{2\sigma_y^2}} \cdot e^{2j\pi fy\sin\theta} \cdot e^{-2j\pi vy} dxdy$$

$$= \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma_x^2}[x^2+j(4\pi\sigma_x^2 ux-4\pi\sigma_x^2 fx\cos\theta)]} dx \cdot \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma_y^2}[y^2+j(4\pi\sigma_y^2 vy-4\pi\sigma_y^2 fy\sin\theta)]} dy$$

$$= \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma_x^2}[x+2j\pi\sigma_x^2(u-f\cos\theta)]^2} dx \cdot e^{-2\pi^2\sigma_x^2(u-f\cos\theta)^2}$$

$$\cdot \int_{-\infty}^{\infty} e^{-\frac{1}{2\sigma_y^2}[y+2j\pi\sigma_y^2(v-f\sin\theta)]^2} dy \cdot e^{-2\pi^2\sigma_y^2(v-f\sin\theta)^2}$$

$$= \sqrt{2}\sigma_x \cdot \int_{-\infty}^{\infty} e^{-t_1^2} dt_1 \cdot e^{-2\pi^2\sigma_x^2(u-f\cos\theta)^2} \cdot \sqrt{2}\sigma_y \cdot \int_{-\infty}^{\infty} e^{-t_2^2} dt_2 \cdot e^{-2\pi^2\sigma_y^2(v-f\sin\theta)^2}$$

$$\text{where } t_1 = \frac{1}{\sqrt{2}\sigma_x}[x+2j\pi\sigma_x^2(u-f\cos\theta)] \quad \text{and} \quad t_2 = \frac{1}{\sqrt{2}\sigma_y}[y+2j\pi\sigma_y^2(v-f\sin\theta)]$$

$$= \sqrt{2}\sigma_x \cdot \sqrt{\pi} \cdot e^{-2\pi^2\sigma_x^2(u-f\cos\theta)^2} \cdot \sqrt{2}\sigma_y \cdot \sqrt{\pi} \cdot e^{-2\pi^2\sigma_y^2(v-f\sin\theta)^2}$$

$$= 2\pi\sigma_x\sigma_y \cdot e^{-\frac{1}{2}[\frac{(u-f\cos\theta)^2}{\sigma_u^2}+\frac{(v-f\sin\theta)^2}{\sigma_v^2}]}$$

where $\sigma_u = \frac{1}{2\pi\sigma_x}$ and $\sigma_v = \frac{1}{2\pi\sigma_y}$.

Similarly,

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-\frac{1}{2}\{\frac{x^2}{\sigma_x^2}+\frac{y^2}{\sigma_y^2}\}} \cdot e^{j(-\theta_1-\theta_2)} \cdot e^{-2j\pi(ux+vy)} dxdy = 2\pi\sigma_x\sigma_y \cdot e^{-\frac{1}{2}[\frac{(u+f\cos\theta)^2}{\sigma_u^2}+\frac{(v+f\sin\theta)^2}{\sigma_v^2}]}$$

The Fourier Transform of equation (4-9) is:

$$F(u,v) = \frac{1}{2}[2\pi\sigma_x\sigma_y \cdot e^{-\frac{1}{2}[\frac{(u-f\cos\theta)^2}{\sigma_u^2}+\frac{(v-f\sin\theta)^2}{\sigma_v^2}]} + 2\pi\sigma_x\sigma_y \cdot e^{-\frac{1}{2}[\frac{(u+f\cos\theta)^2}{\sigma_u^2}+\frac{(v+f\sin\theta)^2}{\sigma_v^2}]}]$$

$$= A \cdot \left(e^{-\frac{1}{2}[\frac{(u-f\cos\theta)^2}{\sigma_u^2}+\frac{(v-f\sin\theta)^2}{\sigma_v^2}]} + e^{-\frac{1}{2}[\frac{(u+f\cos\theta)^2}{\sigma_u^2}+\frac{(v+f\sin\theta)^2}{\sigma_v^2}]} \right) \qquad 4\text{-}10$$

where $A = \pi\sigma_x\sigma_y, \sigma_u = \frac{1}{2\pi\sigma_x}, \sigma_v = \frac{1}{2\pi\sigma_y}$.

Finally the power spectrum result is

$$PS = \left| A \cdot \left(e^{-\frac{1}{2}[\frac{(u-f\cos\theta)^2}{\sigma_u^2}+\frac{(v-f\sin\theta)^2}{\sigma_v^2}]} + e^{-\frac{1}{2}[\frac{(u+f\cos\theta)^2}{\sigma_u^2}+\frac{(v+f\sin\theta)^2}{\sigma_V^2}]} \right) \right|^2 \qquad 4\text{-}11$$

4.5 Experimental analysis

The experimental study was split into two classes of tests: 1) Objective (approaches based), e.g. power spectrum approach (PS), Directional contrast approach (DC), Gabor feature approach (GF), Neural network approach (NN) and Gabor spectrum method (GSM). 2) Subjective (human observers based) which taken as quality assessment reference standard. Correlation, scatting and reliability results will be the performance evaluation of all approaches. Matlab was chosen as the implementation platform for all approaches except neural network method of NFIQ, where NFIQ was introduced as an independent quality estimator that is intensely trained to forecast matching performance [35] and is publicly available as a package of NIST Fingerprint Image Quality, NIST Fingerprint Image Software 2, [37, 100]. The approaches were tested on 135 different combinations of fingerprint images, i.e. 90 good images, 45 faulty images, TIMA database [22]. Images were cropped from centre into 256x256 sizes, JPG format and converted to WSQ format for NFIQ test.

4.5.1 Subjective Test

Subjective evaluation is still a method commonly used in measuring image quality. It is used to quantify image changing, degrading and quality is by asking specialist viewers to subjectively evaluate image quality. A set of fingerprint images [TIMA database] were viewed by 15 human observers working in image processing and biometrics fields using web based image quality survey (IQS) Figure (4-13). TIMA database was used because it contained a different quality degree of fingerprint images, e.g. bad, good, cut, no contact.

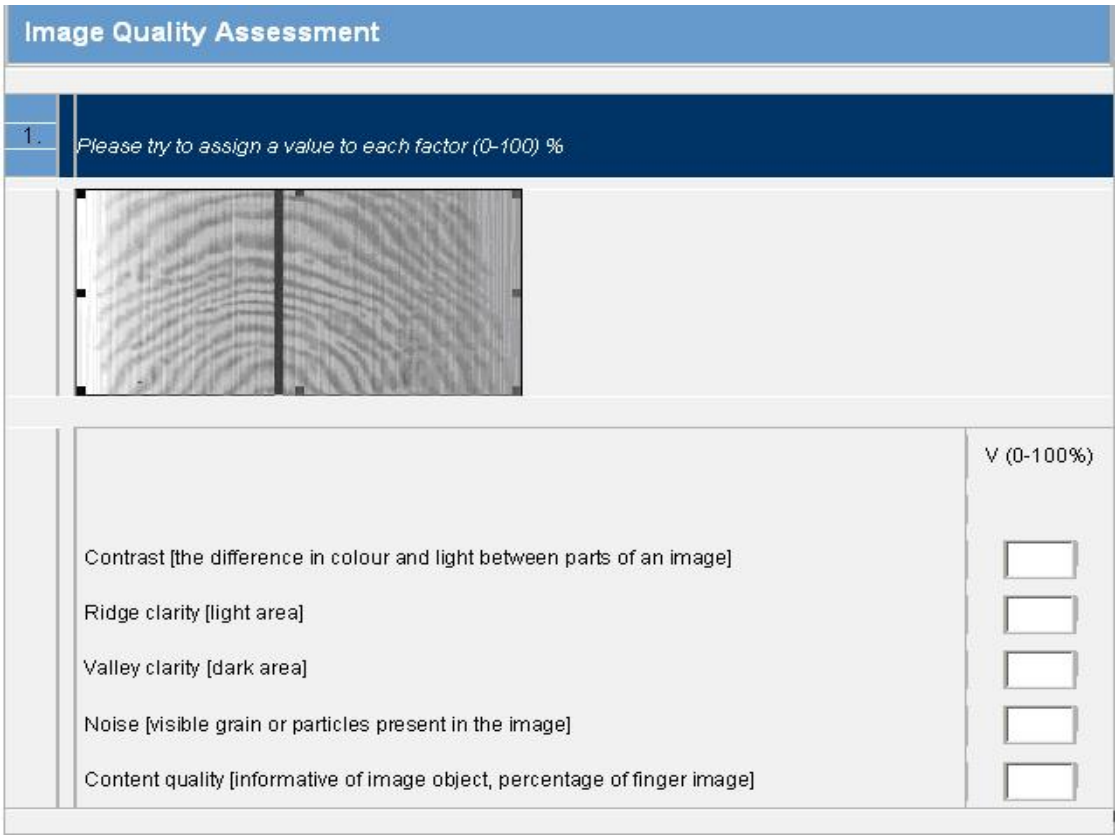


Figure 4-13 Image quality survey

IQS was subjectively rated by human observer participants. IQS was done based on visual assessment (subjective measurement), it was conducted on different image quality, and validity taken from previous database, the validity factors were taken as image contrast, ridge clarity, valley clarity, image noise, and image content quality [informative of image object, percentage of finger image], the validity factors are selected between [0 and 100], 0 for none factor satisfaction, 100 for excellent presence of factor. The scores of each image were averaged to a final validity and quality MOS Equation (4-12). Table (4-1) shows a partial data of studied database within investigated estimator's i.e. PS, DC, GF, NN, and GSM with reference to MOS.

$$MOS = \frac{1}{N}\sum_{i=1}^{N} score_i \qquad 4\text{-}12$$

where N=15

Image	MOS	PS	DC	GF	NN	GSM
4_nik_index1.tif	0.3	0.34858	0.34813	0.3561	0.28	0.2247
7_nik_index12.tif	0.6	1.0271	0.37602	0.55714	0.55	0.895
no_contact_pb3.tif	0.124	0.42663	0.34275	0.38329	0.33	0.2247
4_nik_index3.tif	0.24	0.34536	0.34203	0.43132	0.36	0.2247
7_nik_index3.tif	0.68	0.80369	0.37297	0.5087	0.42	0.717
no_contact_pb5.tif	0.18	0.237	0.10766	0.22726	0.33	0.2247
4_nik_majeur1.tif	0.35	0.29413	0.33335	0.49927	0.43	0.2247
7_nik_majeur11.tif	0.59	0.6765	0.3697	0.72013	0.49	0.654
shift5.tif	0.27	0.37306	0.3716	0.22877	0.4	0.2247
1_ben_index2.tif	0.63	1.1697	0.3973	0.78126	0.51	0.895
4_nik_majeur3.tif	0.27	0.3264	0.31765	0.4949	0.41	0.2247
7_nik_pouce4.tif	0.51	0.8582	0.38976	0.7603	0.39	0.714
shift9.tif	0.54	0.72729	0.28156	0.90739	0.51	0.895
2_ben_for_ben.tif	0.5	0.2963	0.29555	0.44655	0.42	0.2247
4_nik_majeur4.tif	0.34	0.27675	0.28525	0.56322	0.39	0.2247
Strange13.tif	0.15	0.43839	0.40161	0.46243	0.3	0.2247
3_ben_index1.tif	0.36	0.39664	0.38335	0.37187	0.32	0.2247
4_nik_majeur5.tif	0.27	0.33683	0.33639	0.38928	0.38	0.2247
cut1.tif	0.38	0.34014	0.35812	0.50606	0.32	0.2247
Strange14.tif	0.14	0.25069	0.24745	0.59567	0.48	0.2247
3_ben_majeur6.tif	0.52	0.35877	0.38989	0.67835	0.42	0.2247
4_nik_pouce1.tif	0.27	0.29945	0.33075	0.54178	0.32	0.2247
cut3.tif	0.17	0.45529	0.41772	0.30789	0.27	0.2247
Strange6.tif	0.2	0.39757	0.39373	0.54719	0.4	0.2247
3_gui_index1.tif	0.3	0.39965	0.37967	0.29201	0.36	0.2247
4_nik_pouce3.tif	0.25	0.33416	0.33839	0.36871	0.27	0.2247
cut6.tif	0.16	1.0498	0.38311	0.39633	0.33	0.895
3_mar_index3.tif	0.31	0.29204	0.30181	0.57446	0.49	0.2247
4_nik_pouce4.tif	0.3	0.28912	0.28912	0.58932	0.38	0.2247
3_nik_index1.tif	0.35	0.31636	0.31692	0.38066	0.38	0.2247
7_nik_auricu1.tif	0.63	0.80909	0.34182	0.98746	0.42	0.895
3_nik_pouce_1.tif	0.31	0.37077	0.35334	0.38553	0.36	0.2247
7_nik_index1.tif	0.68	0.83553	0.37605	0.61696	0.4	0.667
nik_annu_g_9.tif	0.51	0.77328	0.39711	0.50023	0.42	0.614

Table 4-1 Part of "MOS-IQS, PS, DC, GF and NN- NFIQ quality results",

4.5.2 Accuracy and Correlation Analysis

Correlation coefficient indicates the strength and direction of a linear relationship between objectives estimators and subjective MOS, how strong this relationship, and whether the correlation is positive or negative. For image quality estimators the Pearson correlation coefficient is chosen, because it is the best estimate of the correlation of two series. Correlation coefficient is used after drawing a scatter plot of the data that suggests a linear relationship. Scatter plots are illustrated in Figures (4(14-18)), and the correlation coefficients in Table (4-2). Each point in scatter graphs represents one test image, with its vertical and horizontal coordinates representing its subjective MOS and the model prediction, i.e. quality estimators, respectively. It is clear that, the GSM results exhibit better consistency with the subjective data than the results of the other estimators. Table (4-2) shows the numerical evaluation results, where GSM is the more accurate and highest correlated order to the MOS. The GSM used benefit of spectrum analysis on Gabor feature detection to enhance and construct image blind quality assessment, and to be used as a function of monitoring and controlling of image enrolment for the sake of increasing the efficiency of whole dependent system, i.e. verification, identification and crypto key generation systems. The prediction monotonicity can be measured with the Spearman rank order correlation coefficient (SROCC) [101]. This measures correlation between the objective measure's rank orders of the subjective scores (MOS). The SROCC is described by the following equation:

$$\rho = 1 - 6\left(\sum D^2\right) \Big/ N\left(N^2 - 1\right) \qquad 4\text{-}13$$

where D refers to the difference between subjects ranks on the two variables, and N is the number of data points. The results of estimators ranking and monotonicity is shown in Table (4-3), where the greatest monotonicity and accuracy is still found using GSM.

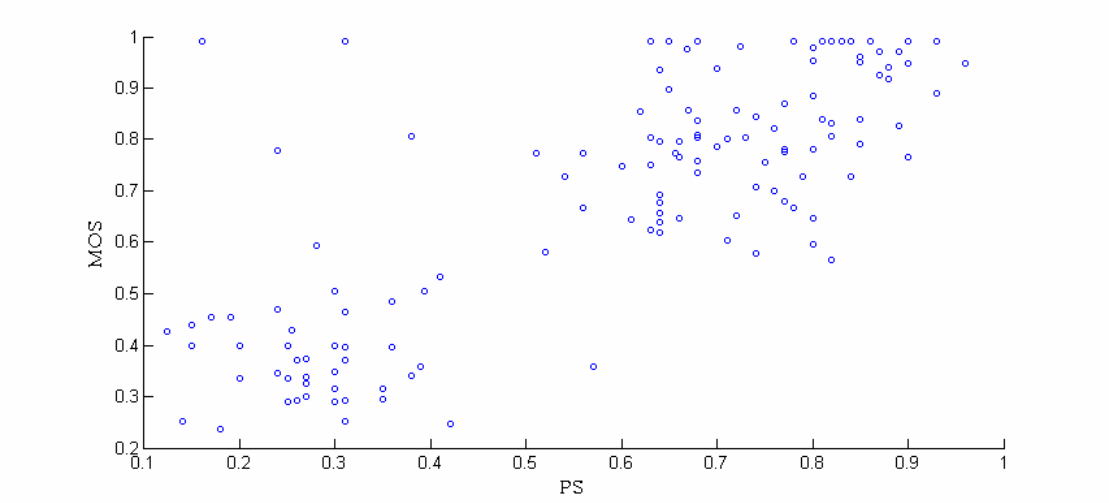


Figure 4-14: Scatter plot of PS vs. MOS with Pearson correlation: 0.7822

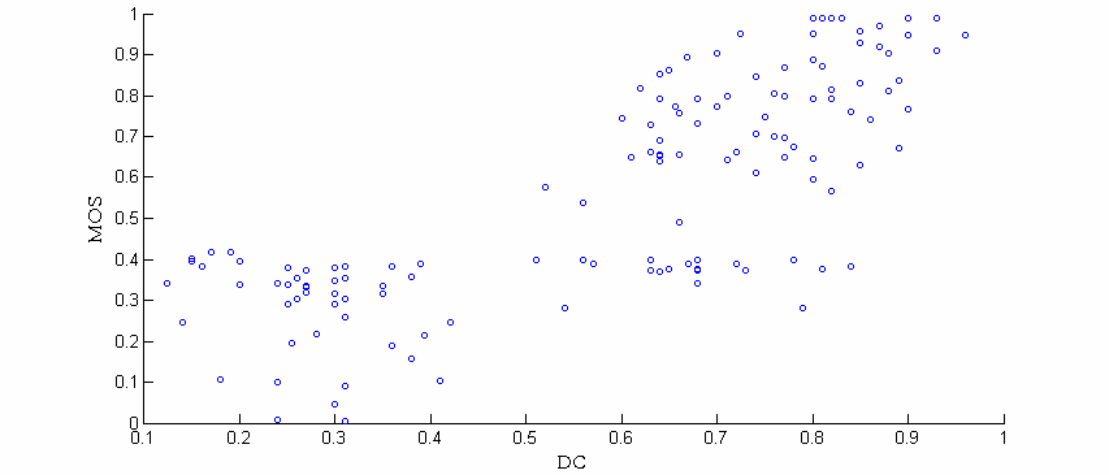


Figure 4-15: Scatter plot of DC vs. MOS with Pearson correlation: 0.7641

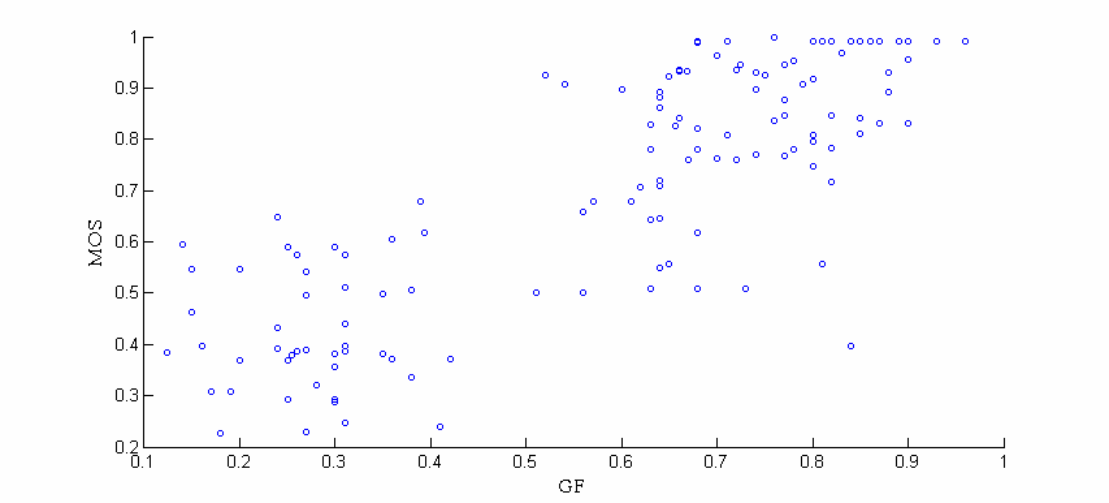


Figure 4-16: Scatter plot of GF vs. MOS with Pearson correlation: 0.8231

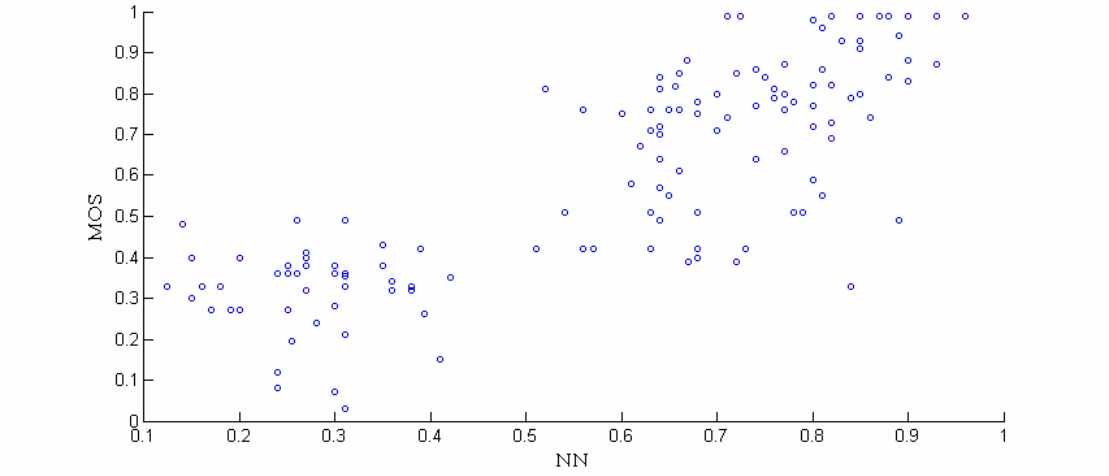


Figure 4-17: Scatter plot of NN vs. MOS with Pearson correlation: 0.8009

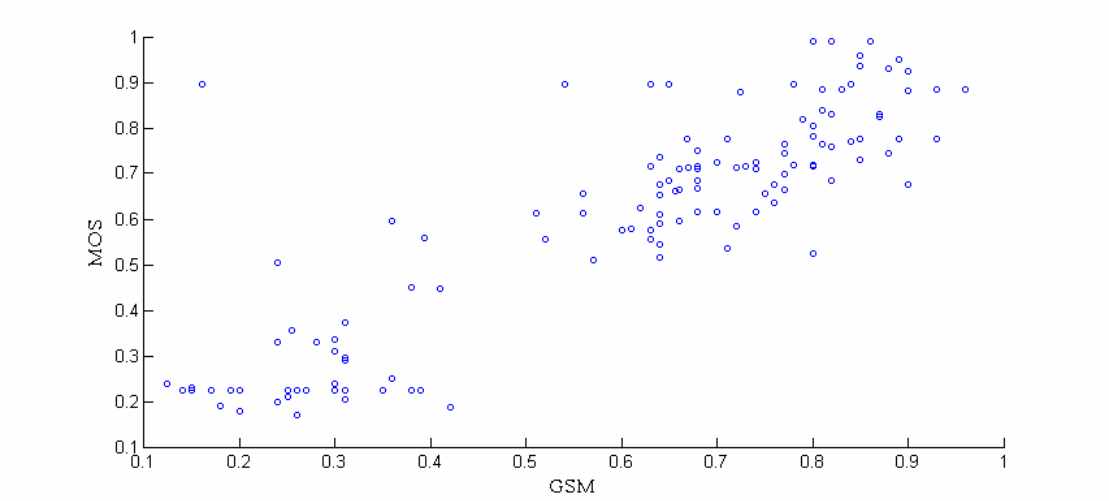


Figure 4-18: Scatter plot of GSM vs. MOS with Pearson correlation: 0.8811

	MOS	PS	DC	GF	NN	GSM
MOS	1	0.7822	0.7641	0.8231	0.8009	0.8811
PS	0.7822	1				
DC	0.7641		1			
GF	0.8231			1		
NN	0.8009				1	
GSM	0.8811					1

Table 4-2: Correlation relation results of image quality measures

	MOS	PS	DC	GF	NN	GSM
MOS	1	0.7146	0.7336	0.7865	0.7927	0.8326
PS	0.7146	1				
DC	0.7336		1			
GF	0.7865			1		
NN	0.7927				1	
GSM	0.8326					1

Table 4-3 Correlation rank order of image quality estimators

4.5.3 Reliability Analysis

In this test, approaches will be investigated by reliabilities decisions of False and True outcome rates. The test idea based on calculating the ratio of correctness matches to the total samples as True Rate (TR), while the False Rate (FR) was taken as results of false matches to the total samples. This test indicates the trustiness' automation usage of the

investigated estimator. Result of test shows that GSM is high reliable among evaluated estimators, Table (4-4), Figure (4-19).

	PS	DC	GF	NN	GSM
FR	0.04	0.1	0.06	0.05	0.02
TR	0.96	0.9	0.94	0.95	0.98

Table 4-4 FR versus TR results

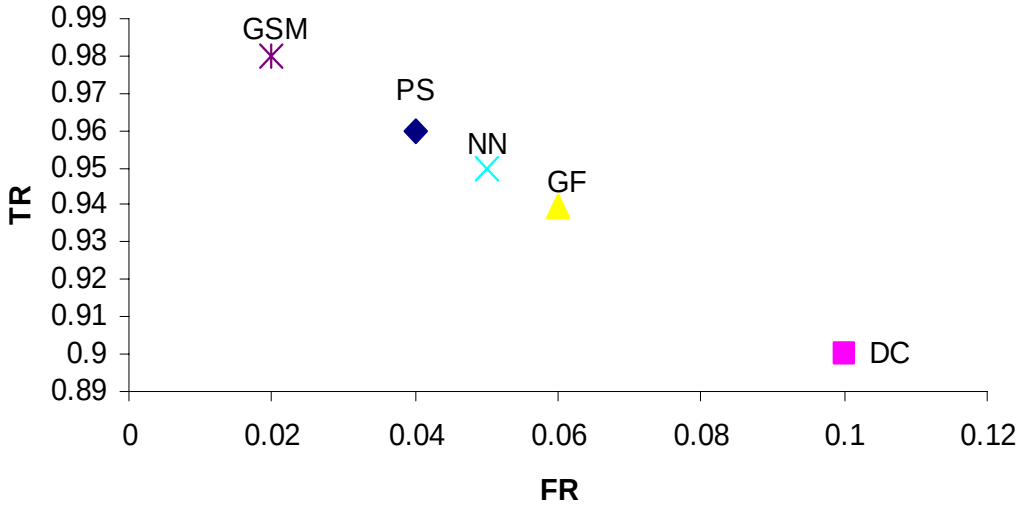


Figure 4-19: False rate (FR) versus True rate TR of image quality assessment approaches

4.5.4 Verification Performance

According to the quality methods the verification performance was examined using VeriFinger Software [102]. The verification system used the same algorithms (pre-processing, frequency estimation, enhancement and matching) with the exception of the quality estimation algorithm. The thresholds for each quality estimation algorithm were chosen at the point of minimum quality decision error. GSM was compared with other

conventional methods using TIMA DB. Figure (4-20) shows the matching results with the Receiver Operating Curves (ROC) in order to compare the proposed algorithm with existing algorithms. From this experiment, it is observed that performance of the fingerprint verification system was significantly improved when GSM quality estimation algorithm was applied to the input fingerprint images.

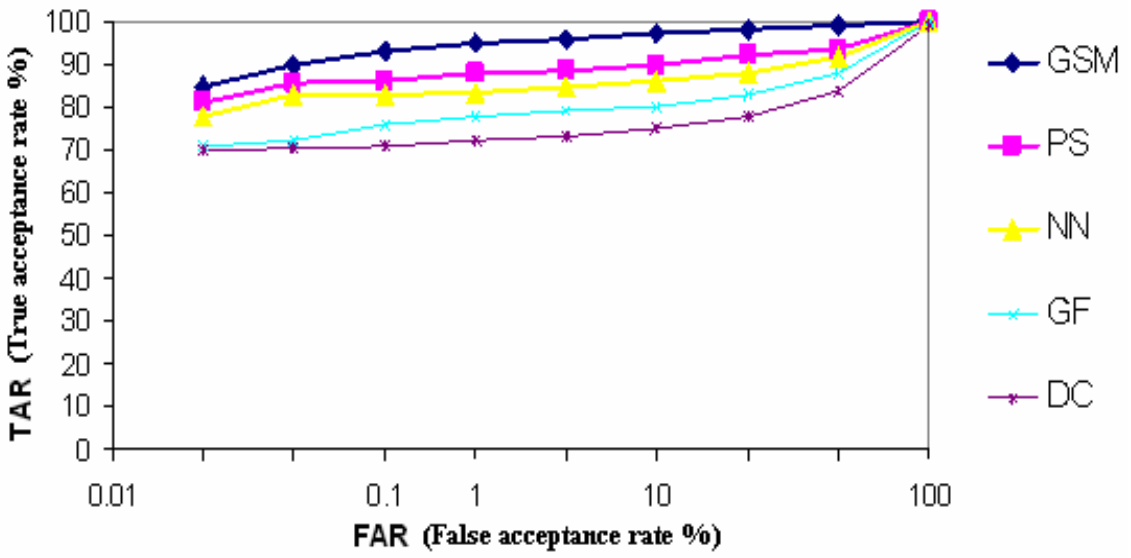


Figure 4-20 Receiver Operating Curves TIMA Database

4.6 Summary

In this chapter, a heuristic non reference image quality assessment and validity check approach based on Gabor feature spectrum analysis is presented. Different image quality approaches were evaluated for the sake of quality assessment competition, the proposed approach competes well with the other investigated methods. It was behaving closest to human opinion on fingerprint validity and quality analysis, which comes out as excellent in comparison to studied approaches. Proposed approach can effectively guide the template selection at the enrollment stage and fingerprint image quality classification for automatic parameter selection in fingerprint image pre-processing.

Chapter 5 Fingerprint Crypto Key Structure

5.1 Introduction

With the rapid diffusion of information technology (IT) and its outputs, biometrics-based security systems are widely used in access control to computing resources, bank accounts in ATM systems, computer security, and user validation in e-business[11]. Biometric techniques as a core of biometric security systems have much superiority compared to traditional methods (token or knowledge based schemes) such as increasing user convenience and robustness against impostor users, but they are vulnerable to attacks from a template production to the storage database through transmission media. Thus, the possibility that a biometric database is compromised is one of the main concerns in implementing secure biometric systems, protecting biometric template during its journey from enrolment to the matching stages. It is difficult to control and trace hacking and cracking bio systems by unauthorized people. Cryptographic techniques are being used for information secrecy and authentication insurance in computer based security systems [103]. Many cryptographic algorithms are available for securing information. For all traditional algorithms the security is dependent on the secrecy of the secret or private key when a user deploys a symmetric or a public key system, respectively. The user chooses an easily remembered password that is used to encrypt the cryptographic key and this key is then stored in a database. In order to retrieve the key back, the user enters the password which will then be used to decrypt the key. In such systems, security of the cryptographic key is weak due to practical problems of remembering various pass-codes or writing them down to avoid data loss. Additionally, since the password is not directly tied to a user, the system is unable to differentiate between the legitimate user and the attacker. The limitations of password systems can be alleviated by stronger user tied password such as biometrics. Bio-Crypt technology is a result of merging two important aspects of

digital security environment, biometrics and cryptography. There are various methods that can be deployed to secure a key with a biometric. First one involves remote template matching and key storage, i.e. key release. In this method, the 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 [12, 15]. Second method hides the cryptographic key within the enrolment template itself via a secret bit-replacement algorithm, i.e. key binding. When the user is successfully authenticated, this algorithm extracts the key bits from the appropriate locations and releases the key. The drawback of this scheme is that the key will be retrieved from the same location in a template each time a different user is authenticated [12, 15]. Using data derived directly from a biometric image is another method. In this manner biometric templates are used as a cryptographic key. But sensitivities due to environmental and physiological factors and compromising of the cryptographic keys stand as a big obstacle [13, 39, 104]. Due to the biometric variability, we will study the possibility of consistently extract and generate a relatively small number of bits from biometric template to serve as a key or to bind a secret key within template itself. In this chapter, we will study a biometric crypto key structure, its vulnerabilities and problematic of implementation possibilities scenarios.

5.2 Biometric Security Construction

The biometric security system consists of a general biometric system (based on fingerprint in our case) and a general cryptographic system Figure (5-1). An art of pipe through both systems has been proposed as connection step. This connecting step corresponds to the key generation from the fingerprint source information, i.e. extracted minutiae points. The biometric system acquires and processes fingerprint images. Then a key is generated in an intermediate step and such key is delivered to a cryptographic module. Alternative scenario of key generation is a binding scenario, where a secret key is bound with biometric extracted information. Any biometric attributes can be used as the input biometric information. The only requirement is the entropy power in the selected biometric attribute. If there is no information, it is impossible to generate strong cryptographic keys, even if the process of key generation is realizable. The strength of fingerprint information is quite enough to generate the key which is suitable for

symmetrical cryptography, but the stability and uniqueness of the key is the question of research.

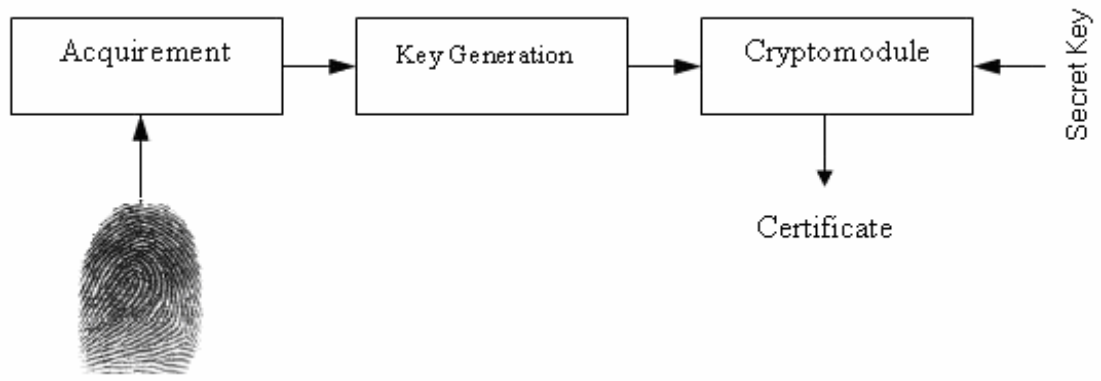


Figure 5-1 Generic Biometric Security System structure

5.2.1Fingerprint Acquirement

The acquirement stage is based on scanning, capturing and features registration processing to detect a high resolution image with enough gray levels, in most cases 256 levels (8 bits/pixel). Further image enhancement process or direct enrolment within validity and quality assessment (see Chapters 2 and 3) could affect the performance evaluation of built based system. Therefore, we consider the following steps: image enhancement, thresholding, ridge thinning and minutiae extraction Figure (5-2), to get the fingerprint features, the final results is a set of minutiae points with their characteristic information, i.e. position, gradient and type [77, 105, 106].

The most commonly employed method of minutiae extraction is the crossing number (CN). The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3 x 3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhoods. Then according to the computed CN, the ridge pixel can be classified as a ridge ending, bifurcation or non minutia point. If CN value equal to one then that pixel is classified as ridge ending point, and if it is equal to three then it is classified as bifurcation. Otherwise it is considered as non minutiae point. In the crossing number conditions and their corresponding properties are shown in Table (5- 1), and Figure (5-3).

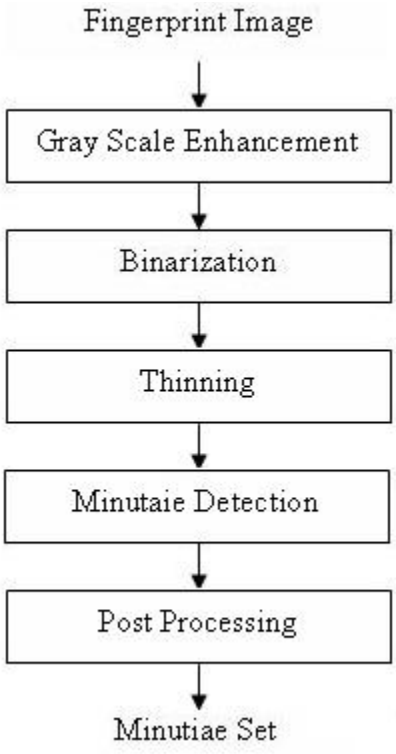


Figure 5-2 Block diagram for minutiae based feature extraction

The CN for a ridge pixel *P* is given by:

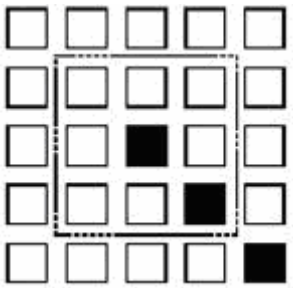
$$CN = 0.5\sum_{i=1}^{8} | P_i - P_{i+1} |, \quad P_9 = P_1 \qquad 5\text{-}1$$

where P_i is the pixel value in the neighbourhood of *P*. The eight neighbouring pixels of the pixel *P* are scanned in an anti-clockwise direction.

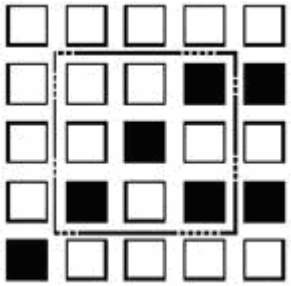
This means that a pixel is classified according to the value of projected *3x3* window. If it has only one neighbouring ridge pixel so it is classified as ridge ending, and classified as bifurcation if it has three separated pixels that are only connected to the centre pixel of the projected window.

CN	**Property**
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Table 5-1 Properties of the Crossing Number.



(a)



(b)

P4	P3	P2
P5	P	P1
P6	P7	P8

(c)

Figure 5-3: (a) Ridge ending CN=1, (b) Bifurcation CN=3 and (c) The eight connected neighbourhood of the pixel P in the 3x3 projected window.

For quality assurance of minutiae points we suggest to perform this process approximately five times. The quality of this set means that the minutiae included in this set will be found next time again with a very high probability and the appropriate extracted minutiae points are stored. Let us call the minutiae μ_i^j , where i is the descriptor of the fingerprint image $(i = 1,...,5)$, and j is the number of minutiae n_i found in the appropriate fingerprint $(j = 1,...,n_i)$. Each minutia (only ridge ending and ridge bifurcation are considered) has three items (position, gradient, and type) Equation (5-2).

$$\mu_i^j = \left(x_i^j, y_i^j, \phi_i^j, t_i^j\right) \qquad 5\text{-}2$$

where x_i^j is the x-coordinate position, y_i^j is the y-coordinate position, ϕ_i^j is the gradient and t_i^j is the type of a particular minutia.

Another important factor is the position of the core point or reference point of the fingerprint. The core point position should be determined before assembling an appropriate set of minutiae. The centre point of the fingerprint must not be affected by any translation or rotation of the fingerprint image. Fingerprint centre is computed based on minutiae gravity centre or ridge count or orientation field. Minutiae gravity center computation is based on the position of all the minutiae μ_i^j , more precisely on their x and y coordinates. The computational procedure is based on the definition of the Euclidean distance of a straight line between two points [107] :

$$d = \sqrt{|x_1 - x_2|^2 + |y_1 - y_2|^2} \qquad 5\text{-}3$$

The Euclidean distance expression is extended for the minutiae set μ_i^j calculation, equation (5-3) as is shown in equation (5-4).

$$d_i^j = \frac{1}{n_i - 1} \sum \sqrt{\left|x_i^j - x_i^k\right|^2 + \left|y_i^j - y_i^k\right|^2} \qquad 5\text{-}4$$

The minimum distance value of all minutiae set in each fingerprint can be computed as:

$$\delta_i = \min\left(d_i^1, ..., d_i^{n1}\right) \qquad 5\text{-}5$$

The minutia with the minimal distance δ_i has the same coordinates as the centre of the fingerprint with coordinates $[C_X, C_Y]$. The centre could vary, if the image acquisition device provides images which contain a lot of information noise in the image data. These problems can be solved by eliminating the image if it's quality under validity and quality threshold. If the image within threshold but there is an improper minutia then improper minutiae can be deleted by removing the false minutiae post processing step. The second method of centre determination is based on ridge count, Figure (5-4). The fingerprint ridges are represented as some art of the sine wave in the figure cross section, and they are shown in the figure as homocentric circles with the origin in the real centre of the fingerprint. The number of through passes in the horizontal and vertical direction could

be computed, where the number of circle through passes in the centre of all circles is greater than in outlying region. These through passes define the ridge count for each column or row. The following expression can be used for the computation of vertical ridge count:

$$RC_{V,All} = \{RC_i | i = 0...Height\} \quad 5\text{-}6$$

where Height is the number of pixels in the vertical direction and RC_i is the ridge count for the corresponding row in the image. For the selection of the vertical centre, the value of RC_V needs to be computed:

$$RC_V = avg(\max(RC_{V,all})) \quad 5\text{-}7$$

which represents the coordinate position C_Y and is computed as an average of the region with maximal value of the ridge count from the whole set $RC_{V,All}$. Similar equations can be used for the horizontal ridge count:

$$RC_{H,All} = \{RC_i | i = 0...Width\} \quad 5\text{-}8$$

$$RC_H = avg(\max(RC_{H,all})) \quad 5\text{-}9$$

The value RC_H represents the centre position C_X.

Figure 5-4 Fingerprint ridge counts

Another method of computing the centre point is based on Orientation Field (OF), where fingerprint can be viewed as an oriented texture image [108]. The OF is used to compute the optimal dominant ridge direction in each $w \times w$ window or block. OF has been proposed in several literatures [2, 108, 109]. The main steps in determining the orientation image using the algorithm based on the least mean square iteration method are as follows [105]:

Divide the input fingerprint image into blocks of size $w \times w$. For 500 *dpi* images, the initial recommended value of w is 16.

Compute the gradients $\partial_x(i, j)$ and $\partial_y(i, j)$ at each pixel (i, j). Depending on computational requirements, the gradient operator may vary from the simple *Sobel* operator to the more complex *Marr-Hildreth* operator.

Estimate the local orientation of each block centered at (i, j) using the following equations [77, 105]:

$$v_x(i,j) = \sum_{u=1-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v) \qquad 5\text{-}10$$

$$v_y(i,j) = \sum_{u=1-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \partial_x^2(u,v) - \partial_y^2(u,v) \qquad 5\text{-}11$$

$$\theta(i,j) = \frac{1}{2}\cot\left(\frac{v_y(i,j)}{v_x(i,j)}\right) \qquad 5\text{-}12$$

where $\theta(i,j)$ is the least square estimate of the local ridge orientation at the block centered at pixel (i,j). Mathematically, it represents the direction that is orthogonal to the dominant direction of the Fourier spectrum of the $w \times w$ window.

Due to noise, corrupted ridge and valley structures, unclear minutiae, etc., in the input image, the estimated local ridge orientation $\theta(\mathrm{i},\mathrm{j})$, may not always be correct. Since local ridge orientation varies slowly in a local neighbourhood where no singular points appear, a low-pass filter can be used to modify the incorrect local ridge orientation. In order to perform the low-pass filtering, the orientation image needs to be converted into a *continuous vector field*, which is defined as follows [77]:

$$\Phi'_x(i,j) = \sum_{u=-\frac{w_\Phi}{2}}^{2} \sum_{v=-\frac{w_\Phi}{2}}^{2} h(u,v)\Phi_x(i-uw, j-vw) \qquad 5\text{-}13$$

$$\Phi'_y(i,j) = \sum_{u=-\frac{w_\Phi}{2}}^{2} \sum_{v=-\frac{w_\Phi}{2}}^{2} h(u,v)\Phi_y(i-uw, j-vw) \qquad 5\text{-}14$$

where h is a 2-dimensional low-pass filter with a unit integral and

$w_\Phi \times w_\Phi$ specifies the size of the filter.

Compute the local ridge orientation at (i, j) using

$$O(i,j) = \frac{1}{2}\cot\left(\frac{\Phi'_y(i,j)}{\Phi'_x(i,j)}\right) \qquad 5\text{-}15$$

Compute the consistency level of the orientation field in the local neighborhood of block (i, j) by the following formula:

$$C(i,j) = \frac{1}{n}\sqrt{\sum_{(i',j')\in D}\left|O(i',j') - O(i,j)\right|^2} \qquad 5\text{-}16$$

$$\left|O(i',j') - O(i,j)\right| = \begin{cases} d & \text{if} \quad d < 180^\circ \\ d - 180_\circ & \text{otherwise} \end{cases} \qquad 5\text{-}17$$

$$d = \left(O(i',j') - O(i,j) + 360^\circ \quad \text{mod} \quad 360^\circ\right) \qquad 5\text{-}18$$

where D represents a local neighbourhood around the block (i, j); n is the number of blocks within D; $O(i', j')$ and $O(i, j)$ are local ridge orientations for blocks (i', j') and (i, j) respectively.

If $C(i, j)$ is above a certain threshold T_c, then the local orientation in this block is re-estimated at a lower resolution level until $C(i, j)$ is below a certain threshold.

After the orientation field of an input fingerprint image is determined, Figure (5-5), an algorithm for the localization of the region of interest is applied, based on the local certainty level of the orientation field.

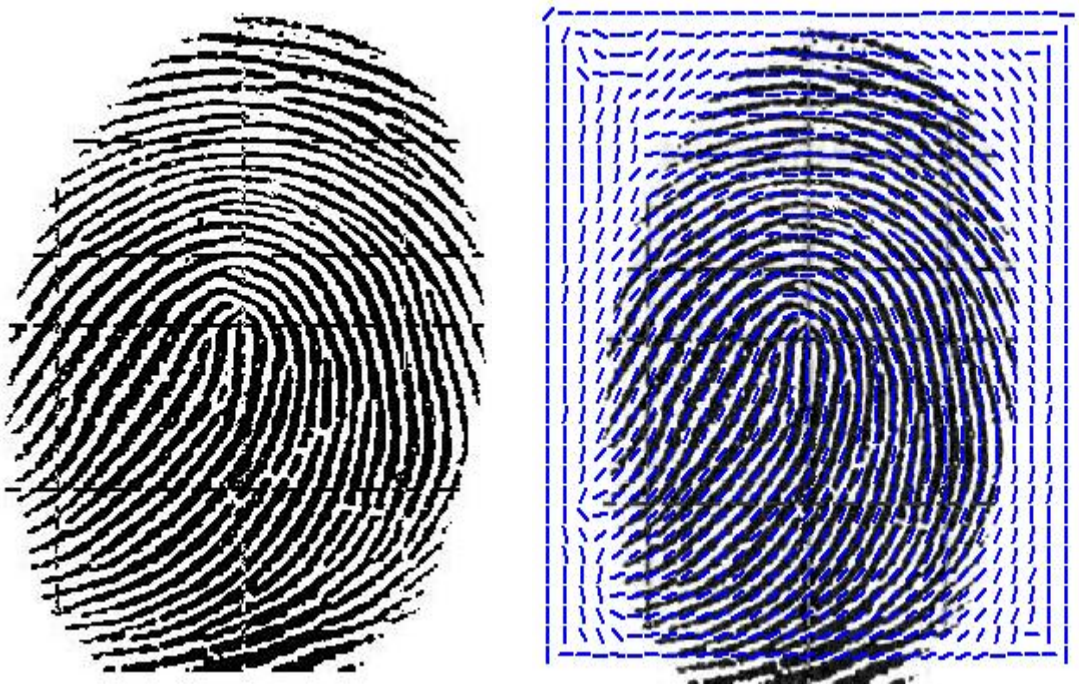


Figure 5-5 Original fingerprint image with its result of orientation field computation

The result is the located region of interest within the input image. The level of certainty of the orientation field in the block (i, j) is defined as follows:

$$\varepsilon(i,j) = \sqrt{\frac{1}{w \times w} \cdot \frac{\left(v_x(i,j)^2 + v_y(i,j)^2\right)}{v_c(i,j)^2}} \qquad 5\text{-}19$$

$$v_c(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} \partial_x^2(u,v) - \partial_y^2(u,v) \qquad 5\text{-}20$$

Based on orientation field calculation, the computational of the center consists of the following steps:

For the estimation of the centre of the fingerprint, some reduction of the number of directions needs to be done. Normally, 8 possible directions are used in each block $w \times w$ [109]. These directions are shown in Figure (5-6). The directions have the following angle values: $1 = 90^\circ$, $2 = 67.5^\circ$, $3 = 45^\circ$, $4 = 22.5^\circ$, $5 = 0^\circ$, $6 = 157.5^\circ$, $7 = 135^\circ$

and $8 = 112.5^\circ$. This number of directions is necessary for the classification. But for the fingerprint centre computation, the number of directions could be reduced. In our case, only 4 directions are sufficient, namely [1, 3, 5 and 7]. The direction 1 and 5 remain without change. The directions 2 and 4 are assigned to the direction 3. The directions 6 and 8 are assigned to the direction 7. Now, each direction has the angle resolution of 45°. The orientation field with only 4 directions is called O_{4R} .

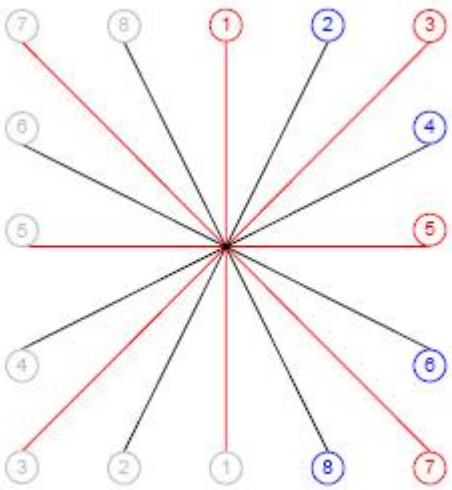


Figure 5-6 Direction of orientation field pixels

The fingerprint image needs to be divided into four uniform blocks Figure (5-7). These blocks can be considered as the particular blocks of the coordinate system, with the same centre in the middle of the fingerprint image. The origin of the image could be defined in the upper left corner, i.e. in the position $[0,0]$; and the end of the image could be in the lower right corner, i.e. in the position $[m,n]$. The procedure for gravity centre computation would be as follows:

$$C_{x(h)}^{(r_1+r_2)} = \max\left(\sum_{j=c}^{d} O_{4r}^{(h)}(i,j)\right), \quad i = a \ldots b \qquad 5\text{-}21$$

$$C_{y(h)}^{(r_1+r_2)} = \max\left(\sum_{j=a}^{b} O_{4r}^{(h)}(i,j)\right), \quad i = c \ldots d \qquad 5\text{-}22$$

where $C_{x(h)}^{(r_1+r_2)}$ is the x position and $C_{y(h)}^{(r_1+r_2)}$ is the y position of the orientation field direction h in the image blocks r_1 and r_2. The term $O_{4r}^{(h)}(i,j)$ denotes the value of the orientation field at the point (i,j). To determine the centre of the fingerprint, it is necessary to compute the centres of gravity for the dedicated orientation field directions.

Figure 5-7 Block division of the fingerprint image

The gravity centre points can be connected and expressed as continuous lines. The intersections of two lines with perpendicular directions are computed. These intersections create a short abscissa and the middle point of this abscissa denotes the centre point of the fingerprint. The final result of acquirement stage is a vector of extracting minutiae points and reference centre point. This vector will be used as input data for crypto key generation stage, to construct a direct minutiae point's key.

5.2.2 Crypto Key Generation

The minutiae from the acquirement stage are taken as inputs for the key generation stage where some mathematical operations are performed. These mathematical operations generate vectors from the set of minutiae points and these vectors can be considered as a

key in simple way. A reconstruction of minutiae points will be used to make these points more secure to generate a combined encapsulated cryptographic key based on reforming graph and adjacency matrix of extracted minutiae data.

5.3 Contour Graph Algorithm

Contour based construction graph algorithm (CBCG) is proposed for generating the encapsulation cryptography key and this is illustrated in Figure (5-8).

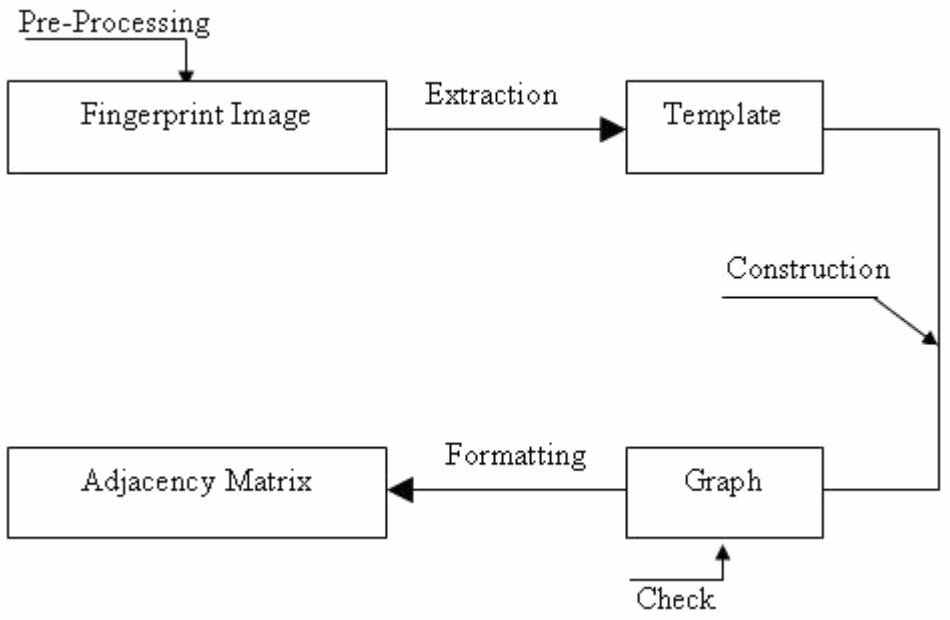


Figure 5-8 Contour Based Construction Graph algorithm block diagram.

The process of generating the key comprises all necessary functions to achieve no-repudiation, encryption, digital signing and strong authentication in an open network [11]. The major novelty of proposed CBCG consist of keeping minutiae points away from several attacks as a first security level of crypto-key generation life cycle. Extracted minutiae set μ, Equation (5-2) grouped into tracing neighboring contours, a neighboring relation defined by upper and lower level of contours. Using graph relation based on vertices and edges, i.e. minutiae set, ridge connection lines, respectively, the CBCG formulate a minutiae graph within specific conditions. A connection line must be only between two neighboring contours of fingerprint extracted information; all vertices must be visited within that contour. CBCG using the graph relation of vertices and edges is

constructed as shown in Figure (5-9). Key generation will be studied into two scenarios: First, including detected singular point (SP); Second scenario, SP will be excluded.

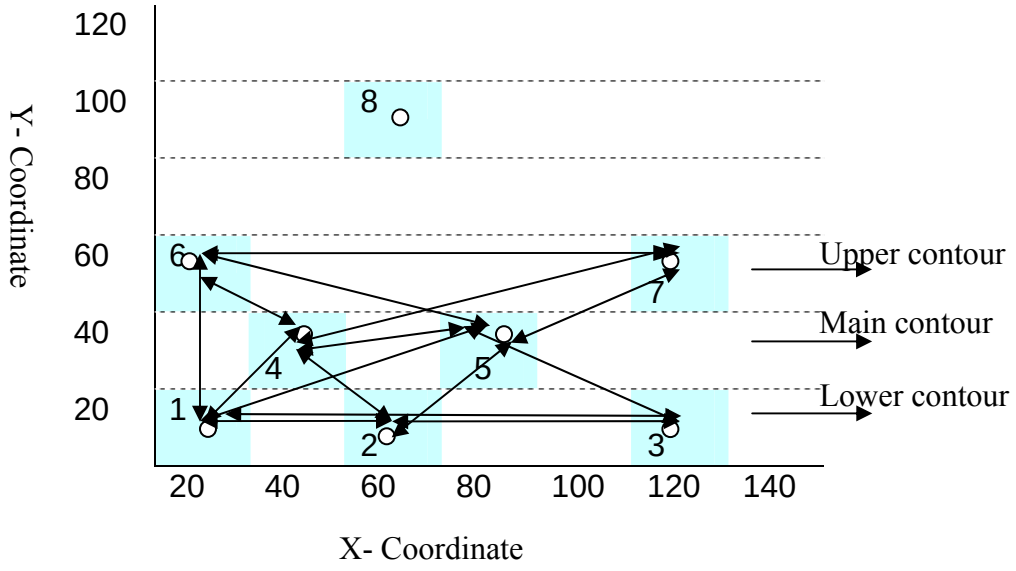


Figure 5-9 Constructed Interconnected Graph

In the experimental graphical phase, the minutiae points were extracted from cropped (200x200) image size. Extracted minutiae μ $(N \times M)$ pixels are grouped Figure (5-10) according to their coordinate (x, y) within contours.

$$CQ = \frac{\mu A}{CW} \qquad 5\text{-}23$$

where CQ is counters quantity, μA is minutiae points area, and CW is contour width.

```
Function [minutiae points] =grouping (minutiae points);
m = minutiae numbers size;
    For i=1:m
    Fix the points of X coordinate in width size
    End
End
```

Figure 5-10 Grouping Pseudo-Code

In the mathematical and key generation phase, adjacency matrix formatted within traced and grouped points (vertices) according to their connections order (edges) within the following rules:

Visiting all vertices on the same, upper, and lower contours $v_i \rightarrow v_{i+1}$.

Formulate the adjacency matrix of visited vertices, matrix $A\ (N \times N)$, in which $a_{ij} = 1$ if there exists a path from $v_i \rightarrow v_j$, $a_{ij} = 0$ otherwise. This is illustrated in Figure (5-11).

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Figure 5-11 Adjacency Matrix for the given graph in Figure (5-9)

The output matrix is taken as an input for crypto generator to be processed by defined mathematical operations. These mathematical operations generate vectors and sub vectors which will be dependent on cryptographic module algorithms, existing modules such as symmetric (DES, 3DES) are considered [8]. Another scenario is to partition the matrix into sub-matrices, those could be used as secure encapsulated headers as shown in Figure (5-12), without de-capsulation previous headers, cipher text cannot be decrypted into plain one. Suggested encapsulation technique working as associated headers, that change the plain text formatting shape in type of encryption style, forwarding can be thought of one or more messages (locked text) inside locking header. This is illustrated in Figure (5-12). By applying entire summation of previous generated matrices and finding prime numbers vector, the largest primes can be used for crypto-module algorithm such as RSA [8, 40]. Applying RSA rules of encryption and digital signatures generation within its privileges offer maximum security due to the involved huge key size.

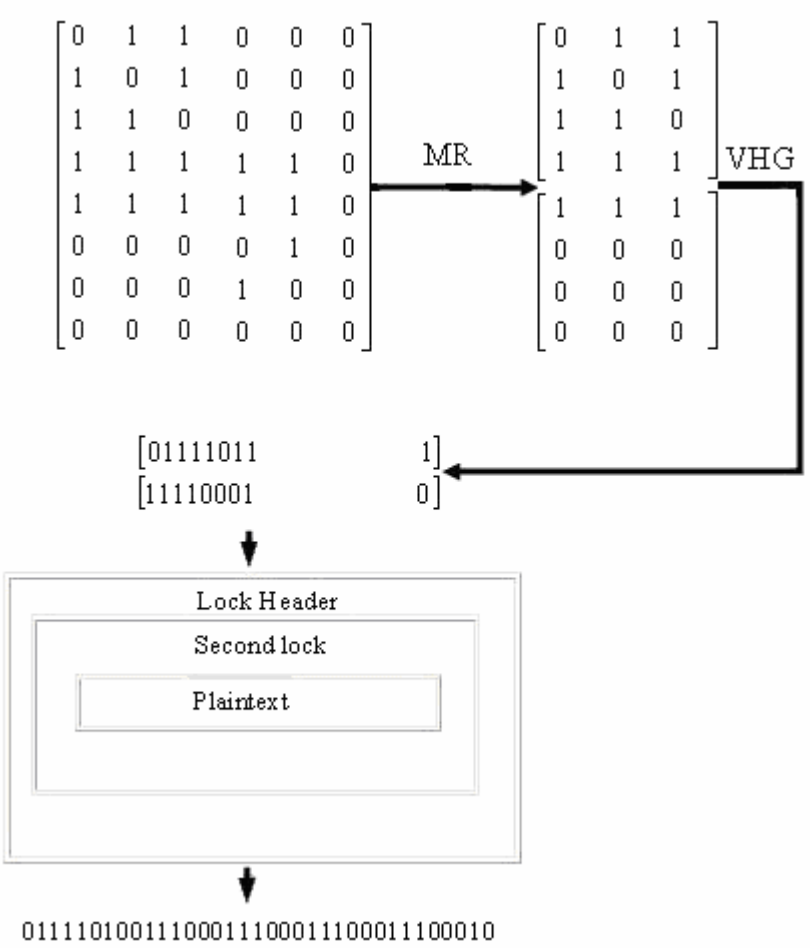


Figure 5-12 Encryption encapsulation technique, where MR is matrices regenerator, VHR is vector header generator

5.3.1Contour graph analysis

The proposed algorithm is extensively tested on DB1, FVC2002 database, 880 fingerprints images (TIFF, format, 374x388 size, and 500 dpi resolution), 800 images was used in our tests. The algorithm is tested on both scenarios (with singular point, and without singular point detection). Figure (5-13) shows adjacency matrix size under singular point detection averaging 103, is less than the matrix without SP, averaging 148. The average size differed because of the exclusion of the SP cropping relation.

.

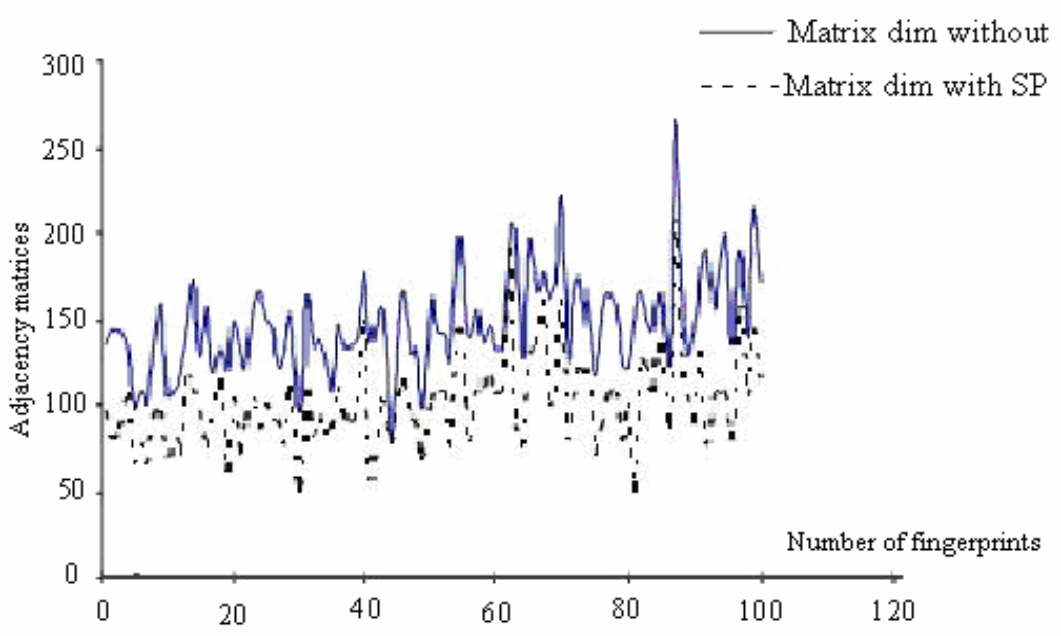


Figure 5-13 Adjacency matrices dimension

Because of different sizes of generated matrices, the key strength will be higher resistant brute force attack. Uniqueness of the key will be determined by the uniqueness of the fingerprint minutiae used in the key. Applying string matching algorithm on the generated matrices, it is found that 100% uniqueness on both cases as input to the crypto module phase. The protocols of FVC2002 is used to evaluate the False accept Rate (FAR) and Genuine Accept Rate (GAR) for overall phases. FAR is ratio of the number of false acceptances divided by the number of identification attempts, while GAR is the ratio number of true positive parameter. Using these parameters, we have plotted the receiver operating characteristic (ROC) curves of both cases when implemented as core point detection as well as without core detection (see Figure (5-14)).

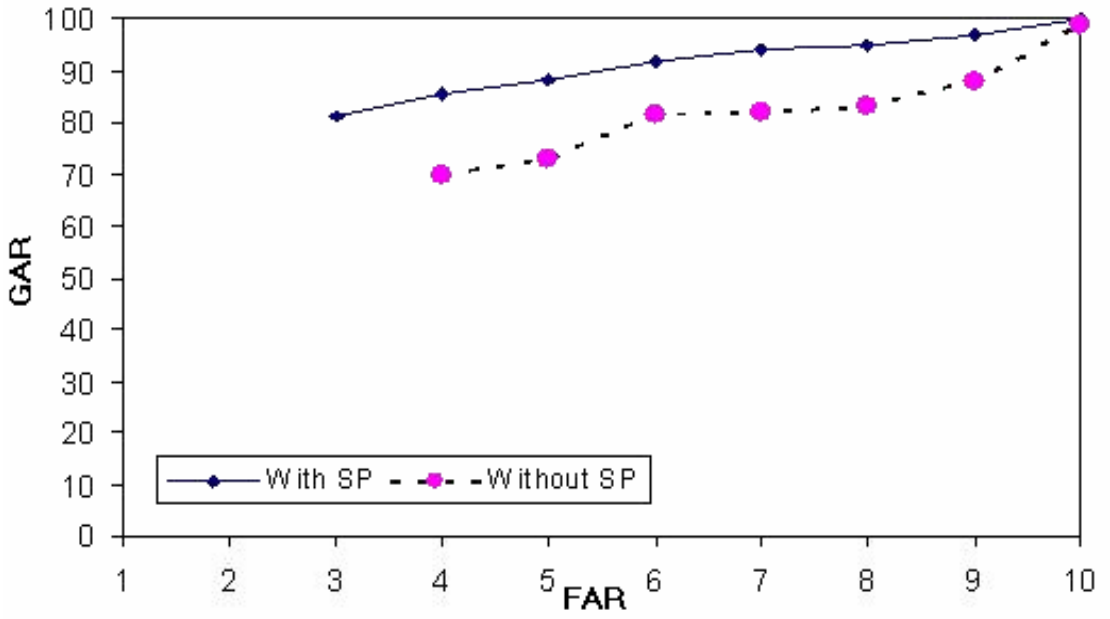


Figure 5-14 ROC curves estimated for both cases

The curves in Figure (5-14) show that 100% ratio of both scenarios (with and without singular point). At some points of threshold, first case (area surrounding core point) shows an improvement performance compared to the other case (without singular point detection). Results show that key generation depends completely on quality assurance of images and perfect minutiae extractor; empirically a minutiae detector (MINDTCT) released by NIST fingerprint image software 2 [37] is suggested. MINDTCT is standard software, automatically locates and records ridge ending and bifurcation in fingerprint images, and it includes minutiae quality assessment based on local image condition

5.4 Slicing Window Algorithm

The conceptual diagram of slicing window algorithm (SWA) is depicted in Figure (5-15). SWA used extracted core point as fundamental step. This step is particularly important since a reference centre is required to start with the expanded $(w \times w)$ slicing window. Figure (5-14) shows that SWA depends on detecting a unique reference point for computing a reference orientation for translational and rotational alignment as solution of misalignment problems. Reference point (RP) defines the coordination system of the fingerprint image regardless to the global transformation on the acquired fingerprint

image [110]. RP is identified by its symmetry properties, and is extracted from the complex orientation field estimated from the global structure of the fingerprint, i.e. the overall pattern of the ridges and valleys. Complex filters, applied to the orientation field in multiple resolution scales, are used to detect the symmetry and the type of symmetry. RP detection algorithm is mathematically represented bellow:

1. Orientation tensor image field computation:

$$z = \left(f_x + if_y\right)^2 \tag{5-24}$$

where f_x and f_y denote the derivatives of the image in x and y direction respectively.

The tensor is implemented by convoluting the grey value image with separable Gaussians and their derivatives. Already the calculation of the tensor implies complex filtering [111].

2. Complex filter computation:

$$c(x,y) = (x+iy)^m . \exp\left\{-\left\{\frac{x^2+y^2}{2\sigma^2}\right\}\right. \tag{5-25}$$

where m represents filter order and σ is standard deviation of modulated filter which is in this case modulated by Gaussian envelope.

3. The magnitude of the computed orientation tensor field is set to unity:

$$z'(x,y) = \frac{z(x,y)}{|z(x,y)|} \tag{5-26}$$

where z' is the normalized complex tensor and present the angel of this field.

4. Only one convolution operation is performed between the filter and the angles of the complex orientation tensor field as following:

$$z''(x,y) = \sum_{u=-\frac{w}{2}}^{\frac{w}{2}} \sum_{v=-\frac{w}{2}}^{\frac{w}{2}} C(u,v) \cdot z'(x - wv, y - wu)$$

where z'' is the magnitude of the filter response that is applied to the complex orientation tensor field, C is the mask of the complex filter and w is the width of that mask.

The aim is to trace all pixels to find the maximum value and to assign its (x,y) coordination to the core point i.e. reference point. Fingerprint feature extraction relies on detected RP at the centre of the distance between the extracted points and RP, by applying the Crossing Number (CN) concept. CN extracts the ridge points from the skeleton image by examining the local neighbourhood of each ridge pixel using a 3x3 window, Equation (5-1). Extracted minutiae $\mu(NxM)$ points which contain

$$\mu = \{\ \mu_i \mid \mu_i = (x_i, y_i, t_i, d_i) \mid i = 1 \ldots n_\mu\ \} \qquad 5\text{-}27$$

where x_i is the x-coordinate position, y_i is the y-coordinate position, t_i is the type and d_i distance of a particular minutiae, Equation (5-27) differ from (5-2) by using point distance. Distance defined according to the Euclidean distance, and computed between the extracted minutiae and the reference point:

$$D = \sqrt{(x_r - x_m)^2 + (y_r - y_m)^2} \qquad 5\text{-}28$$

where (x_r, y_r) is the reference point coordination and (x_m, y_m) are the minutiae point coordinates. Table (5-2) is showing some template information

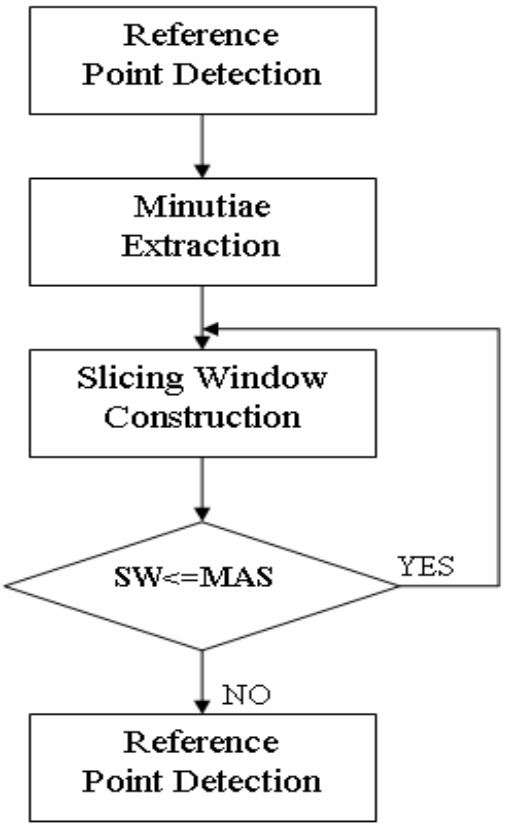


Figure 5-15 Basic block diagram

x	y	t	d
9	124	6	85.094
14	182	2	96.519
24	115	2	71.197
24	182	2	88.408
28	144	6	67.912
30	152	2	68.352
34	24	6	120.07
34	143	6	61.847
36	182	2	79.246
39	154	2	60.836

Table 5-2 Minutiae points' coordination's

The following procedure builds a slicing window based on principal of choosing first window as a first region of interest surrounding RP, empirically, it was chosen to be (64×64) window and the following windows will be its doubling $(128, 256, 512)$:

For i=1: T; // T is template size

Window size=64x64

Do minutiae counting entire window;

Vector generating; // number of minutiae by window size

Next windows; // 128… 256, till end of template size

End

End

Example result of formatting Table (5-2), shown in Figure (5-16)

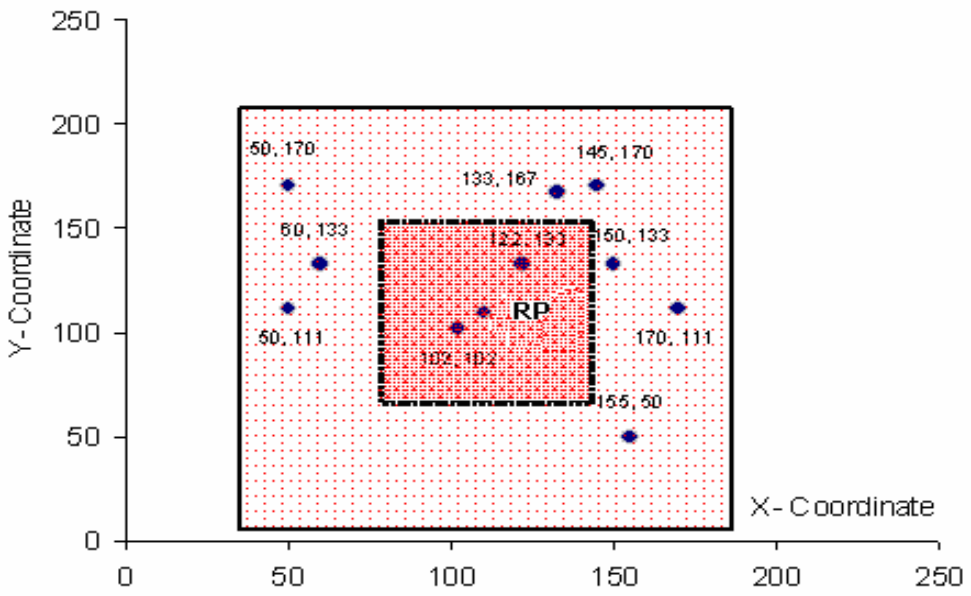


Figure 5-16 Windows structure based on template information.

According to the template area size, there will be at least 4 slicing windows, vector will be slicing window size multiplied by minutiae points' quantity, Generated vectors will be used for header locker key and encryption provider key usage. Header locker key (HLK) will be produced by V1, V3 concatenating, while encryption provider key (EPK) by V2, V4 concatenating, Figure (5-17).

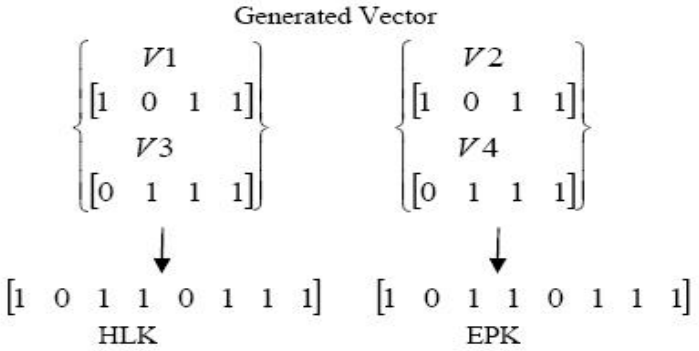


Figure 5-17 Generated keys, where HLK is Header Locker Key, EPK is Encryption Provider Key.

The stability of the generated keys will be dependent on the verified distinguished fingerprint extracted features from aligned qualified fingerprint images. HLK will be used as encrypted text closing key. Without passing this key the system cannot deal with the entire encryption procedure provided by EPK. EPK is a source key that will be used on either DES or RSA encryption algorithm sources.

5.4.1Slicing window analysis

SW algorithm is extensively tested on a database of 400 fingerprint images (TIFF, format, 300x300 sizes, and 500 dpi resolutions). The use of fingerprints was chosen for several reasons. First, it is the most studied biometric to date and large databases of fingerprint data are available for analysis [6]. Second, fingerprint recognition has been shown to be effective for distinguishing between users [112]. Third, fingerprint recognition is becoming widely accepted as the biometric most suitable for large scale implementation [113]. Tests show that generated key length depends on extracted minutiae points and their positions in slicing windows. The average key was 14 byte size Table (5-3). Table (5-4) shows the 100% uniqueness of generated keys.

Sub Keys	SIZE	KEY	SIZE
s101_1	7	s1	14
s101_2	7		
s102_1	8	s2	15
s102_2	7		
s103_1	6	s3	13
s103_2	7		
s104_1	7	s4	15
s104_2	8		
s105_1	7	s5	14
s105_2	7		
s106_1	7	s6	13
s106_2	6		
s107_1	7	s7	13
s107_2	6		
s108_1	7	s8	14
s108_2	7		
s109_1	8	s9	15
s109_2	7		
s110_1	7	s10	15
s110_2	8		
average	7.05	average	14.1

Table 5-3 Average of sub and whole key sizes

The entropy of applicable system feed by HLK and EPK is depending on secure system construction, which is in slicing window analysis (SWA) case has two secure criteria, cipher header closing as a part of file encryption certificate and plain text encoding instead of developing simply longer cryptographic keys to resist brute force attacks. SWA parts serve as infrastructure key for merging cryptography and biometrics. Tests were done on chosen fingerprint images with perfect quality and that impossible to find in practice, because fingerprint could not be identical from scanning to scanning, since measurement errors are inescapable when the fingerprint is scanned. Fingerprint will never be used as a seed of private key unless we can convert fingerprint to just one and the same identification in real time

KEY	s1	s2	s3	s4	s5	s6	s7	s8	s9	s10
s1	1	0	0	0	0	0	0	0	0	0
s2	0	1	0	0	0	0	0	0	0	0
s3	0	0	1	0	0	0	0	0	0	0
s4	0	0	0	1	0	0	0	0	0	0
s5	0	0	0	0	1	0	0	0	0	0
s6	0	0	0	0	0	1	0	0	0	0
s7	0	0	0	0	0	0	1	0	0	0
s8	0	0	0	0	0	0	0	1	0	0
s9	0	0	0	0	0	0	0	0	1	0
s10	0	0	0	0	0	0	0	0	0	1

Table 5-4 Uniqueness of generated keys where logical 1 (true) value indicates full matching and logical 0 (false) otherwise.

5.5 Summary

Approaches for generating biometric cryptographic keys for merging cryptography and biometrics have been presented. They take advantage of fingerprint template extracted information and standard encryption algorithms to provide a novel way of generating cipher keys without having to remember complicated sequences which might be lost, stolen, or even guessed. In addition these approaches provide encouraging prospects to be used as a platform for stable fingerprint extracted features; otherwise it could be used as seed of public key infrastructure (PKI) in which the private key is generated on a carry on device, e.g. smart card at the event that the legitimate user gives as seed of private key to his carry device in order to sign a message. To overcome key repeatable problems, a combination of fuzzy commitment prosperities and generation technique will be useful. To reduce fingerprint quality and dependence on alignment, Fuzzy scheme extraction and or vault generation will be useful too. In this case additional work will be performed to see if fingerprint parameters or classifiers may serve as a more stable and unique fingerprint biometric feature.

Chapter 6 Fuzzy Vault Cryptography Key Structure

6.1 Introduction

Crypto-biometric system [5, 15] has recently emerged as an effective process for key management to address the security weakness of conventional key generation, release, and binding systems using traditional password, token or pattern recognition based biometrics systems. It intends to bind a cryptographic key with user's biometric information in a manner to meet the following requirements [45, 61] of distortion tolerance, discrimination and security, see chapter (2.3):

- Distortion tolerance is the ability to accommodate the variance of the biometrics. The system is expected to output the same key for the same user even if the biometrics is acquired at a different time or under different conditions.

- Discrimination is the ability of the system to distinguish all users of the system and output different keys for different users.

- Security of the system means that neither the key, nor the user's original biometric information can be extracted or calculated when the stored information is compromised.

Chapter 5 showed techniques of key generation from biometric data in which the key is extracted directly from the biometric information. Crypto key generation algorithms have a very high proven security, but they suffer from the key management problem. However, there are two main problems with those methods First, as a result of changes in the biometric image due to environmental and physiological factors, the biometric template is generally not consistent enough to use as a cryptographic key. Secondly, if the cryptographic key is ever compromised, then the use of that particular biometric is

irrevocably lost. In a system where periodic updating of the cryptographic key is required, this is catastrophic. One of the main challenges in direct key generation approaches is to maintain the entropy of the key and keep the security of the biometric information simultaneously. The principle obstacle for direct crypto biometric key is the inherent variability of user biometric and to overcome this, crypto key generation moved from direct to the fuzziness binding approaches. The fuzziness principle of construct vault reformed from the fuzziness of fingerprint information. The development of fuzzy construct vault was started from commitment reconstruction, where the fuzzy commitment scheme was first proposed in [61] to integrate well-known error-control coding and cryptographic techniques to construct a novel type of cryptographic system. Instead of an exact, unique decryption key, a reasonable close witness can be accepted to decrypt the commitment. This characteristic makes it possible for protecting the biometric data using traditional cryptographic techniques. However, since the fuzzy vault used in this scheme does not have the property of order invariance, any elements missing or adding will result in the failure of matching. To overcome this problem, [45] proposed a new architecture, which possesses the advantage of order-invariance. At the same time, the author suggested that one of the important applications of the fuzzy commitment is secure biometric systems. Following this direction, [63] employed the fuzzy vault scheme on a secure smartcard system, where the fingerprint authentication is used to protect the private key. In the biometric cryptosystem, the secret information is hidden as coefficients in a polynomial, which acts as the frame of the fuzzy commitment. The fuzzy vault construct is a biometric cryptosystem that secures both the secret key and the biometric template by binding them within a cryptographic framework. The fingerprint vault construction is based on the assumption that the fingerprint features are extracted and well aligned in a black box. The work in this chapter will address the management analysis problems of fuzzy vault crypto structure, a new capsulation approach based on fingerprint fuzzy vault (FFV) will be proposed. FFV will be navigated through anatomy and attack, a performance evaluation of FFV will be demonstrated through out this chapter. This was the motivation to investigate the tolerance necessary for FFV to function, to see the effect of different vault and tolerance parameters and to determine the consequences on varying several of the vault and tolerance parameters.

6.2 Fuzzy Vault Anatomy

Fuzzy vault scheme (FVS) [45] was developed and built upon the ideas of the fuzzy commitment scheme [61]. The FVS consists of two parts, encryption, and decryption Figure (6-1, 2).

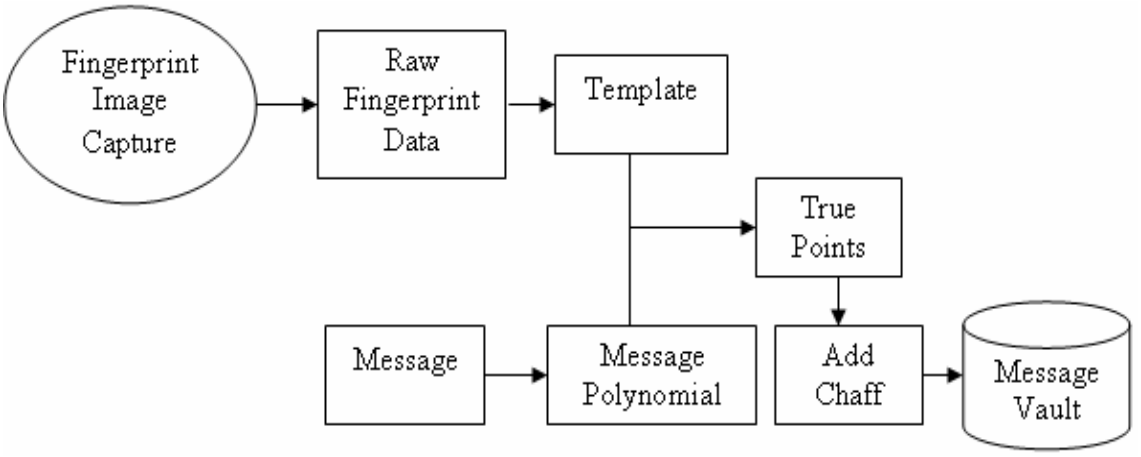


Figure 6-1 Fingerprint minutiae fuzzy vault message encryption.

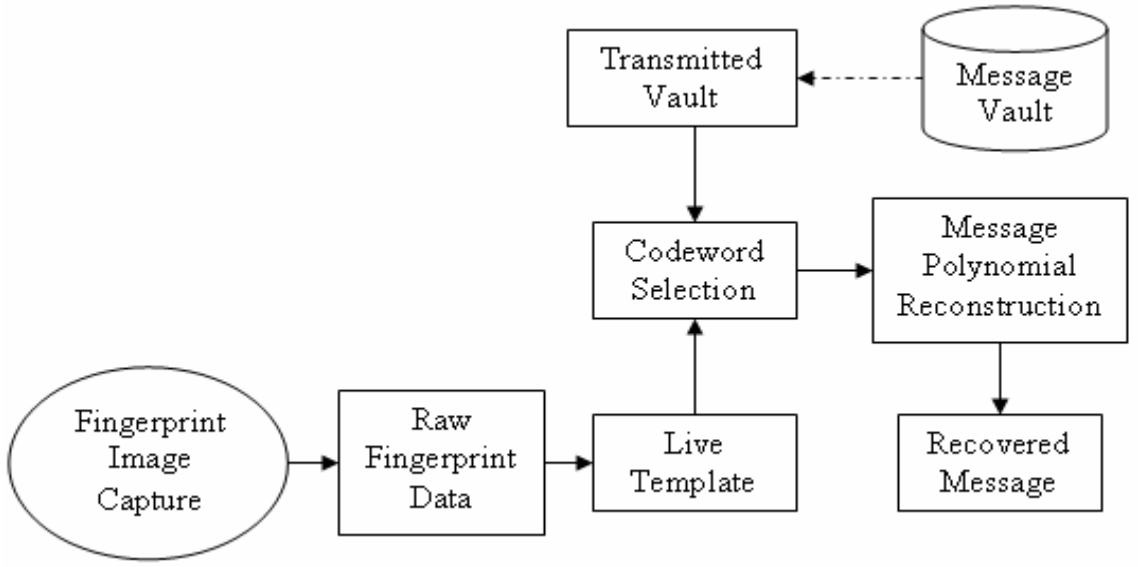


Figure 6-2 Fingerprint minutiae fuzzy vault message decryption.

In FVS, the message m is encoded as coefficients of a k-degree polynomial, in x (data points on the polynomial) over a finite field F_q. This polynomial is then evaluated at the

data points $(=X)$ in the input template to determine $f(X)(=Y)$. These (X,Y) pairs, known as true points, constitute the locking set of what is to become the fuzzy vault. To hide the identity of the true points, many false points (chaff) are then added to the set of true points. This completes the fuzzy vault, which is then stored. The security of the fuzzy vault scheme is based upon the difficulty of the polynomial reconstruction problem, or as described later, the problem of decoding Reed-Solomon codes. For an overview of research related to cryptography based on polynomial reconstruction, see [114, 115]. To unlock the vault and recover the message, the data points (X') from the "live" template (the unlocking set) are used for decryption. If a substantial number (i.e. within the symbol-correcting capability of the system) of these data points overlap (after error-correction) the true points in the stored vault, then the message can be successfully recovered. The main advantage to this system is that the order of the data points does not matter. Also, it can be shown to be secure, if there are sufficient chaff points in the vault relative to the number of true points.

6.3 Algorithm Mathematical Theory

The fuzzy vault scheme relies on methods of error correction commonly used in data communications to recover information sent over noisy transmission lines. The method often chosen in conjunction with the fuzzy vault scheme is Reed-Solomon (RS) coding which uses Galois field (GF) computations. The specific algorithm implemented in most fingerprint vault Berlekamp-Welch (BW) algorithm. These fundamental concepts were reviewed as infrastructure material to the fuzzy fingerprint vault and capsulation techniques.

6.3.1 Galois Fields

A Galois field is a finite field with order $q = p^n$ elements where p is a prime integer and $n \geq 1$. By definition, arithmetic operations (addition, subtraction, multiplication, division, etc.) on field elements of a finite field always have a result within the field. An element with order $(q-1)$ in $GF(q)$ is called a primitive element in $GF(q)$. All non-zero elements in $GF(q)$ can be represented as $(q-1)$ consecutive powers of a primitive

element (α). All elements in $GF\left(2^m\right)$ are formed by the elements $\{0,1,\alpha\}$. Taking the field $GF\left(2^3\right)$ and generator polynomial $x^3+x+1=0$, the elements of the field can be calculated, starting with an element called α which is called the primitive root (in this case, $\alpha=2=x$). All elements of the field (except 0) are described uniquely by a power of α. For any finite field $GF\left(2^n\right)$, $\alpha^{2n-1}=\alpha^0=1$. In this case, the field is constructed as follows [116]:

Power	Polynomial	Vector	Regular
0	0	000	0
$\alpha^0=\mathrm{x}^0$	1	001	1
$\alpha^1=\mathrm{x}$	x	010	2
$\alpha^2=\mathrm{x}\cdot\mathrm{x}$	x^2	100	4
$\alpha^3=\mathrm{x}^3$	$\mathrm{x}+1$	011	3
$\alpha^4=\alpha\cdot\alpha^3=\mathrm{x}\cdot(\mathrm{x}+1)$	$\mathrm{x}^2+\mathrm{x}$	110	6
$\alpha^5=\alpha\cdot\alpha^4=\mathrm{x}\cdot\left(\mathrm{x}^2+\mathrm{x}\right)=\mathrm{x}^3+\mathrm{x}^2$	$(\mathrm{x}+1)+\mathrm{x}^2$	111	7
$\alpha^6=\alpha^2\cdot\alpha^4=\mathrm{x}^2\cdot\left(\mathrm{x}^2+\mathrm{x}\right)=\mathrm{x}\cdot(\mathrm{x}+1)+(\mathrm{x}+1)$	x^2+1	101	5
$\alpha^7=\alpha\cdot\alpha^6=x\cdot\left(x^2+1\right)=x^3+x$	$(x+1)+x$	001	$1\ \left(=\alpha^0\right)$

$\alpha^8=\alpha\cdot\alpha^7=\alpha\cdot1=\alpha$ and the cycle repeats

Galois fields are used in a variety of applications such as linear block codes, classical coding theory and in cryptography algorithms.

6.3.2 Reed-Solomon Codes

Reed-Solomon codes employ polynomials derived from Galois fields to encode and decode block data. They are especially effective in correcting burst errors and are widely used in audio, CD, DAT, DVD, direct broadcast satellite, and other applications. An RS code can be used to correct multiple, random, error patterns. An (n, k) code can be defined where an encoder accepts k information symbols and appends separately a set of r redundant symbols (parity bits) derived from the information symbols, so that $n=k+r$. An (n,k) code is cyclic if a cyclic shift of a codeword is also a codeword. A cyclic binary code (for digital coding) can be specified such that codewords are binary polynomials

with specific roots in $GF\left(2^m\right)$. Inherited from the generator polynomial, these roots are common to every codeword.

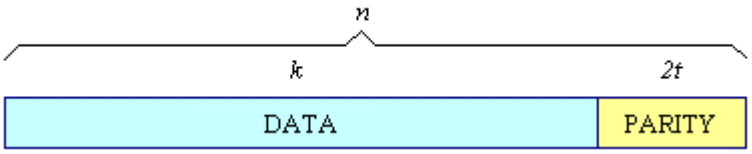


Figure 6-3 RS encoded block

As shown in Figure (6-3), the difference, $\left(n-k\right)$ (called 2t), is the number of parity bits that are appended to make the encoded block, with t being the error correcting capability (in symbols). A Reed-Solomon codeword is generated using a special polynomial. All valid codewords are exactly divisible by the generator polynomial which has the general form:

$$g(x)=\left(x-\alpha^{i}\right)\left(x-\alpha^{i+1}\right)\ldots\left(x-\alpha^{i+2t}\right) \qquad 6\text{-}1$$

The codeword is constructed as:

$$c(x)=g(x)\cdot i(x) \qquad 6\text{-}2$$

where $c(x)$ is the generator polynomial, $i(x)$ is the information block, $c(x)$ is a valid codeword and is referred to as primitive element of the field.

Example: Generator for RS(255,249) showing the general form and expanded polynomial form.

$$g(x)=\left(x-\alpha^{0}\right)\cdot\left(x-\alpha^{1}\right)\left(x-\alpha^{2}\right)\cdot\left(x-\alpha^{3}\right)\left(x-\alpha^{4}\right)\cdot\left(x-\alpha^{5}\right)$$
$$g(x)=x^{6}+g_5x^{5}+g_4x^{4}+g_3x^{3}+g_2x^{2}+g_1x^{1}+g_0$$

From the example, it can be seen that the original terms are expanded and simplified. The g coefficients $\left(g_5,g_4,g_3,g_2,g_1,g_0\right)$ are constants made up of additions and

multiplications of $\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4$ and α^5 and can be computed using Galois field computations. Reed-Solomon codes are cyclic codes but are non-binary, with symbols made up of m-bit $(m > 2)$ sequences. RS codes achieve the largest possible code minimum distance for any linear code with the same encoder input and output block lengths. The distance between two code words for non binary codes is defined as the number of symbols in which the sequences differ. Given a symbol size s, the maximum codeword length (n) for an RS code is: $n = 2^s - 1$. Given 2t parity symbols, an RS code can correct up to 2t symbol errors in known positions (erasures) or detect and correct up to t symbol errors in unknown positions.

6.3.3Welch-Berlekamp Algorithm

The Welch-Berlekamp algorithm is one of algebraic methods for decoding Reed Solomon codes. It can be thought of as a kind of curve fitting process of points, and a curve can be constructed to fit any *k* points. When two or more points are added, the curve must fit at least *k+1*, but the curve is allowed to miss one of the points. After adding another two points, the curve must fit at least *k+2* of them. When eventually all *n* points have been considered, the curve must fit at least $(n+k)/2$ of them. For more explanation, suppose that Alice sends Bob a message over a noisy channel. When Bob receives the message, some of the transmitted packets have been corrupted, but it is not known which packets are corrupt and which are not. Using RS encoding, Alice must transmit $(k+2t)$ characters to enable Bob to recover from *t* general errors. Therefore, the message is encoded as a polynomial $P(x)$ of degree $(k-1)$ such that: $c_j = P(j)$ for $1 \le j \le (k+2t)$. The received message is $R(j)$, for $1 \le j \le (k+2t)$. It differs from the polynomial $P(x)$ at *t* points. Bob now needs to reconstruct P(x) from the (k + 2t) values (the polynomial reconstruction problem). If Bob can find any polynomial P′(x) of degree (k – 1) that agrees with R(x) at (k + t) points, then P′(x) = P(x). This is because out of the (k + t) points, there are at most, t errors. Therefore, on at least k points, P′(x) = P(x). The transmitted polynomial of degree (k – 1) is uniquely defined by its values at k points. The polynomial reconstruction (PR) problem can be stated as follows [117] :

Given a set of points over a finite field $\{(z_i, y_i)\}_{i=1}^{n}$, and parameters [*n, k, w*], recover all polynomials *p* of degree less than k such that $p(z_i) \neq y_i$, for at most *w* distinct indexes, $i \in \{1,\ldots,n\}$. A unique solution can only be guaranteed when $w \leq (n-k)/2$. The BW algorithm can be used to recover the solution in polynomial-time given this constraint of *w*. The key idea is to describe the received message, $R(x)$ (which is not a polynomial because of the errors) as a polynomial ratio. The *t* positions at which errors occurred are defined as $e_1,\ldots,e_t$. The error locator polynomial is then defined as:

$$E(x) = (x - e_1)(x - e_2)\ldots(x - e_k) \qquad 6\text{-}3$$

At exactly the *t* points at which errors occurred, *E(x)* = 0. For all (k + 2t) points where *1* $\leq x \leq$ *(k + 2t),* $P(x) \cdot E(x) = R(x) \cdot E(x)$. At points *x* at which no error occurred, this is true because P(x) = R(x). At points *x* at which an error occurred, this is true because E(x) = 0. Let $Q(x) = P(x)E(x)$. Specified by (k + t) coefficients, *Q(x)* is a polynomial of degree *(k + t – 1)*. Described by *(k + 1)* coefficients, E(x) are a polynomial of degree t. There are only t unknowns because the coefficient of x^t is 1. There are also (k + 2t) linear equations in $Q(x) = R(x)E(x)$ for 1 ≤ x ≤ (k + 2t). For these equations, the unknowns are the coefficients of the polynomials Q(x) and E(x). The known values are the received values for R(x). The BW algorithm is illustrated by the following example (non-finite fields are used to simplify the calculations):

The information packets to be sent are "1", "3", and "7" (therefore, k = 3). By interpolation, we find the polynomial:

$$P(x) = X^2 + X + 1 \qquad 6\text{-}4$$

This is the unique second-degree polynomial evaluated at X = 1, 2, and 3:

$$P(0) = 0^2 + 0 + 1 = 1,$$
$$P(1) = 1^2 + 1 + 1 = 3,$$
$$P(2) = 2^2 + 2 + 1 = 7.$$

To be able to correct for one error (i.e., t = 1), (k + 2t), or 5, packets are transmitted (2 redundant):

$$\mathrm{P}(0)=1,\ \ \mathrm{P}(1)=3,\ \ \mathrm{P}(2)=7,\ \ \mathrm{P}(3)=3^2+3+1=13,\ \ \mathrm{P}(4)=4^2+4+1=21..$$

Now, assume P (1) is corrupted and 0 is received, instead of 3, in that packet. When correcting for a single error, the error-locator polynomial is: $E(X) = X - e$, where e is not yet known. R(X) is the polynomial whose values at $0,\ldots,4$ are those received over the channel (1, 0, 7, 13, 21).

As previously described:

$$P(x)E(x)=R(x)E(x) \qquad \text{6-5}$$

for $X = 0,1,\ldots,4$. Although P and E are not known (although it is known that P is a second-degree polynomial), the above relationship can be used to obtain a linear system of equations whose solution will be the coefficients of P and E.

Let

$$Q(x)=P(x)E(x)=aX^3+bX^2+d \qquad \text{6-6}$$

where a, b, c, d represent the unknown coefficients to be determined. Also,

$$aX^3+bX^2+cX+d=R(X)E(X)=R(X)(X-e) \qquad \text{6-7}$$

which can be rewritten as:

$$aX^3+bX^2+cX+d+R(X)e=R(X)X. \qquad \text{6-8}$$

Five linear equations are generated when substituting $X = 0,\ X = 1,\ ,\ldots, X = 4$ into the above formula:

$$\begin{aligned}
a(0)^3+b(0)^2+c(0)+d+(1)e&=1(0);\\
a(1)^3+b(1)^2+c(1)+d+(0)e&=0(1);\\
a(2)^3+b(2)^2+c(2)+d+(7)e&=7(2);\\
a(3)^3+b(3)^2+c(3)+d+(13)e&=13(3);
\end{aligned}$$

$$\begin{aligned}
d+\ \ e\ &=\ 0\\
a+\ \ b+\ \ c+d\ &=\ 0\\
8a+\ \ 4b+2c+d+\ \ 7e\ &=14\\
27a+\ \ 9b+3c+d+13e&=\ 39
\end{aligned}$$

$a(4)^3 + b(4)^2 + c(4) + d + (21)e = 21(4);$ $64a + 16b + 4c + d + 21e = 84.$

The result of solving these linear equations is: a = 1, b = 0, c = 0, d = -1, e = 1. This enables the generation of the polynomials *Q(X)* and *E(X)*. *P(X)* is then computed as the quotient $Q(x)/E(X)$. The original, uncorrupted values can now be recovered from P(X). The mathematical background of pertinent error correction codes and BW algorithm made the implementation of the fuzzy vault scheme understandable. In next sections, the fuzzy vault scheme uses the BW algorithm for error correction with calculations performed in a Galois field will be evaluated in terms of FVS parameters.

6.4 Fingerprint Vault Implementation

Fuzzy vault scheme was implemented and simulated based on Figures (6-1, 2), using fingerprint minutiae points. Fingerprint minutiae were extracted using MINDTCT option of NIST Fingerprint Image Software Version 2. FVC 2004 DB1-A database used as simulation database platform, which contain 100 fingers and 8 impressions per finger, image size (640x480 (307 K pixels)), resolution 500dpi.

6.4.1Fingerprint Vault Encryption

Creating the Template

The encryption portion of the system is the creation of the fuzzy vault for the message. A template created from multiple images of the same fingerprint is used as a cryptographic key to encode a message defined by the coefficients of a polynomial. Data points that represent the polynomial are stored in the fuzzy vault. Many random data points (chaff) are added to the vault to hide the identity of the true polynomial data points. MINDTCT is used to create the fingerprint template Figure (6-5).

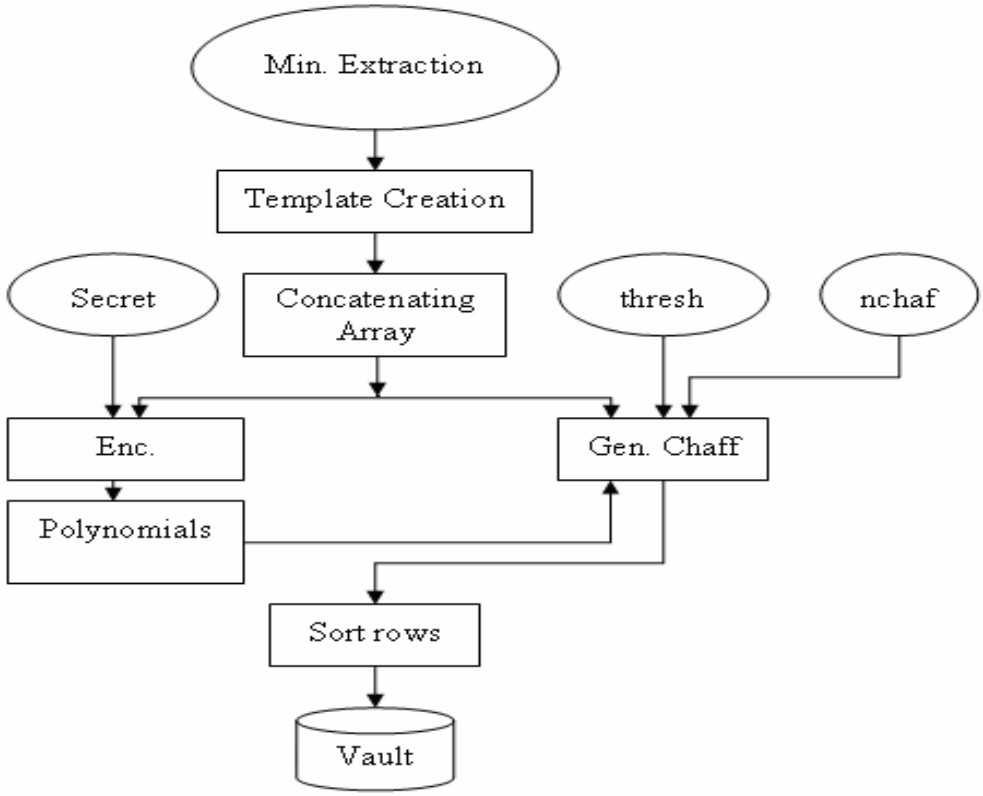


Figure 6-4 Fingerprint vault encryption implementation model

No	X	Y	Theta
0	162	248	45
1	177	162	56
2	180	143	236
3	181	227	236
4	186	201	236
5	187	224	56
6	190	188	56
7	192	277	34
8	197	284	214
9	199	215	236
10	207	136	79
11	209	214	56
12	213	106	304
13	218	153	79
14	222	83	326
15	224	297	0
16	228	176	236
17	230	111	304
18	239	179	45
19	240	167	202
20	241	72	315
21	242	148	112
22	242	103	304

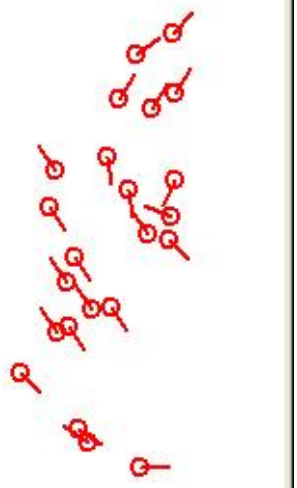


Figure 6-5 Extracted minutiae points using NSIT MINDTCT

Extracted information contains: minutiae coordinate (x, y) and orientation angle (θ). To obtain repeatable data points, only those data points found to occur (within a predefined threshold) in more than half of impressions were used to create the input fingerprint template. The $X-$ value (codeword) for the true data points is calculated by concatenating either $(x\|y), (x\|\theta)$, or $(y\|\theta)$, where the decryption process will concatenate the identical data variables. Since it is desirable that all values be constrained to a finite size, all symbols are defined to be within a finite field and all calculations are performed using finite field operations. In practice, data communications (especially with error-correction) often use finite fields referred to as Galois Fields. In particular, $GF(2^n)$ fields are used, where the 2 indicates that the field is described over binary numbers and *n* is the degree of the generating polynomial [116].

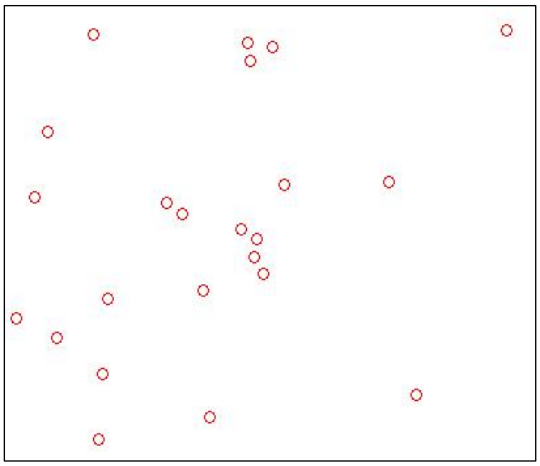
Creating the Message Polynomial:

The symbols of the message are encoded as the coefficients of a *k*-degree polynomial. For example, the string "Mokhled", or ASCII (77,111,107,104,108,101,100), could be represented by the 6^{th}-degree polynomial:

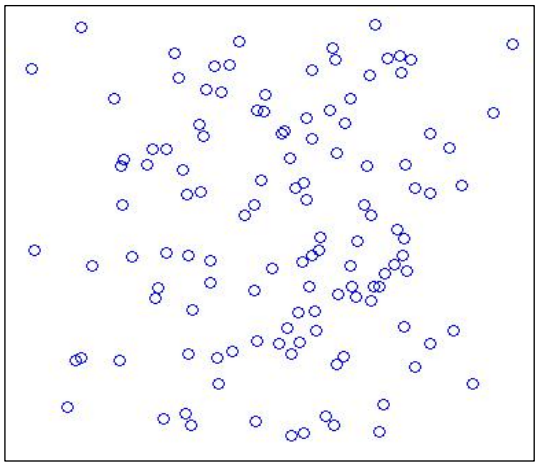
$$77x^6 + 111x^5 + 107x^4 + 104x^3 + 108x^2 + 101x^1 + 100.$$

Creating the Message Vault

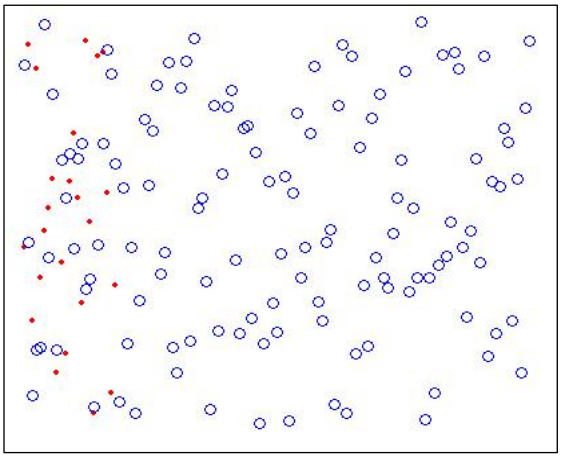
To hide the identity of the true points, many false points (chaff) are added to the vault Figure (6-6). The false points are added far enough away from true points so they do not cause attraction of values within the fuzziness (threshold distance) of the true points. Also, they are placed outside the threshold distance of other chaff points since they would otherwise be redundant. As a final step in the vault creation, all points in the vault are sorted, resulting in a mixture of true and false points from which the true points must be discovered when decrypting the message.



(a) True points distribution



(b) Chaff points distribution



(c) True and Chaff points distribution

Figure 6-6: True, chaff, True-Chaff distribution

Chaff point generation is dependent on the number of chaff points and a predefined threshold. The threshold is the radius from a vault point that a live point would match. This value is given in integer normalized (x, y) coordinate units. Therefore, a value of one corresponds to a Euclidean distance radius threshold of $\sqrt{1^2+1^2} = \sqrt{2} \approx 1.41$ units (Table 6-1). Therefore each subsequent increment would increase the threshold by this distance, range: 0 to 6 incremented by 1.

Units	Distance
1	1.414
2	2.828
3	4.243
4	5.657
5	7.071
6	8.485
7	9.899
8	11.314
9	12.728
10	14.142
11	15.556
12	16.971

Table 6-1 Unit to Euclidian distance equivalence

6.4.2Fingerprint Vault Decryption

The message vault is received and is attempted to be decrypted by the input template created from a live fingerprint template Figure (6-7). The minutiae data from the live template (X') are compared to the X values (codewords) in the vault pairs. If enough codewords overlap, then the message can be recovered through polynomial reconstruction. The template creation process is identical to the process used during encryption, except that data captured from only a single fingerprint impression is processed. The resulting data is identified as X'.

Codewords Selection

To reconstruct the message polynomial, the user must identify true codewords from the vault, since the corresponding (X, Y) pairs define the polynomial. The X' data is used to select the true codewords from the vault. Since biometric data are expected to be inexact (due to acquisition characteristics, sensor noise, etc.), X' template values are matched to X vault values within a predefined threshold distance, thus allowing for exact symbol matching. This is the "fuzziness" built into the system, since multiple X' values (i.e., those within the threshold distance of X values) will result in a single X value.

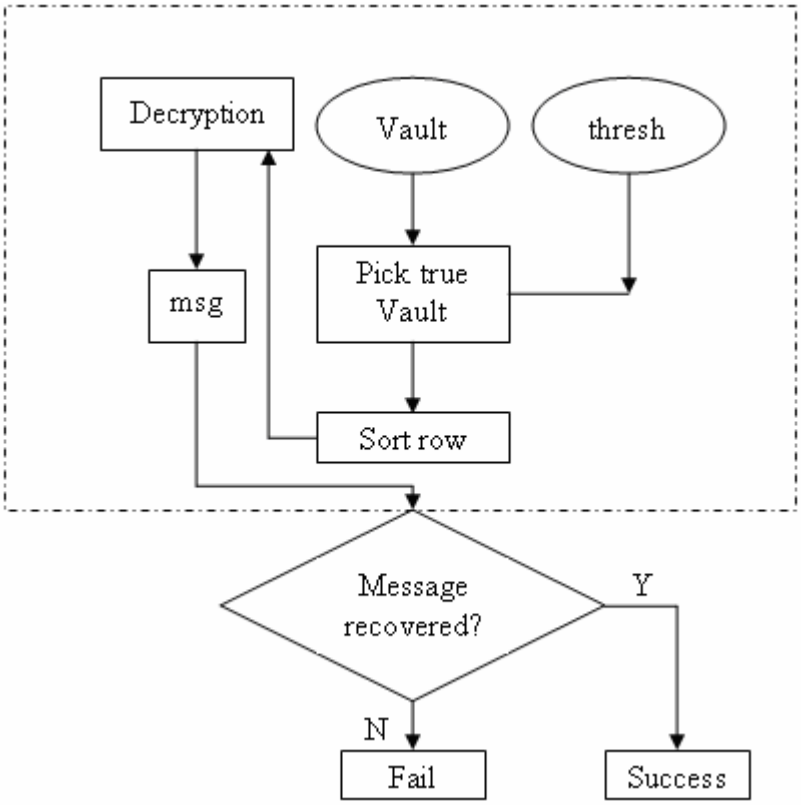


Figure 6-7 Fingerprint Vault Decryption implementation model (dashed box)

Message Polynomial Reconstruction

The message polynomial is attempted to be reconstructed using the (*X*, *Y*) pairs identified by the live template. A valid live template may contain more/less/different minutiae than those extracted when the original template was created. However, if there is significant overlap of *X* and *X*′ codewords, the message can still be recovered by using a typical telecommunications error-correcting scheme for recovery of data over a noisy channel, such as a Reed-Solomon (RS) code. As reviewed earlier, RS (*k*, *t*) codes are those in which codewords consist of *t* symbols and each codeword corresponds to a unique polynomial *p* of degree less than *k* over the finite field *F* of cardinality *q*. Therefore, there are q^k total codewords. In the implemented system, Welch-Berlekamp algorithm is used for detected error-correction [118]. Given m pairs of points (X_i, Y_i), where $i = 1,2,\ldots m$, there exists a polynomial $p(x)$ of degree at most *d*, such that $Y_i = p(X_i)$ for all but *k*

values of (X_i, Y_i). Using the BW algorithm, if $2k + d < m$, this condition can be verified by finding the solution for a linear constraint system:

$$N(X_i) = Y_i * W(X_i), \quad i = 1,2,\ldots,m \qquad 6\text{-}9$$

where polynomial degree $(W) \leq k$

$p(x) = N / W$ is the result polynomial after the $2k + d + 1$ unknowns are calculated.

Message Recovering

The recovered message is simply made up of the coefficients of the reconstructed message polynomial. It is usually the case that an invalid live template will result in a polynomial that cannot be reconstructed within the error tolerance of the system, and therefore no message is decrypted.

6.5 Fingerprint Vault Experimental Analysis

Fingerprint vault system implemented with the assumption of reference point detection, fingerprint image alignment. Using a database of 800 fingerprint impressions (FVC DB1-A) It was found that the fuzzy vault scheme was able to successfully unlock 69% of created vaults. This result proves the claim that the fuzzy vault scheme without additional security is vulnerable to such attacks. The system was also investigated to determine the necessary tolerance parameters, i.e. chaff points, threshold and true points. It is investigated in the following environment

Number of true points	Number of chaff points	Thresh	Number of tries
[25-60] step 5	[0-500] step 100	[0-6] step 1	[3]
8 options	6 options	7 options	3 options

Table 6-2: Fuzzy vault investigation environment

The distribution of the number of successful message recoveries from 4368 simulations [(8 number of true x 6 number of chaff points x 7 thresh x 13 the vary distance between live points), done 3 times]:

zero	one	two	three
2889	194	151	1134

Table 6-3 Successful message recovery

The simulation effects on successful message recovery, when varying the parameter [Number of true points, Number of chaff points, Threshold, and live check points]; these parameters were examined through a series of box plot. Box plot was chosen because it provides excellent visual summary of all parameter distribution. In these plots, the box has lines at the lower quartile (25%), median (50%), and upper quartile (25%) values. The whiskers are lines extending from each end of the box to show the extent of the rest of the data. Outliers are data with values beyond the ends of the whiskers. If there is no data outside the whisker, a dot is placed at the bottom whisker. In each plot, Y-axis parameters are plotted against number of successful recovered messages.

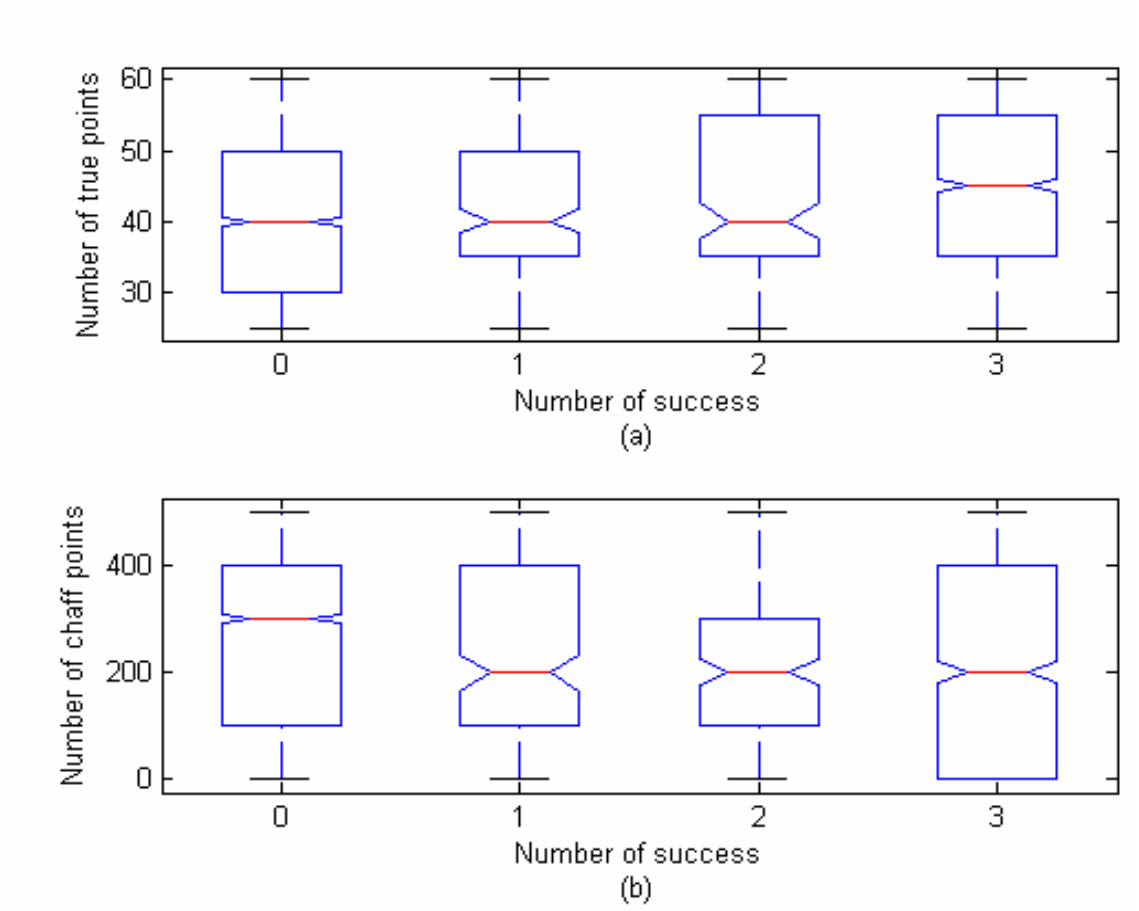


Figure 6-8 Effect of points parameter (a) true points, (b) chaff points

The number of true points from Figure (6-8 (a)) is between (30 & 55). Within the range simulated, this parameter has little significant effect. This result is expected because the number of true points is small in relation to the number of total vault points, i.e. the true points represent a small proportion of the total vault points. Low median value is 40 for 0, 1 & 2 success. Within the parameter range, there is a small effect due to the number of chaff points. As the number of chaff points increases, it is somewhat more difficult to recover the message, as shown in Figure (6-8b), the increased median value of 300 chaff points, when the message is never recovered (success =0). The median value is 200 when the message is recovered at least once.

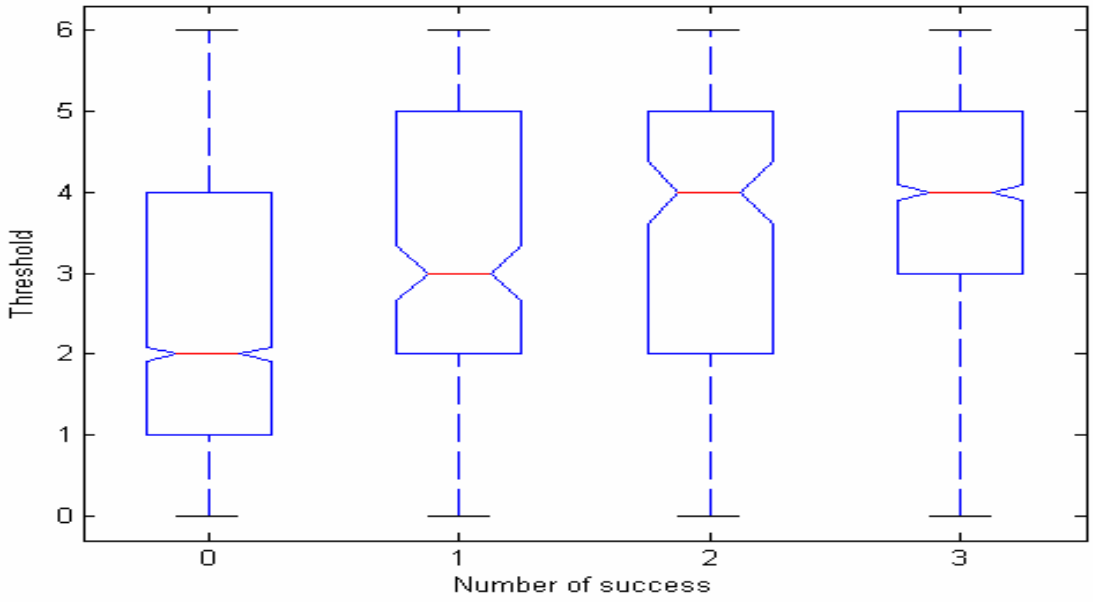


Figure 6-9 Effect of threshold parameter

Figure (6-9) shows that, as the value of the threshold parameter increases, the success rate increases. It shows the median value for no message recovery is 2 and the median value for all messages recovered is 4. The upper quartile for successes [1, 2 and 3] is identical. This parameter is clearly shown to be positively correlated with success since the greater the threshold parameter the more tolerance for matching true points.

6.6 Fingerprint Vault Key Capsulation Technique

With the rapid growth of information technology fields, the live interaction of electronic information management becomes impossible as the validity of contact has to be verified

as well as certified by secured verification and or authentication scenarios. Therefore, the idea of cryptography and biometrics has been introduced as part of a privacy enhancing technology (PET) with respect to personal data protection, user convenience, reliability and robustness against impostor user. However, it is vulnerable to attacks, e.g. cracking, and tracking of information sources. A bio-crypt key has been introduced to solve the security management problems, i.e. they must be stored securely and released based on some strong authentication mechanisms. Fingerprint vault results prove the claim that the fuzzy vault scheme without additional security measures is indeed vulnerable to correlation attacks, for this reason, biometric key capsulation proposed.

6.6.1 Biometric Key Capsulation

Biometric based authentication is a potential candidate to provide a capsulation cover for traditional and general cryptographic keys. Fingerprint has been chosen as a construction core of fuzzy vault for encapsulation technique due to its maturity in terms of availability, uniqueness, permanence, feasibility, ease of use and acceptance. Biometric key capsulation (BKC) is a combination of both biometric authentication and cryptography-based control. A cryptographic key and vault are encapsulated using fuzzy encapsulation of the transformed biometric data. Fuzziness means that a value close to the original is sufficient to extract the encapsulated value. Fuzzy encapsulation technique is both conceals and binds thus making it difficult for an attacker to learn the encapsulated value.

Capsulation pre-processing

It is well-known that for encryption, keys at both the sender and receiver sides must match exactly. However, repeated capture of biometric data from the same subject usually does not result in identical data in each capture, but similar feature extraction. This is due to several factors, including sensing errors, alignment errors, presentation angles, finger deformation, skin oils, dirt, etc. Because of this inexact reproducibility, a method is needed to “correct” the data before it is presented to the processing subsystem in order to obtain reproducible results. This can be accomplished by applying error-correcting codes [48], as a common practice when recovering messages transmitted over a noisy channel. Yoichi, et al. [119] proposed a statistical A/D conversion as effective

scheme to convert biometric data to just one identification number; their solution could be used as another scenario to overcome the template reproducibility problems. Either [48] or [119] are useful for preparing minutiae based templates as a first stage of capsulation approach Figure (6-10).

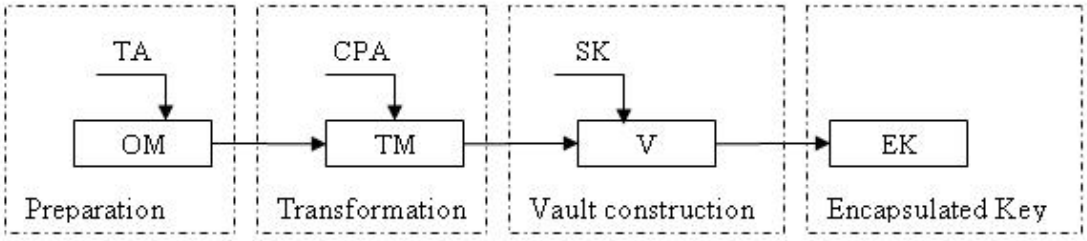


Figure 6-10 Biometric Key capsulation block diagram

6.6.2 Encapsulation Algorithm

The encapsulation portion of the security diagram, Figure (6-10), creates capsulation shields, which are the seeds for the BKC approach. A transformed template features are constructed by applying the concatenation transformation on true data points to avoid using direct template; the transformed matrix (TM) values are represented as transformed features string.

$$TM = \left((x \,||\, y) \| \theta\right) \qquad 6\text{-}10$$

where x, y are minutiae point coordination, θ is orientation

A chaff point algorithm, Figure (6-11), is used to generate random chaff points (CP) to add to the TM based on union relation to generate a total points set (TP).

$$TP = TM \bigcup CP \qquad 6\text{-}11$$

Chaff Point Algorithm

Inputs: Transformed points (true points)

Threshold distance

Output: TP (total points) – Array containing all true and chaff points.

Algorithm $TP \leftarrow (\text{number of chaff points, thresh, true points})$

Point uniformly and randomly chosen from the coordinate's domain $(0..2^{16})$

Do while conditions

Conditions:

If it within distance from any previously selected points {

Then discard it}

If not {

Select it}

$TP = TM \bigcup CP$

Return

End

Figure 6-11 Chaff point generation algorithm

The TP servers as first capsulation shield. Next, a construct vault $V_{(TP)}$ is computed from the TP, and the injected secret key (SK), Figure (6-12). $V_{(TP)}$ could be used as a second capsulation shield and it is stored in the header of the encrypted file in clear for vault reconstruction usage at the decryption stage.

Vault Construction Algorithm

Inputs: Injected secret key (SK); Total points (TP)

Output: $V_{(TP)}$ (Vault total points) % Array containing.

Algorithm

$V_{(TP)} \leftarrow (\text{SK encoded message as coefficients of polynomial, Galois field array from TP})$

Do compute

Galois field array of SK in the coordinate's domain $(0..2^{16})$

% Galois field array created from SK in the field GF 2^m , for 1<=M<=16. The elements % of SK must be integers between 0 and $2^m - 1$.

Galois field array of TP in the coordinate's domain $(0..2^{16})$

$V_{(TP)}$ = Evaluate polynomial value of encoded SK & TP

Return $V_{(TP)}$

End

Figure 6-12 Vault construction algorithm

Finally, a part of encrypted vault servers as file header for the encryption usage, or could be stored in the header of the encrypted file, which it will be the final encapsulation shield.

6.6.3 Decapsulation Algorithm

To decapsulate the vault and recover its components (i.e. the message, chaff points, transformed points), the data points (OM′) from the "live" template (the unshielded set) are used for decapsulation. If a transformed substantial number (i.e. within the symbol-correcting capability of the system) of these enquiry data points overlap (after error-correction) with the true transformed points in the stored vault, then the message can be

successfully recovered, as well as partially vault (header file key) will be released from final shield of encrypted file. In decapsulation portion of the security capsulation algorithm, a FIFO (first in first out) rule must be applied for the whole decryption process. Follow the principles, the constructed vault will be unshielded, decapsulated to the key release, finally the bound secret key, and header key are released Figure (6-13).

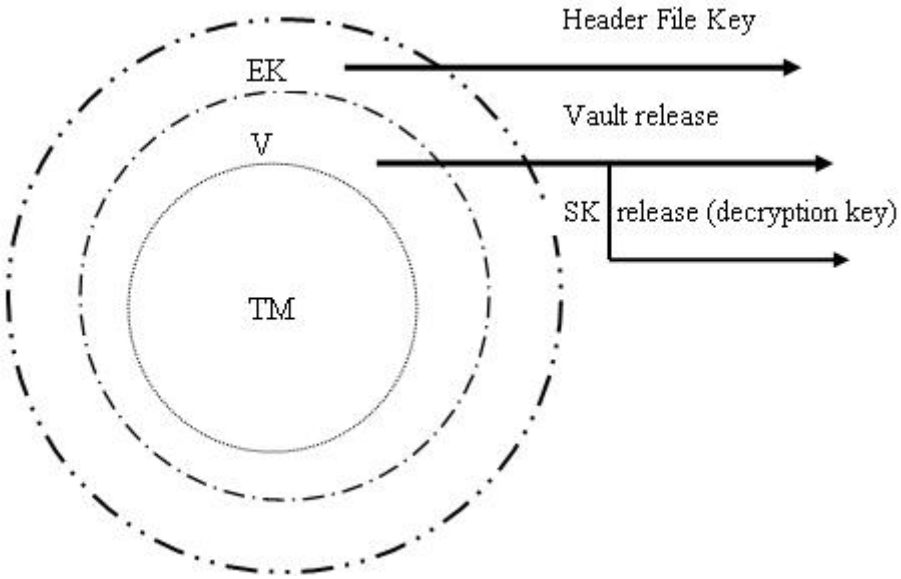


Figure 6-13 Biometric Key decapsulation diagram

6.7 Expected Attack

Biometric key capsulation approach benefits from binding crypto biometric techniques. It combines revocable transformable templates, generated chaff points, hiding secret transformable amidst chaff points, vault construct, and shielding (encapsulation, decapsulation) technique. Referring to the Figure (6-13) attackers have to brutally attack the cycles of shielding to yield encapsulated keys, which they are related to each other hierarchy. The total complexity of the proposed approach belongs to the nested loop analysis computational complexity. BKC contain three nested loops, core inner, and two outer, thus the complexity is:

$$O(first\_outer\_times * second\_outer\_times * inner\_times).$$

It could be concluded that, the classes of attacks against BKC approach include: brute force attack against all BKC shields (i.e. EK, V, and TM), and chaff point identifications to find the original ones [120]. For example, the vault could be attacked by brute-force method, $bf(r,t,k)$, where r is the total number of points, t is the number of real points, and k is the degree of the polynomial. For an attacker, r and t are of the same length as the ones in the vault parameter, however for a valid user, r is the size of their unlocking set and t is the number of non-chaff points in that set. The complexity of brute force (C_{bf}) can be calculated according to equation (6-12).

$$C_{bf} = \binom{r}{\sigma}\binom{t}{\sigma}^{-1} \qquad 6\text{-}12$$

where σ is the point that interpolate a degree k polynomial, which is $\sigma = k+1$.

6.8 Simulation result and analysis

Biometric Key Capsulation Technique was implemented on the FVC2004-DB1 [21], a public domain database with 800 images (100 fingers and 8 impressions for each finger), (cropped into 256x256 sizes, 500 dpi resolutions), converted into WSQ format, for convenience to simulate the capsulation processes. Original minutiae were extracted using minutiae detector (MINDTCT) released by NIST fingerprint image software 2 [37]. The transformed points formatted by concatenating the original points coordination and orientation, where the average of extracted minutiae is 52 points while chaff points were chosen to be 300 points. The point threshold distance was adapted to 6 according to the Berlekamp Welch error correcting code theory with a polynomial degree d. The equation condition is $2k + d < m$, that means to successfully decode the finger vault, the number of impostor points must satisfy $k < (m-d)/2$, where m is the total number of the input transformed points. The core of the proposed BKC is the cancellable constructed vault, which we will test under all reconstruction parameters, like polynomial degree, minimum distance of point distribution, and vault complexity. Figure (6-14) shows the relationship between chaff points, minimum distance and release ability of locked key. We set the minimum distance to satisfy the following rules: chaff points cannot be placed too close

to real points, no reason to place chaff points next to each others at any distance less than minimum distance, because the attacker can immediately ignore them as unlikely candidates. While Figure (6-15) shows the relationship between polynomial degree and vault complexity where the used extracted minutiae is 52 points while chaff points were chosen to vary from 100 to 500 points.

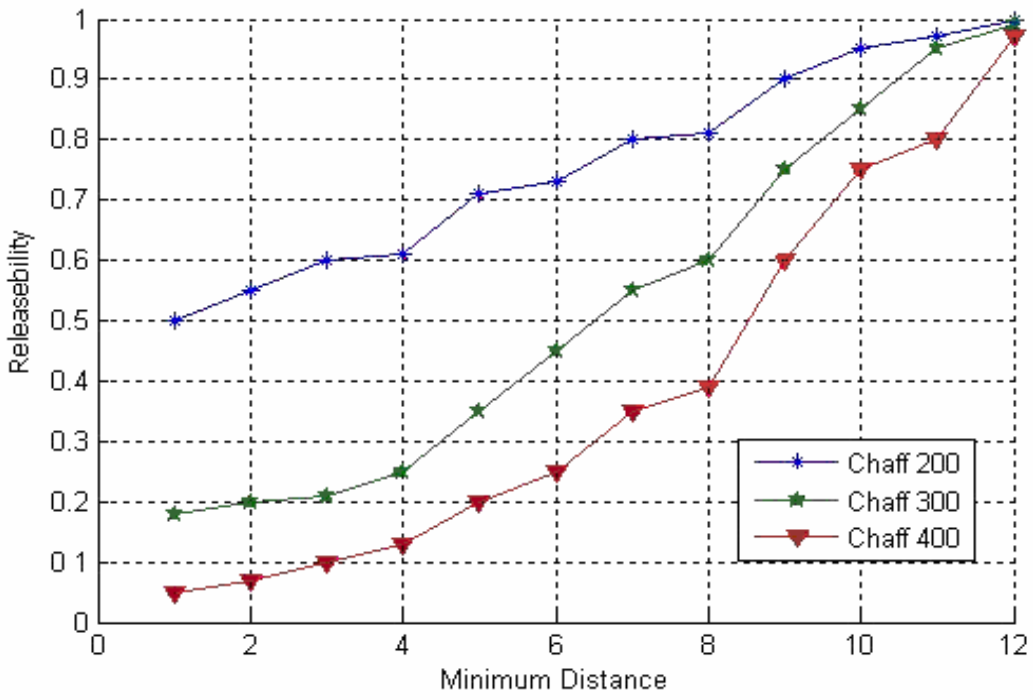


Figure 6-14 The relationship between chaff points, minimum distance and release-ability of locked key.

A basic anatomy of vault unlocking can be viewed in two contexts. The first is the complexity of a valid user unlocking a vault with a matching fingerprint image. One goal is to minimize this complexity. The second context is the complexity of an attacker without fingerprint information trying to crack the vault. All researchers in this field wish to maximize this complexity while the attacker wishes to minimize it. Figure (6-15) shows that a higher level of security is related to higher degree of polynomial as well as a maximum number of chaff points. However, it is clear that a higher complexity could be achieved with maximum values of vault parameters.

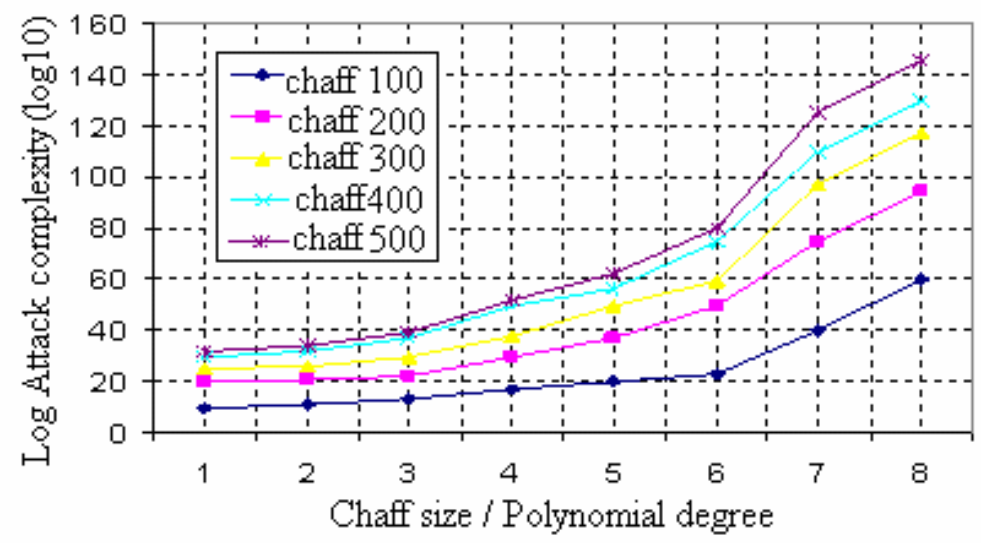


Figure 6-15 The relationship between chaff points, Polynomial degree, vault complexity

6.9 Finger Vault Vector Features

Fuzzy vault based on fingerprint features vector, or so called FingerCode [121, 122] is constructing a bound bio crypto key. The idea behind using FingerCode as a replaceable seed of minutia set fuzzy construct is the ability to distinguish the extracted FingerCode where it is reasonably stable. A FingerCode is composed of an ordered enumeration of the feature extracted from the local information contained in each image sector in cropped images. A feature vector is the collection of all features in each filtered image. These features capture both the global pattern of ridges and valleys and the local characteristics. The FingerCode scheme of feature extraction tessellates the region of interest in cropped image, i.e. cropped images into [16X16], [32X32] and [64X64] surrounding the image reference point. The scheme is divided into two stages: pre-processing and feature extraction stages Figure (6-16).

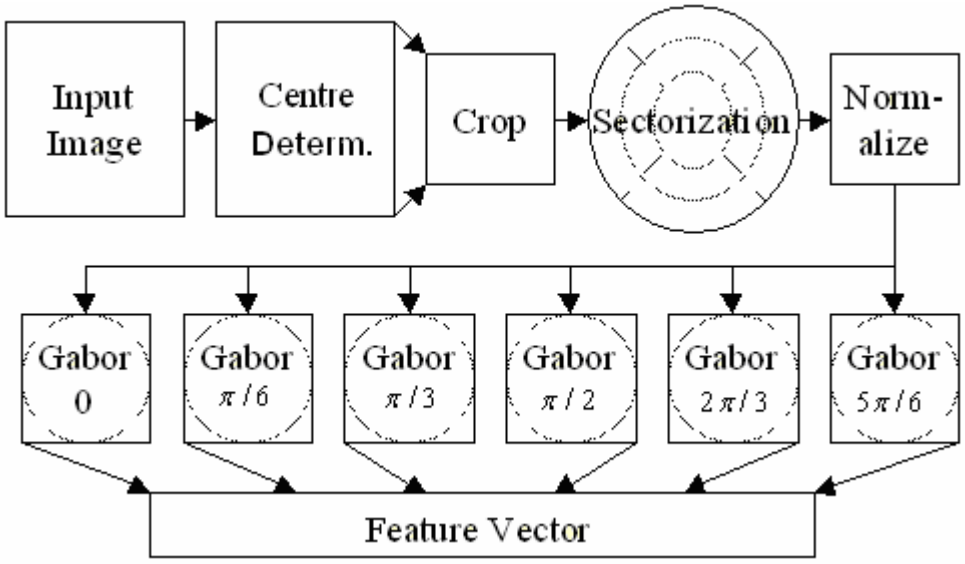


Figure 6-16 Fingerprint Vector Features scheme

6.9.1Preprocessing

The preprocessing stage contains three main steps: Centre Point Determination, Cropping, Sectorization and normalization the region around the reference point.

6.9.2 Centre Point Determination

Centre point location is done to find the point of most curvature by determining the normal's of each fingerprint ridge, and then following them inwards towards the centre. The following steps are used to determine finger print reference point

- Image Noise reduction using 2-D Gaussian lowpass filter.
- Image division into [16X16] none overlapping blocks.
- Determine the x and y magnitudes of the gradient at each pixel in each block, G_x and G_y.
- Gradient smoothing by applying 2-D Gaussian lowpass filter.
- With each block, compute the slope perpendicular to the local orientation field using equation (6-13)

$$\Theta = \frac{1}{2}\tan^{-1}\left(\frac{\sum_{i=1}^{16}\sum_{j=1}^{16} 2G_x(i,j)G_y(i,j)}{\sum_{i=1}^{16}\sum_{j=1}^{16} G_x^2(i,j) - G_y^2(i,j)}\right) + \frac{\pi}{2} \qquad 6\text{-}13$$

- Only looking at blocks with slopes with values ranging from 0 to π/2, trace a path down until you encounter a slope that is not ranging from 0 to π/2 and mark that block.

- The block that has the highest number of marks will compute the slope in the negative *y* direction and output an *x* and *y* position which will be the centre point of the fingerprint.

The image is then cropped into three options of cropping images centred around this pseudo –centre point.

6.9.3 Sectorization and Normalization

The cropped fingerprint image is divided into 5 concentric bands centred around the pseudo-centre point. Each of these bands has a radius of 20 pixels, and a centre hole radius of 12 pixels. Thus, the total radius of the sectors is 223 pixels. Each band is evenly divided into 12 sectors. The centre band is ignored. This process of sectoring is done because of the feature extraction section. 6 equi-angular Gabor filters will be used which will align with the 12 wedges formed by the bands. In other words, each sector will capture information corresponding to each Gabor filter. The centre band is ignored because it has too small an area to be of any use. The radius of the sectoring was chosen to avoid the effects of circular convolution in applying a Gabor filter. Thus we have a total of 60 sectors (12 wedges × 5 bands). Another reason for sectoring is for normalization purposes. Each sector is individually normalized to a constant mean and variance to eliminate variations in darkness in the fingerprint pattern, due to scanning noise and pressure variations. All the pixels outside of the sector map are considered to

be one giant sector. This will yield in an image that is more uniform. The following equation is used for normalization of each pixel. A constant mean M_0 and variance V_0 are 100. i is the sector number, M_i is the mean of the sector, and V_i is the variance of the sector.

$$N_i(x,y)\begin{cases} M_0 + \sqrt{\dfrac{V_0\left(I(x,y)-M_i^2\right)}{V_i}}, & if\ I(x,y) \rangle M \\ M_0 - \sqrt{\dfrac{V_0\left(I(x,y)-M_i^2\right)}{V_i}}, & otherwise \end{cases} \qquad 6\text{-}14$$

6.10 Feature Extraction

Gabor Filtering

The normalized image is then passed through a bank of Gabor filters. Each filter is performed by producing a 33x33 filter image for 6 angles (0, π/6, π/3, π/2, 2π/3 and 5π/6), and convolving it with the fingerprint image. Spatial domain convolving is rather slow, so multiplication in the frequency domain is done; however, this involves more memory to store real and imaginary coefficients. The purpose of applying Gabor filters is to remove noise while preserving ridge structures and providing information contained in a particular direction in the image. The sectoring will then detect the presence of ridges in that direction. The Gabor filter has also an odd height and width to maintain its peak centre point. The following is the definition of the Gabor filter [122]:

$$G(x,y,f,\theta) = e^{-\frac{1}{2}\left\{\frac{x'^2}{\sigma_{x'}^2}+\frac{y'^2}{\sigma_{y'}^2}\right\}} \cdot \cos(2\pi f x') \qquad 6\text{-}15$$

where $x' = (x\cos\theta + y\sin\theta), y' = (-x\sin\theta + y\cos\theta)$ are rotated coordinates,

Feature Vector

After obtaining the 6 filtered images, the variance of the pixel values in each sector is calculated. This will reveal the concentration of fingerprint ridges directions in that part of the fingerprint. A higher variance in a sector means that the ridges in that image were going in the same direction as is the Gabor filter. A low variance indicates that the ridges were not, so the filtering smoothed them out. The resulting 360 variance values (6 × 60) are the feature vector of the fingerprint scan. The following is the equation for variance calculation. $F_{i\theta}$ are the pixel values in the ith sector after a Gabor filter with angle θ has been applied. $P_{i\theta}$ is the mean of the pixel values. K_i is the number of pixels in the ith sector.

$$V_{i\theta} = \sqrt{\sum_{K_i} \left(F_{i\theta}(x,y) - P_{i\theta}\right)^2} \qquad 6\text{-}16$$

The result will be three vector features for cropped images. A concatenation value of these vectors will formulate the final used feature (6-17).

$$V = V_1 \| V_2 \| V_3 \| \qquad 6\text{-}17$$

Where this vector is used as true data point to replace the minutiae points' feeder in Fuzzy vault scheme [45, 63-65] construction to generate the needed vault.

6.11 Simulation and Results

The proposed approach was implemented on the FVC2004-DB1 [17], a public domain database with 800 images (100 fingers 8 impressions each finger), cropped into 256x256 sizes, 500 dpi resolutions. True points were taken based on the concatenation extracted vectors from three cropped images, where the average of extracted vectors is 21. Chaff points were chosen to be 300 points, and point threshold distance adapted was 6. The constructed vault result is tested under all reconstruction parameters, like polynomial degree, minimum distance of point distribution, and vault complexity. Figure (6-17)

shows the relationship between polynomial degree and vault attack complexity where the used extracted feature points are 21 points while chaff points were chosen to vary from 100 to 300 points. Figure (6-18) shows the relationship between chaff points, minimum distance and release ability of locked key. The minimum distance was set to satisfy the following rules: chaff points cannot be placed too close to real points, no reason to place chaff points next to each others at any distance less than minimum distance, because the attacker can immediately ignore them as unlikely candidates.

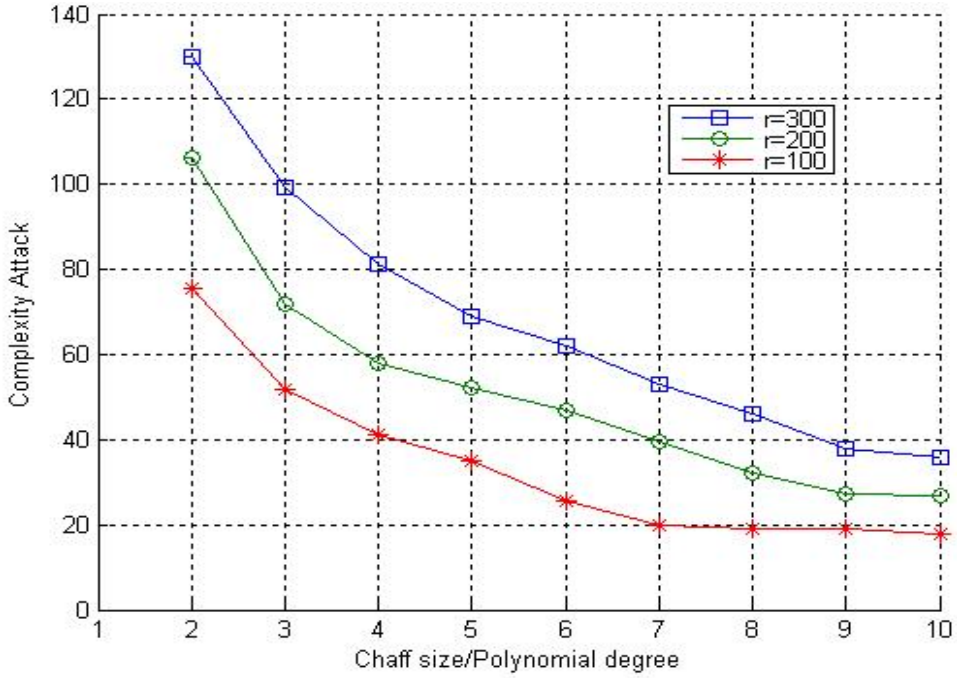


Figure 6-17 The attack complexity varies according to the degree of polynomial

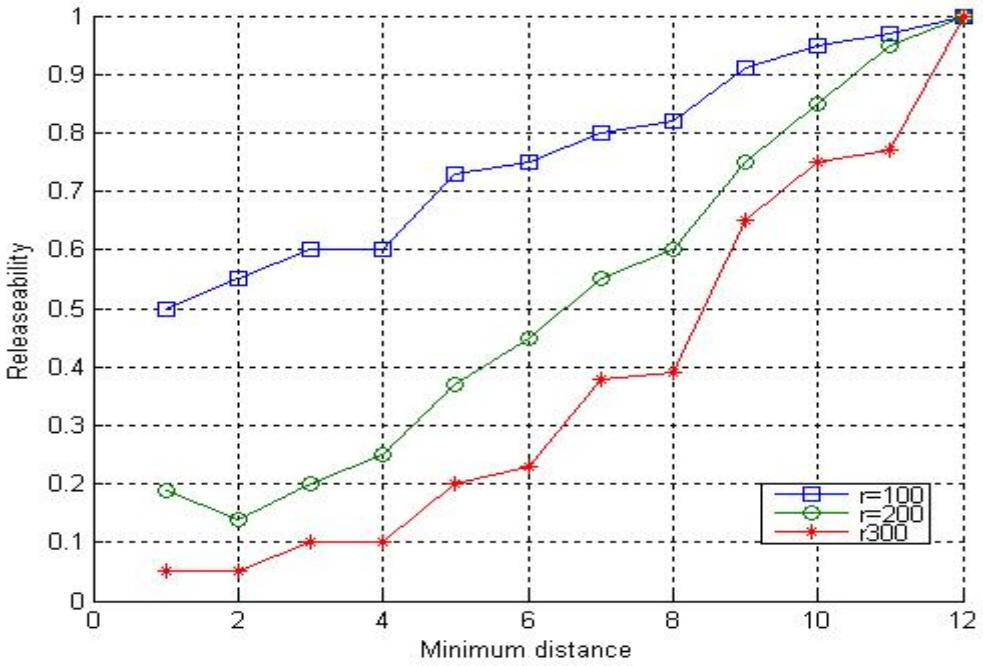


Figure 6-18 The relationship between the key releasability and the minimum distance.

6.12 Summary

Biometric systems are being widely used to achieve reliable user authentication and these systems will proliferate into the core information technology infrastructure. Therefore, it is crucial that biometric authentication is secure. Fuzzy vault is one of the most comprehensive mechanisms for secure biometric authentication and cryptographic key protection. Fuzzy vault cryptography key structure investigated for the reason to obtain and run the guidelines for appropriate vault parameters and system tolerance. A shielding technique "capsulation" was proposed to overcome fingerprint fuzzy vault key management and to increase strength of key against crack and attack possibilities. Practical fuzzy vault system based on fingerprint vector features was proposed. It can easily secure secrets such as 128-bit AES encryption keys.

Chapter 7 Conclusion and Future Work

7.1 Conclusion

Biometrics and cryptography have been seen as competing technologies and identified as two of the most important aspects of digital security environment. Working separately, the two technologies develop activities in isolation, sometime in competition with each other. For various types of security problems the merging between these aspects has led to the development of new bio crypt technology. Based on merging technique, the bio crypt categorized into: (i) loosely-coupled mode, the biometric matching is decoupled from the cryptographic part. Biometric matching operates on the traditional biometric template: if they match, the cryptographic key is released from its secure location, e.g. a server or smart card. (ii) tightly-coupled mode, 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. Bio crypt is giving hope to an ideal technology combination and security integration. The bio crypt process can be carried out in three different modes: key generation, binding and construction.

The biometric key generation usually suffer from low ability to discriminate which can be assessed in terms of key stability and key entropy. Key stability refers to the extent to which the key generated from the biometric data is usually repeatable. Key entropy relates to the number of possible keys that can be generated. While it is possible to derive a key directly from biometric features, it is difficult to simultaneously achieve high key entropy and high key stability.

In a key-binding mode, the biometric template is secured by monolithically binding it with a key within a cryptographic framework at the time of enrolment. A single entity that embeds both the key and the template is stored in the database. This entity does not

reveal much information about the key or the biometric template, i.e., it is impossible (or computationally infeasible considering cost and time limitations) to decode the key or the template without any knowledge of the user's biometric data. A bio crypt matching algorithm is used to perform authentication and key release in a single step.

Biometric cryptosystems that work in the key binding or generation ways are difficult to implement due to the large intra-class variations in biometric data, i.e., samples of the same biometric trait of a user obtained over a period of time can differ substantially. For example, in the case of fingerprints, factors such as translation, rotation, partial overlap, non-linear distortion, pressure and skin condition, noise and feature extraction errors lead to large intra-class variations.

The cryptographic construction mode is designed to work with biometric features which are represented as an unordered set. The ability to deal with intra-class variations in the biometric data along with its ability to work with unordered sets which is commonly encountered in biometrics makes the construction mode "Fuzzy vault" a promising solution for biometric cryptosystems.

The bio crypt key has the following benefits: (i) to increase the security of the system and (ii) to enhance the privacy issues related to the biometric template and extracted feature vectors. The bio crypt technology suffers from several limitations e.g. biometric image based quality, validity, image alignment, cancelability, key revoking and repeatability. The previous challenges affect the performance, accuracy and interoperability of any developed bio crypt system based.

To circumvent the biometric image quality problems, three new non reference algorithms were proposed:

- Fingerprint image validity check based on statistical weight calculation. It is statistically calculates the weight of the image base element (pixel). Image element describes an image object with the contrast, brightness, clarity and noising attributes. The value of these attributes is used to determine the image object properties and validity factors. The algorithm depends on fingerprint

object segmentation, background subtraction, total image threshold and pixel weight calculation.

- Fingerprint image quality assessment using Gabor spectrum analysis. This algorithm used local and global analysis level in evaluating fingerprint image. It uses Fourier spectrum analysis of Gabor features for non overlapping image blocks to determine the total fingerprint image quality. The benefit of this algorithm is concluded in deciding on the enrolment rejecting or accepting as well as on the type of image enhancements technique that is needed.

- A Hybrid Method for Fingerprint Image Validity and Quality Computation. Here both statistical and spectrum analysis are combined to detect the validity as well as the quality of tested image

The biometric template information was used to generate and construct revocable and cancelable key by:

- Contour graph algorithm, where the seed of fingerprint extraction phase (minutiae points) is used to construct graphical contours. The graph relation based on edges and vertices is used to formulate the adjacency matrix and the output matrix is processed by some mathematical operations to generate the final vector keys. The major novelty of this algorithm consists in keeping minutiae points away from several attacks as a first security level of bio crypt key generation life cycle.

- Slicing window algorithm used to generate encryption key from fingerprint sample. It uses slicing window to partitioning the area of extracted minutiae, then using the Euclidean distance between detected core point and extracted minutiae points for vector key generation. The derived biometric key can be used to encrypt a plaintext message and its header information. This algorithm eliminates the need for biometric matching algorithms and reducing the cost associated with lost keys.

- Biometric capsulation technique. Capsulation shields are used to protect biometric data and to overcome management key problem. The first shield of this technique is a generated random chaff points that used to hide the concatenating values of minutiae points coordination and formulating vault construct representation The vault construct is used as second shield to hide the secret key encoded message. The last shield is a portion of constructed vault that used as a header of encrypted file for reconstruction drawback.

- A cancellable feature vector vault. This algorithm used fingerprint feature vectors (FingerCode) to construct the fuzzy vault seed of bio crypt key. Finger code vector is composed of an ordered enumeration extracted features. The extracted feature is a result of image texture oriented components processed by Gabor filter banks. These features capture both global and local characteristic of fingerprint image. Extracted vectors are concatenating to final feature vector, and then this vector will be used to generate the fuzzy construct. The algorithm not only outputs high entropy keys, but also conceals the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is open to an attacker.

7.2 Future Work

This thesis addressed some limitations regarding bio crypt technology; there still remain a number of unresolved issues. Therefore, the following solutions could be further explored:

- Vulnerability of the bio crypt key against different attacks.

  The actual overall vulnerability of bio crypt architecture is typically made up of several areas of variable risk. If any of these areas are omitted within vulnerability assessment, then an unrepresentative conclusion will result. The vulnerability of bio crypt key to several types of attack could be an interesting issue to study and it

may help raising the security level of the bio crypt to cryptographic acceptable values.

- Fuzzy vault construct using combined biometrics.

  Fuzzy vault construction using combined biometrics, e.g. fingerprint minutiae, iris data will increase the capacity of cryptographic key and solve the key management problem. A combining multi mode biometric features is promising approach to enhance the vault security and reduce the false accept rate of the system without affecting the false reject rate. Employing multimodal biometric systems will overcome the accuracy and vulnerability limitations.

- Fuzzy construct computation complexity time reduction.

  Vault unlocking can be viewed in two contexts. The first is the complexity of a valid user unlocking a vault with a matching fingerprint image. The second context is the complexity of an attacker without fingerprint information trying to crack the vault. Using combine error correction codes with stable and ordered multi mode biometric templates will maximize attacking complexity and reduce valid user unlocking computation complexity that could be promising future research.

- Automatic alignment within the fuzzy vault construction.

Bio crypt based system has several advantages over traditional password based systems. Bio crypt vault aims to secure critical data (e.g. secret encryption key) with the fingerprint data in a way that only the authorized user can access the secret by providing the valid fingerprint, and some implementations results for fingerprint vault have been reported. However, all the previous results assumed that fingerprint features were pre-aligned, and automatic alignment in the fuzzy vault domain is open and challenging issue, therefore, integrating align fingerprint features in the domain of the fuzzy fingerprint vault systems could be future research direction.

References:

[1] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints," *IEEE Transactions on PAMI*, vol. Vol. 24,, pp. 1010-1025, 2002.

[2] A. K. Jain and D. Maltoni, *Handbook of Fingerprint Recognition*: Springer-Verlag New York, Inc., 2003.

[3] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*: Kluwer Academic Publishers, 1998.

[4] D. D. Zhang, *Automated Biometrics: Technologies and Systems*: Kluwer Academic Publishers, 2000.

[5] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, pp. 948-960, 2004.

[6] A. Jain, L. Hong, and R. Bolle, "On-Line Fingerprint Verification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, pp. 302-314, 1997.

[7] A. C. Leniski, R. C. Skinner, S. F. McGann, and S. J. Elliott, "Securing the biometric model," presented at Security Technology. Proceedings of the 37th IEEE Annual 2003 International Carnahan Conference, 2003.

[8] B. Scheneier, *Applied Cryptography*, 2nd ed: John Wiley & Sons,New York, 1996.

[9] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*: CRC Press, Inc., 1996.

[10] W. Stallings, *Cryptography and Network Security: Principles and Practice*: Prentice Hall College, 2006.

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

[12] 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.

[13] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "Crypto key generation using contour graph algorithm " in *Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition, and applications* Innsbruck, Austria ACTA Press, 2006 pp. 95-98

[14] M. S. Altarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "Crypto Key Generation Using Slicing Window Algorithm," presented at 5th IEEE Symposium on Communication Systems, Networks and Digital Signal Processing(CSNDSP'06), Patras, Greece, July 19-21, 2006.

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

[16] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, pp. 1494-1498, 2003.

[17] M. S. ALTARAWNEH, L.C.KHOR, W.L.WOO, and S.S DLAY, "A NON Reference Fingerprint Image Validity Check," presented at DCCA 2007, Jordan, Irbid, March, 2007.

[18] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "A NON Reference Fingerprint Image Validity via Statistical Weight Calculation," *Digital Information Management*, vol. 5, pp. 220-224, August,2007.

[19] M. S. ALTARAWNEH, W.L.WOO, and S.S DLAY, "OBJECTIVE FINGERPRINT IMAGE QUALITY ASSESSMENT USING GABOR SPECTRUM APPROACH," presented at DSP 2007, Wales, UK, 2007.

[20] M. S. AlTarawneh, W. L. Woo, and S. S. DLAY, "A Hybrid Method for Fingerprint Image Validity and Quality Computation," presented at The 7th WSEAS International Conference on SIGNAL PROCESSING, ROBOTICS and AUTOMATION (ISPRA '08), Cambridge, UK, February 20-22, 2008.

[21] "http://bias.csr.unibo.it/fvc2004/default.asp."

[22] "Micro and Nano Systems (MNS) research group at TIMA laboratory in Grenoble, France," http://tima.imag.fr/mns/research/finger/fingerprint/index.html.

[23] E. Lim, X. Jiang, and W. Yau, "Fingerprint quality and validity analysis," presented at Proc. IEEE int. Conf. On image Processing, ICIP, Sept.2002.

[24] E. Lim, K.-A. Toh, P. N. Suganthan, X. Jiang, and W.-Y. Yau, "Fingerprint image quality analysis," presented at Image Processing, 2004. ICIP '04. 2004 International Conference on, 2004.

[25] L. Shen, A. Kot, and W. Koo, "Quality Measures of Fingerprint Images,," *Lecture Notes in Computer Scienc*, vol. Volume 2091, pp. 266, 2001.

[26] J. Qi, D. Abdurrachim, D. Li, and H. Kunieda, "A Hybrid Method for Fingerprint Image Quality Calculation," in *Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies*: IEEE Computer Society, 2005, pp. 124-129.

[27] N. B. Nill and B. H. Bouzas, "Objective image quality measure derived from digital image power spectra," *Optical Engineering*, vol. 31, pp. 813-825, April 1992.

[28] N. B. Nill, "IQF (Image Quality of Fingerprint) Software Application," http://www.mitre.org/work/tech_papers/tech_papers_07/07_0580/07_0580.pdf.

[29] Y. Chen, S. Dass, and A. K. Jain, "Fingerprint quality indices for predicting authentication performance," presented at AVBPA, Rye Brook, NY, July 2005.

[30] B. Lee, J. Moon, and H Kim, "A novel measure of fingerprint image quality using the Fourier spectrum," *Proceedings of the SPIE*, vol. 5779, pp. 105-112, 2005.

[31] S. Joun, H. Kim, Y. Chung, and D. Ahn, "An Experimental Study on Measuring Image Quality of Infant Fingerprints," *LNCS*, vol. 2774, pp. 1261-1269, 2003.

[32] N. K. Ratha and R. Bolle, "Fingerprint Image Quality Estimation," presented at ACCV, Taipei, Jan 2000.

[33] N. K. Ratha and R. Bolle, *Automatic Fingerprint Recognition Systems*: SpringerVerlag, 2003.

[34] M. Y. Yao, S. Pankanti, N. Haas, N. K. Ratha, and R. M. Bolle., "Quantifying Quality: A Case Study in Fingerprints," presented at Proc. of IEEE on Automatic Identification Advanced Technologies (AutoID), March, 2002.

[35] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint image quality," NIST research report NISTIR7151, August, 2004.

[36] E. Tabassi, C. Wilson, and C. Watson, "NSIT Fingerprint Image Quality," presented at Biometric Consortium Conference, Arlington, VA, U.S.A, September 20, 2005.

[37] "NIST FINGERPRINT IMAGE SOFTWARE 2," http://www.nist.gov/.

[38] E. Zhu, J. P. Yin, C. F. Hu, and G. M. Zhang, "Quality Estimation of Fingerprint Image Based on Neural Network," presented at Proceedings of International Conference on Natural Computing. LNCS, 2005.

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

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

[41] J. Daugman, "Biometric decision landscapes," TR482, University of Cambridge, UK, 2000.

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

[43] A. Stoianov, C. Soutar, and A. Graham, "High-speed fingerprint verification using an optical correlator," *Proc. SPIE*, vol. 3386, pp. 242-252, 1998.

[44] 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.

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

[46] A. Adler, "Vulnerabilities in Biometric Encryption Systems," presented at Audio- and video-based Biometric Person Authentication (AVBPA). 2005.

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

[48] G. I. Davida, Y. Frankel, B. J. Matt, and R. Peralta, "On the relation of error correction and cryptography to an offline biometric based identification scheme," presented at Workshop Coding and Cryptography (WCC'99), 1999.

[49] J. G. Daugman, " High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, vol. 15, pp. 1148–1161, 1993.

[50] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometrics Effectively," *IEEE Transactions on Computers*, vol. 55, pp. 1081-1088, 2006.

[51] 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.

[52] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic Key Generation from Voice," presented at Proceedings of the 2001 IEEE Symposium on Security and Privacy, 2001.

[53] 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.

[54] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Using Voice to Generate Cryptographic Keys," presented at A Speaker Odyssey, The Speech Recognition Workshop, Crete, Greece, 2001.

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

[56] 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.

[57] 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.

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

[59] W. Zhang, Y.-J. Chang, and T. Chen, "Optimal thresholding for key generation based on biometrics," presented at International Conference on Image Processing, 2004.

[60] 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.

[61] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*: ACM Press, 1999, pp. 28-36.

[62] S. Lin, *An Introduction to Error-Correcting Codes*. Englewood Cliffs: Prentice-Hall, 1970.

[63] 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.

[64] U. Uludag and A. K. Jain, "Fuzzy Fingerprint Vault.," presented at Workshop: Biometrics: Challenges Arising from Theory to Practice, Cambridge, UK, 2004.

[65] 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.

[66] U. Uludag and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Helper Data " in *Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop* IEEE Computer Society, 2006 pp. 163

[67] 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.

[68] 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.

[69] 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.

[70] B. M. Mehtre and B. Chatterjee, "Segmentation of fingerprint images - a composite method," *Pattern Recogn.*, vol. 22, pp. 381-385, 1989.

[71] N. Ratha, S. Chen, and A. Jain, "Adaptive flow orientation based feature extraction in fingerprint images," *Pattern Recognition*, vol. 28, pp. 1657-1672, Nov. 1995.

[72] A. K. Jain, N. K. Ratha, and S. Lakshmanan, " Object Detection Using Gabor Filters," *Pattern Recognition*, vol. 30, pp. 295-309, 1997.

[73] A. M. Bazen and S. H. Gerez, "Directional field computation for fingerprints based on the principal component analysis of local gradients," presented at ProRISC2000, 11th Annual Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, Nov. 2000.

[74] 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.

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

[76] N. Otsu, "A Threshold Selection Method from Gray-Level Histograms," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 9, pp. 62-66, 1979.

[77] L. Hong, Y. Wan, and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, pp. 777-789, 1998.

[78] F. Alonso-Fernandez, J. Fierrez-Aguilar, and J. O.-. Garcia, "A review of schemes for fingerprint image quality computation," presented at 3rd COST- 275 Workshop, Biometrics on the Internet, European Commission, 2005.

[79] T. D. K. Niranjan Damera-Venkata, Wilson S. Geisler, Brian L.Evans and Alan C.Bovik, "Image Quality Assessment Based on a Degradation Model," *IEEE Transactions on Image Processing*, vol. VOL 9, pp. 636-650, 2000.

[80] Z. Wang and A. C. Bovik, *Modern Image Quality Assessment*: Morgan & Claypool, 2006.

[81] E. Tabassi and C. L. Wilson, "A novel approach to fingerprint image quality," presented at IEEE International Conference on Image Processing, 2005.

[82] Y. Chen, S. Dass, and A. Jain, "Fingerprint Quality Indices for Predicting Authentication Performance.," presented at Audio-and-Video-based Biometric Person Authentication, Rye Town, NY, 2005.

[83] K. Uchida, " Image-Based Approach to Fingerprint Acceptability Assessment," in *Lecture Notes in Computer Science*: Springer Berlin / Heidelberg, 2004, pp. 294-300.

[84] T. Ko and R. Krishnan, "Monitoring and reporting of fingerprint image quality and match accuracy for a large user application," presented at 33rd Applied Imagery Pattern Recognition Workshop, 2004.

[85] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*: Prentice-Hall, Inc., 2002.

[86] A. C. Bovik, *Handbook of Image and Video Processing*: Academic Press, Inc., 2005.

[87] I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image. quality measures," *Electronic Imaging*, vol. 11, pp. 206-223, 2002.

[88] R. J. Safranek, T. N. Pappas, and J. Chen, "Perceptual Criteria for Image Quality Evaluation," A. Bovik, Ed.: Academic Press, 2004.

[89] S. Daly, "The visible differences predictor: an algorithm for the assessment of image fidelity " in *Digital images and human vision* MIT Press, 1993 pp. 179-206

[90] A. M. Eskicioglu, "Quality measurement for monochrome compressed images in the past 25 years," presented at Acoustics, Speech, and Signal Processing, 2000. ICASSP '00. Proceedings. 2000 IEEE International Conference on, 2000.

[91] M.S. Altarawneh, L.C.Khor, W.L.Woo, and S. S. Dlay, "A NON Reference Fingerprint Image Validity via Statistical Weight Calculation," *JOURNAL OF DIGITAL INFORMATION MANAGEMENT*, vol. 5, 2007.

[92] H. R. Sheikh, M. F. Sabir, and A. C. Bovik, "A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms," *Image Processing, IEEE Transactions on*, vol. 15, pp. 3440-3451, 2006.

[93] M. Carnec, P. Le Callet, and D. Barba, "Full reference and reduced reference metrics for image quality assessment," presented at Seventh International Symposium on Signal Processing and Its Applications, 2003.

[94] H. Fronthaler, K. Kollreider, J. Bigun, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Fingerprint image quality estimation and its application to multi-algorithm verification.," Technical Report IDE0667 Technical Report IDE0667,2006.

[95] Z. Wang, A. C. Bovik, and L. Lu, "Why is image quality assessment so difficult?," presented at IEEE International Conference on Acoustics, Speech, and Signal Processing, 2002.

[96] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, J. Fronthaler, K. Kollreider, and J. Bigun, "A Comparative Study of Fingerprint Image-Quality Estimation Methods," *IEEE Transactions on Information Forensics and Security*, vol. 2, pp. 734-743, 2007.

[97] L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE transaction on pattern analysis and machine intelligence*, vol. 20, 1998.

[98] L. L. Shen, A. Kot, and W. M. Koo, "Quality Measures of Fingerprint Images," presented at Third AVBPA, June 2001.

[99] A. K. Jain and F. Farrokhnia, "Unsupervised texture segmentation using Gabor filters," *Pattern Recognition*, vol. Vol. 24, pp. 1167-1186, 1991.

[100] C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, and S. Janet, *Users Guide to Fingerprint Image Software 2 - NFIS2. NIST*, 2004.

[101] "Final report from the video quality experts group on the validation of objective models of video quality assessment, phase II, March 2003.."

[102] "VeriFinger Software," http://www.neurotechnologija.com.

[103] W. Stallings, *Cryptography and Network Security*, 4 ed: Prentice Hall, 2006.

[104] M. S. Altarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, "CRYPTO KEY GENERATION USING SLICING WINDOW ALGORITHM," presented at CSNDSP, Patras, Greece, 2006.

[105] L. Hong, "Automatic personal identification using fingerprints," Michigan State University, 1998, pp. 227.

[106] B. Bhanu and X. Tan, *Computational Algorithms for Fingerprint Recognition*: Kluwer Academic Publishers, 2004.

[107] P. E. Black, *Dictionary of Algorithm and Data Structure, NIST*, 2004.

[108] N. Ratha, S. Chen, and A. Jain, "Adaptive flow orientation-based feature extraction in fingerprint images," *Pattern Recognit*, vol. 28, pp. 657-1672, 1995.

[109] M. D. Garris, C. I. Watson, R. M. McCabe, and C. L. Wilson, *User's Guide to NIST Fingerprint Image Software (NFIS), NISTIR 6813*, 2001.

[110] K. Nilsson and J. Bigun, "Localization of corresponding points in fingerprints by complex filtering," *Pattern Recognition Letters*, vol. 24, pp. 2135-2144, 2003.

[111] K. Nilsson and J. Bigun, "Localization of corresponding points in fingerprints by complex filtering," *Pattern Recogn. Lett.*, vol. 24, pp. 2135-2144, 2003.

[112] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, vol. 14, pp. 4-20, 2004.

[113] "Biometrics Market and Industry Report 2007-2012," http://www.biometricgroup.com/reports/public/market_report.html.

[114] A. Kiayias and M. Yung, "Directions in Polynomial Reconstruction Based Cryptography," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. E87-A,no 5, pp. 978-985, 2004.

[115] A. Kiayias and M. Yung, "Polynomial Reconstruction Based Cryptography " in *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography* Springer-Verlag, 2001 pp. 129-133

[116] A. Houghton, *Error Coding for Engineers*: Kluwer, 2001.

[117] A. Kiayias and M. Yung, "Cryptanalyzing the polynomial-reconstruction based public-key system under optimal parameter choice,," presented at 10th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2004), Lecture Notes in Computer Science, Jeju Island, Korea, 2004.

[118] S. Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme," presented at Acoustics, Speech, and Signal

Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on, 2005.

[119] S. YOICHI, M. MASAHIRO, T. KENTA, N. ITSUKAZU, S. MASAKAZU, and N. MASAKATSU, "Mechanism-based PKI : A Real-time Key Generation from Fingerprints," *Transactions of Information Processing Society of Japan*, vol. 45, pp. 833-1844, 2004.

[120] E.-C. Chang, R. Shen, and F. W. Teo, "Finding the original point set hidden among chaff," presented at ACM Symposium on Information, computer and communications security, Taipei, Taiwan, 2006.

[121] S. Prabhakar, "Fingerprint Classification and Matching Using a Filterbank," in *Computer Science & Engineering*: Michigan State University, 2001, pp. 259.

[122] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, " Filterbank-based Fingerprint Matching," *IEEE Transactions on Image Processing*, vol. 9, pp. 846-859, 2000.