Fingerprint Template Protection using Encrypted Fuzzy Vault

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

Master of Engineering
in
Software Engineering

Submitted By
Shamsher Singh Dhillon
(Roll No. 801531013)

Under the supervision of:
Dr. Vinod K. Bhalla
Assistant Professor
Computer Science and Engineering Department

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA-147004

July 2017

Certificate

I hereby declare that this thesis entitled, "*Fingerprint Template Protection using Encrypted Fuzzy Vault*" which is presented in partial fulfillment of the requirements for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, contains literature survey and original research work by the undersigned candidate under the guidance of Prof. Vinod K. Bhalla.

I also declare that, as required by the rules and conduct, I have fully cited and referenced all the material and results that are not original to this work and the matter presented in this thesis has not been submitted for award of any other degree of this or any other University.

Shamsher

Shamsher Singh Dhillon

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Vinod Kumar Bhalla)

(Assistant Prof, CSED)

Acknowledgement

I would like to express my gratitude to my supervisor, **Dr. Vinod K. Bhalla**, whose expertise, understanding, and patience, added considerably to my graduate experience. I appreciate his vast knowledge and skill in many areas, and his assistance in writing reports. Prof. Bhalla was always available whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right the direction whenever he thought I needed it.

I would also like to acknowledge **Dr. Maninder Singh** of the Associate Professor and Head, Computer Science & Engineering Department for motivation and providing uncanny guidance and support throughout the preparation of the thesis report.

Finally, I must express my very profound gratitude to my parents, my sister and to my friends at Thapar University, Patiala especially Amritinder Cheema for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them.

Thank you.

Shamsher Singh Dhillon

Abstract

Fingerprints are by far the most popular biometric features in authentication systems because of their capability to satisfy implementation specifications. Throughout the last two decades, exploration in fingerprint-based authentication systems has observed incredible development. Lately, fingerprints are already employed to authenticate individuals remotely enabling them to access a system. For example, smart phones now have an embedded fingerprint scanner to authenticate a user. Although fingerprints are now being used extensively to protect information as well as for the process of authentication, even the biometric systems are vulnerable to attacks. Some of these attacks may be targeted to the system while other may be carried out with the intention of stealing biometric information of users of the biometric systems. Due to the value of biometric information in recent times, it must be ensured that the biometric information of the users stored in the system is secure and even during a case of a break-in, the users and their information is protected. There has been some research in this area and certain promising methods have been proposed to secure the biometric information in a biometric system. In this thesis, we present such a technique that can be potentially used to protect the biometric information of the users.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

During the late nineteenth century, Alphonse Bertillon, a policeman of French origin is known to be the first person to identify a person on the basis of his anatomical and behavioural features. He also manufactured tools, collectively known as Bertillonage system, in order to identify repeat offenders. This system involved measuring certain traits of person including length of head, breadth of head, and length of fingers as shown in Fig. 1.1.

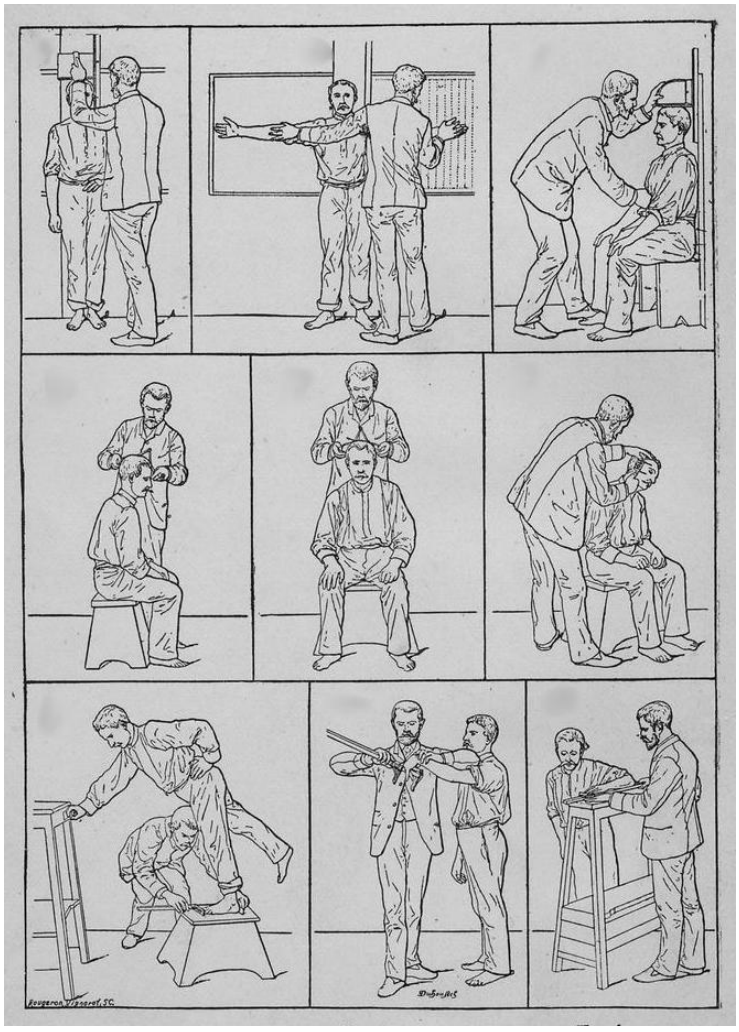


Figure 0.1 Bertillonage System Instructional Diagram

After Bertillonage system, Galton [1], Herschel [2] and Faulds [3] noticed that the patterns present on the fingertips of an individual are significant and can be used to identifying an individual from another. Their studies proved to be the ignition point for the development of the fingerprint matching systems that were reliable enough to replace the less accurate Bertillonage System. The fingerprints in such system were manually matched by fingerprint experts but with the advancements in the computing technologies, efforts were started during the 1960's to automate the whole process (acquiring, matching and storing) of fingerprints [4] ,[5]. Alongside fingerprints, systems were also being developed to automate the process of matching other anatomical traits such as face [6], palmprints [7], iris [8], etc. These traits which are capable of identifying a person uniquely are called biometric traits and the science of acquiring, storing and matching such traits is known as biometric recognition.

With the advancement in techniques and tools to process biometrics in real time, we now have the ability to use biometrics as a mean of user authentication. Biometrics are now being used in real life applications like computer system log-ins, Aadhaar card validation, and even college registrations. All of these applications required the user to either remember a password or carry some tokens like smartcards or NFC cards in order to identify themselves. Biometrics have got many advantages over these traditional security methods. Unlike passwords, Biometrics are a part of an individual and cannot be stolen. Also, since biometrics are something that you are, we need not to carry something alongside to prove our identity. At present, such biometric recognitions systems are being used extensively in government as well as private sectors.

1.1. Biometric Recognition Systems

A biometric recognition system is a system based on pattern recognition that specialises in recognizing individuals on the basis of their biometric traits. These traits may be any of the following: fingerprints, palmprints, iris, face or even a mixture of any of these traits. Any biometric recognition system basically consists of four modules. Each of these modules is responsible for a certain task. These tasks are:

i) Capturing samples of biometric trait.
ii) Extraction of features from the captures sample.
iii) Strong the extracted features into a system database.

iv) Matching the features from a biometric sample with samples enrolled in the database of the biometric system.

The steps involved in biometric enrolment and biometric matching have been illustrated in Fig. 1.2. and Fig. 1.3. respectively.

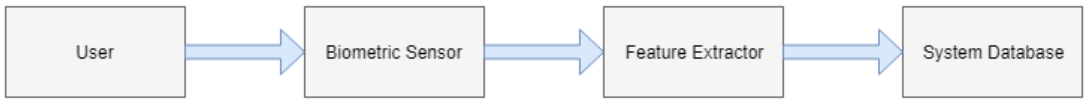


Figure 0.2 Biometric Enrolment Process

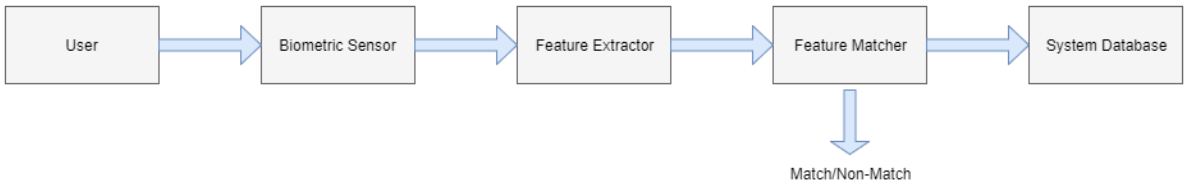


Figure 0.3 Biometric Matching Process

Some of the terminology related to a biometric system:

- **Biometric trait:** As discussed above, biometric trait is an anatomical or behavioural trait that is being used for processing and matching the identification of a person. Examples are fingerprint, iris and face.
- **Biometric instance:** Biometric trait's specific instance like left eye or left middle finger.
- **Biometric sample:** The snapshot or image biometric instance of an individual as captured by the biometric sensor.
- **Biometric template:** The storage of the features extracted from the biometric sample of an individual.
- **Biometric query:** A biometric sample provided by an individual for the process of identification or verification. Biometric template is extracted from this sample and matched against the templates that are already stored in the system database.
- **System threshold:** The minimum limit imposed on the result of the matching process in order to decide if the query can be considered a genuine query or not.

A biometric system usually operates in two modes. These modes are:

Identification: In the identification mode of operation, the user provides only a biometric signature to the system without claiming any identity. This signature is passed through the extraction process to obtain the biometric features of the signature. These extracted features are then matched with all the available templates stored in the database. If the features of a query signature match any of the stored templates, a match is declared; otherwise the system declares a non-match. In addition to the result of the matching process, the identity of the user may also be displayed. This mode of operation is useful when we need to find the identity of a person from a sample of a biometric.

Verification: In verification mode of operation, the user himself provides his identity along with a sample of his biometric signature. This biometric signature is then passed on to the extraction phase to obtain features that are unique to the signature. These features are then matched with the features that are stored against the identity that is claimed by the user. If the matching process is a success, the user is granted access and denied otherwise. Most of the commercially used biometric systems operate in verification mode. This mode of operation is generally used when we need to verify that the person demanding authorization is actually the person that has the authorization.

1.2. System Vulnerabilities

Biometric recognition systems are a huge step forward to traditional security systems but even these systems are prone to security issues. The issue may be due to a deliberate attack by an intruder or an inadvertent security lapse but it can lead to a forced access to the system, denial of service to users or theft of the biometric data of the enrolled users. These types of security lapses usually occur because of factors belonging to one of the following categories: intrinsic failures, administrative privileges, non-secure infrastructure, and access to biometric data.

1.2.1 Intrinsic Failures

Due to non-rigid and genetic nature of the biometric traits along with the variations in the imaging conditions, the captured biometric images and thus features extracted from these images may result in variabilities. As an

example, the fingerprint image of the same finger of an individual may result in slightly different images and hence features. See e.g. Figure 1.4. where two very different fingerprints obtained from the same finger are shown. These variations may lead to incorrect decision during the process of template matching. Such kind of failures are usually determined by metrics such as false acceptance rate (FAR)and false matching rate (FMR).

Figure 0.4 Two fingerprints from the same finger having large variation in the portion of the finger printed.

FMR quantifies the false matching rate while FAR quantifies the frequency with which an intruder was provided access to the system.

Further, if the quality of the image acquired from the user during the time of matching is not acceptable, the system would practically be unavailable for the user. An example would be a user wearing a band-aid on the registered finger while trying to authenticate himself using a fingerprint recognition system.

1.2.2 Administrative Privileges

The system administrators mostly have the authority to make an exception in case a person is incapable of identify him/her using the required biometric traits possibly due to an injury or disease. This intruder can abuse this functionality of the system by colluding with or by coercing the system administrator in order to gain access to the system. In another scenario, the intruder can also be given access to the system by an enrolled user. The enrolled user may do this willingly or unknowingly (e.g. Biometric door lock

system). In order to limit such scenarios, the administrators of the system should be made anonymous and the users accessing the system should be logged carefully.

1.2.3 Non-Secure Infrastructure

The hardware infrastructure of the system can also be exploited by the attacker. Such attacks are categorized into four main categories:

1.2.3.1 User Interface Attacks

A biometric system usually has of a user interface that comprises of a biometric sensor that acquires the biometric signature from the user and passes the information to the feature extraction module. An adversary can damage this biometric sensor with the intention of gaining access to the system by some other less secure authentication methods. The intruder can also try to replicate the biometric trait of the legitimate user in order to gain access to the system. In case of an identification system, the intruder may also try to modify his personal biometric signature so as to avoid being identified with his enrolled template.

In order to minimize the impact of such results, the sensor should be made robust to any attempt that is made to damage the sensor. Also, the liveness detection techniques can be implemented in order to detect spoof biometrics.

1.2.3.2 Module Interface Attacks

In case of an insecure communication channel between the modules, a *man-in-the-middle* attack can be staged by an adversary to intercept or replace the information that is being transferred from one module to another. Such an attack can help the adversary to obtain the biometric information of an enrolled user or inject some malicious information of himself to change the stored information in the system. The first case would allow the adversary to access the system as a legitimate user

without raising any alarms while the second case would allow the adversary to bar any legitimate user from accessing the system.

Such attacks can be avoided by encrypting the information before it is being transmitted from one module to another.

1.2.3.3 Attacks on software modules

A system module can be damaged by an attacker by injecting a virus that provides the attacker with the ability to change the output of the module according to his desires. If an attacker is familiar with the architecture of the system module, he can also leverage from any arithmetic loopholes that may be present in the software. An example would be where a system is unable to activate the matching module for a few second after an outage. An attacker can exploit such a loophole to gain illegitimate access to the system.

Such attacks can be avoided by studying the system thoroughly and analysing and securing all the possible entry points into the system.

1.2.3.4 Attacks on the template database.

If the template database in unsecured and un-encrypted, the attacker can replace the biometric template of a legitimate user with his own so as to gain access to the system. Also, the attacker can extract the biometric template of a user and generate a spoof biometric trait by using a template inversion technique. This spoof biometric can then be used at any place where the original user had registered using that biometric trait.

1.2.4 Access to biometric traits

The last vulnerability of a biometric system arises from the fact that all the biometric features that are used in such systems are not a secret and hence can be covertly captures without the knowledge of the user. This captured biometric data can be used for a number of nefarious purposes as explained in Section 1.3. Although it is not very difficult for an adversary to access biometric traits of individuals in public, it is usually difficult to ascertain the digital identity of the person whose biometric data has been captured.

Furthermore, it is usually easier and safer for an attacker to hack into a system database and obtain biometric information about a large number of individuals along with their identifying information. The security of templates stored in the biometric systems is thus important.

1.3. Template Compromise Consequences

An adversary can use the information obtained from the system database in a number of ways.

1.3.1 Database Linkage

If an attacker is able to obtain templates from more than one databases, he can check if two set of templates belong to a single person. This provides the attacker with the ability to track the user. Also, the enrolled user may have different information related to him in different databases. If an adversary is able to link all these databases that use the biometric signature of the user, it may enable him to prepare for a serious identity theft attack.

1.3.2 System Intrusion

An adversary can obtain access to a biometric system with the help of a stolen biometric template by three methods: spoof construction, template replay and targeted false accepts.

Spoof construction: As discussed in the previous section, an adversary can use one of the various template inversion techniques to regenerate a replica of an original biometric trait and use this replica to gain access to any system where original user is enrolled.

Template replay: The adversary can implant the compromised signature into another system where the user whose biometric has been stolen is already enrolled. This would allow the adversary to gain access to the second system too.

Targeted false accepts: If the user has access to the system database, he can replace the biometric template stored in the database with his own. This would provide the adversary to easily masquerade as the legitimate user and access the system illegitimately.

1.4. Biometric Template Protection Techniques

Traditionally, digital data is protected with the help of passwords, however, in the case of biometric templates, protection using passwords is not the best approach. First, biometrics are used for the sake of convenience. So, remembering passwords in order to decrypt the biometric templates undermines the convenience provided by the biometric systems. Second, the strength of security that a password provides is not enough to protect biometric templates. In order to properly secure data, the password needs to be lengthy as well as complex which again conflicts with the convenience aspect of the biometric systems.

A number of hardware as well as software solutions have been proposed for the protection of the biometric templates. The hardware solutions mostly require construction of a *gapped* recognition system. A system that does not have any interaction with other networks or the internet. An example of such a solution is a commercial product known as privaris PlusID [9]. In this product, all the modules (sensor, matcher, database) of a recognition system are enclosed in a single device. During enrolment, a template is generated by the biometric sensor. This template is stored on the database that exists on the device itself. During authentication, if the query captured by the biometric sensor matches the template that is stored on the device, a key is transmitted to, say, an access control system (e.g. a garage door) that can be opened or closed based on the key that it receives. One of the main limitations of these hardware based solutions is that they are expensive and inconvenient since the user has to carry them and are susceptible to being lost.

Figure 0.5 Privaris PlusID

In the software based techniques, the sensitive biometric templates are generally combined with an external key, such as a password or a system generated random number and resultant data is stored into a database instead of the biometric template. It is expected that the resultant data reveals little information about the original template. Based on the technique used for matching, the software based template protection techniques can be classified into three main categories: Encryption, Biometric cryptosystems, and Template transformation. Figures 1.6.,1.7., and 1.8. show a schematic representation of the three categories.

1.4.1 Encryption

In encryption based technique, an encryption key is used to encrypt the biometric template. This key is usually generated from a password when the user is enrolled. During authentication, encrypted data that is stored in the database is decrypted by using a related decryption key and the result is then compared to the query template (see Fig. 1.6.). Encryption of the biometric can be performed using two different techniques: symmetric encryption and asymmetric encryption. Symmetric encryption, for instance Advanced Encryption Standard (AES) [10], is in fact the most basic kind of encryption in which the encryption and decryption keys are identical. When it comes to asymmetric encryption, the encryption key is different from the decryption key and it is hard to obtain one from the other. In this type of encryption, since the encryption key could possibly be dumped right after encrypting the biometric template, the intruder will never be able to swap the prevailing template with his own even if he knew the decryption key.

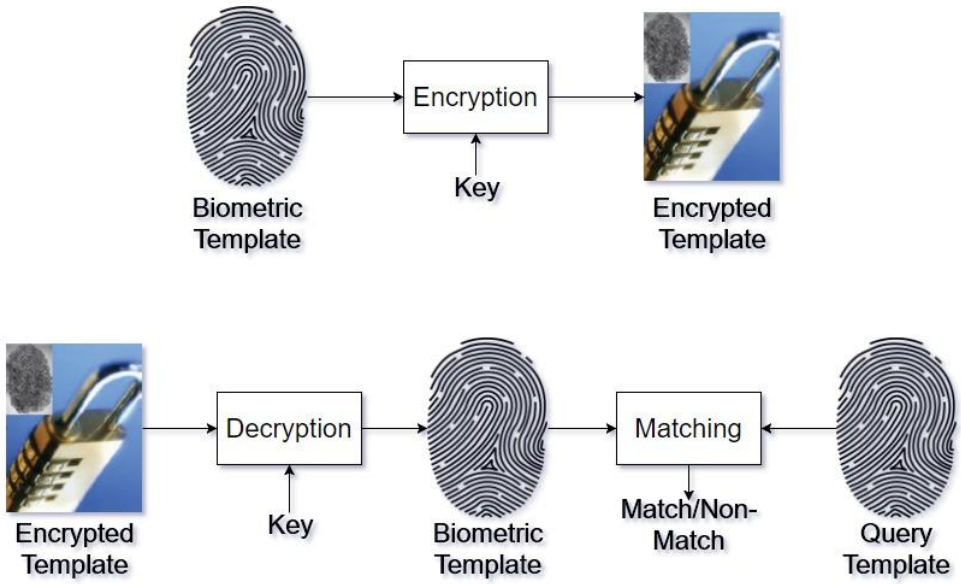


Figure 0.6 Schematic diagrams for enrolment(above) and authentication(below) stages of encryption.

This is helpful in solving the issue of *targeted false accepts* explained in the previous section. One of the main limitations of encryption technique is that at the time of matching the decryption key is exposed each time and thus can be easily stolen if the intruder is familiar with the system and its working. The main advantage however is that any sophisticated matching algorithm can be employed thereby preserving matching accuracy.

1.4.2 Biometric cryptosystems

This is the second software based technique for biometric template security. In a typical biometric cryptosystem, the system obtains a so called secure sketch or helper data using a key associated with the biometric data. This specific helper data will not expose any details regarding the biometric template.

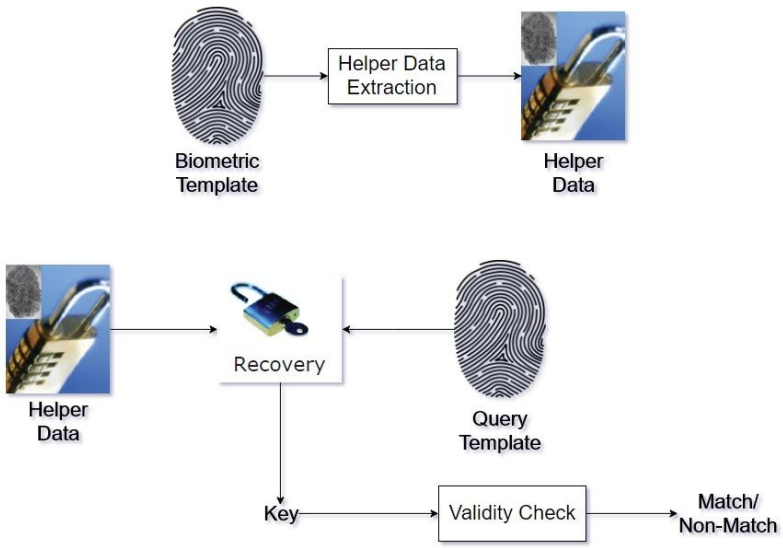


Figure 0.7 Schematic diagrams for enrolment(above) and authentication(below) stages of Biometric Cryptosystems.

While in authentication, data from the query template is used to get original biometric signature stored in the database. This is done with the help of helper data and the precise restoration of the original biometric data is validated in order to authenticate a user (see Fig. 1.7.).

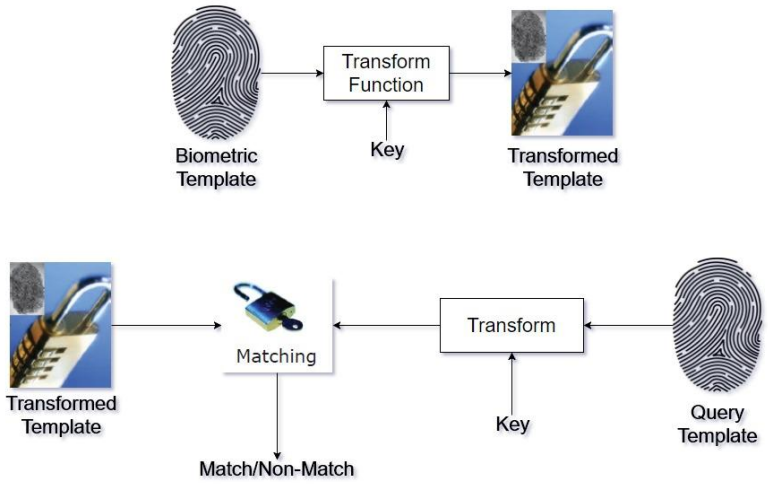


Figure 0.8 Schematic diagrams for enrolment(above) and authentication(below) **stages of Template Transformation.**

One of the advantages of this technique is that the retrieval of the original biometric data enables a system architect to use this data as an encryption key in another cryptosystem.

	Encryption	Biometric Cryptosystem	Template Transformation
Description	Encryption of template; decryption before authentication	Bind a key to biometric to obtain secure sketch; recover key or original biometric for verification	Transform template using password; query also transformed before matching
Match Criteria	Score (Original Biometric)	Key recovery	Score (Transformed Biometric)
Access to Biometric	During Authentication attempt	After accept decision	Never
User's Responsibility	Provide biometric	Provide biometric	Provide biometric and password
System's Responsibility	Key storage	Keep key safe after accept decision	None
Main Advantage	Performance	Provides key management	Non-linkability
Main Disadvantage	Key management	Linkability	Weak security

Table 1 Characteristics of software based template protection techniques.

1.4.3 Template transformation

In this technique, the biometric template is transformed with the help of a user specified password at the time of enrolment. This transformed template is stored in the database. At the time of authentication, the same password is used to transform the query template before matching it with the stored template (see Fig. 1.8.).

This technique usually makes use of geometric (planer or polar) transformations involving projections onto a new space which is determined by the user specified or system generated password applied to the biometric features. One of the advantages of this system is that the biometric data is transformed on a personal device and only this transformed data is sent for matching. Hence, the original biometric data of the user is never at risk.

The techniques discussed above are independent in nature and can even be used in combination with each other. A biometric template can first be protected using a biometric cryptosystem or transformation and then saved in a database after encryption. Various distinctive characteristics of these techniques are discussed in Table 1.

1.5. Fingerprint Biometric

Fingerprint Recognition is a widely used method for biometric verification and identification. This is because of the fact that Fingerprints of an individual are unique, permanent and is always with the individual. Fingerprint identification is used an essential application in forensic and criminal investigations. Fingerprint features known as minutiae points are the ground for most of the modern fingerprint recognition systems. These features are essentially what provides a fingerprint its uniqueness. Hence these are minutiae features should be marked accurately for the recognition process to be successful. However, fingerprint images scanned from the scanners are prone to corruption due to inconsistencies at the time of scanning like scars, humidity, dirt and non-uniform contact with scanning device. Thus, we need to pass the acquired image from a series of image enhancements before the minutiae features can be extracted. The most critical step in the process of fingerprint matching is the extraction of minutiae from the acquired fingerprint images. Rest of the process of fingerprint matching is highly reliant on this step.

1.5.1 Fingerprint and Minutiae

A fingerprint is an impression left by the frication ridges of a human finger. An individual's fingerprint contains a distinct pattern of ridges and valleys. A ridge is a single curved segment on the human finger whereas a valley is an area between two adjacent ridges. So, the dark areas of the fingerprint are called ridges and white area that exists between them is known as valleys (see Fig. 1.9.).

Figure 0.9 Fingerprint Image

1.5.2 Minutiae Points

Minutiae points, the prominent features of a fingerprint are used in the process of matching fingerprints. These minutiae points are also used to examine the uniqueness of the acquired fingerprint. The quantity of the minutiae points obtained determines the quality of a fingerprint image. A good quality fingerprint image must have 25-80 minutiae points.

A Minutiae point defined as the point where the ridge lines either end or fork. These minutiae points can be of many types. These types are (see Fig. 10):

- *Ridge ending* – points where ridge ends.
- *Ridge bifurcation* – points where a ridge branches out into multiple ridges.
- *Ridge enclosure* – when a single ridge bifurcates and then reunites to continue as before.
- *Ridge dots* – very small ridges.
- *Ridge islands* – a short ridge in between two ridges.
- *Bridges* – a ridge that runs between two parallel ridges.

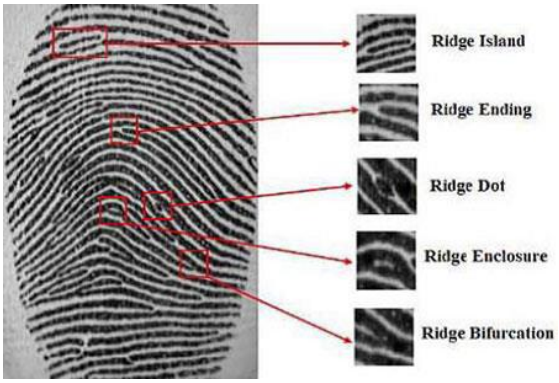


Figure 0.10 Common Minutiae Points

Ridge endings and Ridge bifurcations are known as the level 2 minutiae points. These are most commonly used minutiae points since they require intermediate level of quality. Rest of the minutiae points are known as level 3 minutiae points. These are based on a combination of the level 2 minutiae points and require very high-quality fingerprint image in order to be extracted accurately

Chapter 2

Fingerprint Recognition Process

Fingerprints recognition is just not a straightforward process. It requires a great deal of algorithms as well as procedures such as image processing, feature extraction and matching. The fingerprints representations are often in a grey scale images. Because of some unforeseen external conditions, the image may have noise. The noise is easy to remove with the process of filtering that boost the image quality. The first step which must be performed is always to prepare the image for the features extraction. Once the features have been extracted, the template is stored in order to perform the matching process.

2.1. Pre-Processing

This part includes the process that needs to be performed before actual feature extraction is done. These steps are essential to make the fingerprint image more suitable for feature extraction. Such steps enhance the image for better feature extraction. Pre-processing steps include:

2.1.1 Local ridge orientation

A ridge forms an angle ɵ with the horizontal axis. This angle is known as the local ridge orientation. The fingerprint is represented in the form of a two-dimensional matrix of pixels. Rather than calculating the orientation in each and every pixel, the image is split up into little individual regions and the angle formed by these regions with the horizontal axis describes the local ridge orientation. Graselli in 1969 used a matrix D which contained elements that symbolize the local orientation of the ridges to define the fingerprint orientation of the image. Every element $ɵ_{ij}$ (see Fig. 2.1.), related to the node [i,j] of the square-meshed grid positioned on the pixel [xi,yj], indicates the average orientation of the fingerprint ridges in a neighbourhood of [xi,yi]. The value of r_{ij} displays the actual dependability of the orientation. The value r_{ij} is minimal for noisy areas and substantial for high quality areas in the fingerprint image. This local orientation field is used for further calculations.

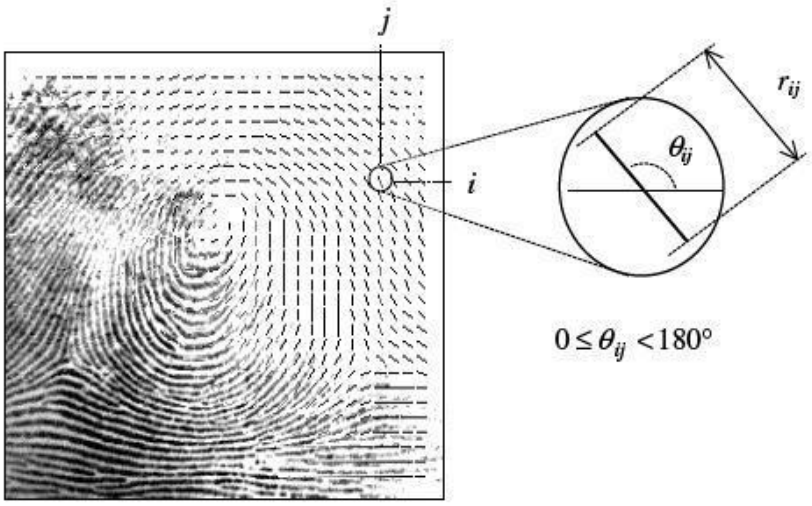


Figure 0.1 Local Orientation Field

2.1.2 Segmentation

This process is utilized by a few of the algorithms. Segmentation does not include the separation of ridges from valleys. Instead, segmentation is the technique to distinguish the background area from fingerprint image area(foreground). This process is needed only if the image has been acquired by a touch-based sensor. In case of sweep based sensor, such operations are not required.

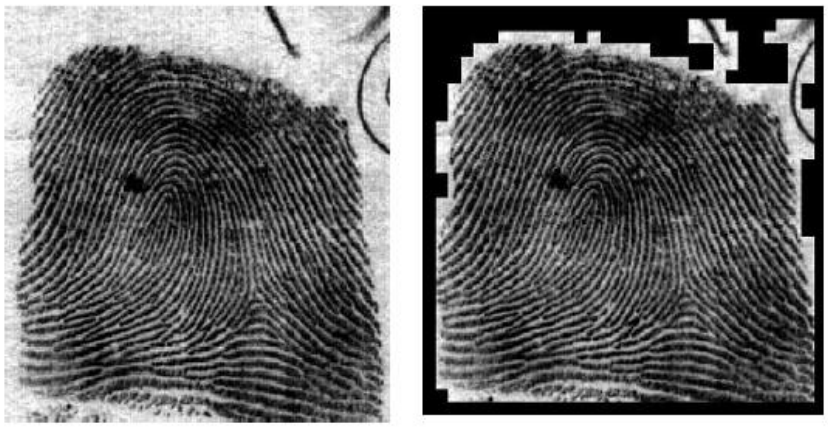


Figure 0.2 Fingerprint image before (left) and after (right) segmentation

Segmentation generally includes a threshold in order to check if the area lies below that threshold or not. This can be done by using a globally fixed threshold or a local adaptive threshold. Segmentation can also be performed based on the orientation field estimation. The certainty level of a block's

orientation field is used to quantify how much the orientation filed of the block agrees with the pixel gradient orientations.

2.1.3 Enhancement

In order to get best results, all the procedures included in the fingerprint recognition systems require a sample i.e. fingerprint image that is of high quality otherwise, the minutiae points cannot be properly extracted. Such a situation may result in an unreliable system. The image resolution required for a system is usually pre-defined in order to avoid future problems. For example, a resolution of 500 x 500 pixels is usually defined by most the professional systems that are used by government authorities.

A quality check is always performed after acquiring the fingerprint image. During enrolment, this is done to make sure that no bad quality fingerprints are used to store templates as it may result in variations in the stored and the actual query template. If an image is not of adequate quality, the fingerprint enrolment is performed again until a high-quality fingerprint is acquired. During the process of identification, quality check is performed to make sure the query template is generated is of good quality as else it would result in wastage of system resources as no suitable match will be found for such a template.

Figure 0.3 Good quality fingerprint image(left) and Bad quality fingerprint(right)

Fig. 2.3. and Fig. 2.4 display the different quality fingerprints.

A large number of procedures are available to enhance an image but the ones preferred by most researchers are normalization, histogram processing, contrast

stretching or Fourier transform. Jain and Wan [11] in 1998 proposed a normalization algorithm to define the value of the new pixel.

$$I'[x,y] = \begin{cases} mo + \sqrt{(I[x,y]-m)^2.v_0/v} \\ mo - \sqrt{(I[x,y]-m)^2.v_0/v} \end{cases}$$

Where m and v represent image values and v_0 and $m_0$represent values after normalizing the pixel.

2.1.4 Binarization and thinning

After the process of enhancement, the image is ready for minutiae extraction. Many of the minutiae extraction are based on a binarized image. In order to obtain a binarized image, the process of binarization is performed. This results in an image which is black and white. After binarization, another step called thinning is performed. This procedure helps to slim down the ridges of a fingerprint right to the skeleton form i.e. one-pixel wide. Fig. 2.5. shows a fingerprint image before and after the processes of binarization and thinning.

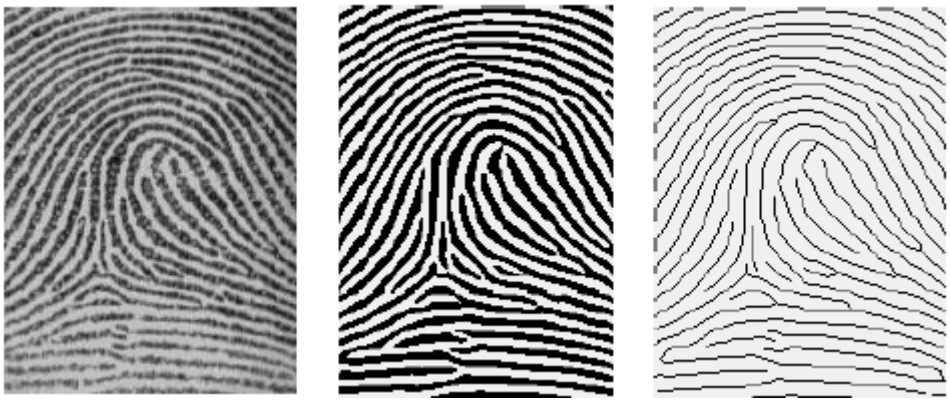


Figure 0.4 Greyscale image (left), binarized image (centre) and thinned image(right).

2.2. Minutiae Extraction

Minutiae extraction is the process of finding minutiae points from a fingerprint image. This is considered the most important step since the steps of enrolment and matching can only be as successful as the process of minutiae extraction. Minutiae are detected by scanning the binary image for ridge endings and bifurcations. These scanning patterns are executed both width wise and top to bottom. The 2x3 pixel structure is needed in order to scan the binary image.

Patterns displayed in Fig. 2.6. demonstrate process of discovering the minutiae points inside the binarized finger-print impression. The first two patterns represent endings of ridges while others represent bifurcation of ridges.

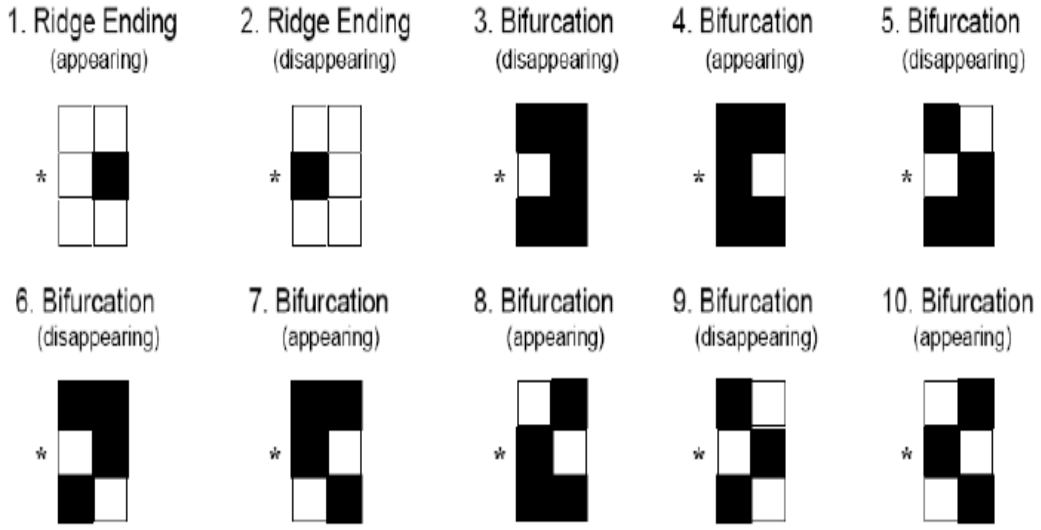


Figure 0.5 Patterns used for minutiae detection

The particular coordinates as well as orientation of every ridge endings as well as ridge bifurcations are crucial to obtain best results during fingerprint matching. Orientation of a minutiae point is defined in the form of degrees. The angle between the line projected from the minutiae point and the horizontal axis represent the orientation of the minutiae point. The horizontal axis represents zero degrees and increases counter clockwise (See Fig. 2.7.).

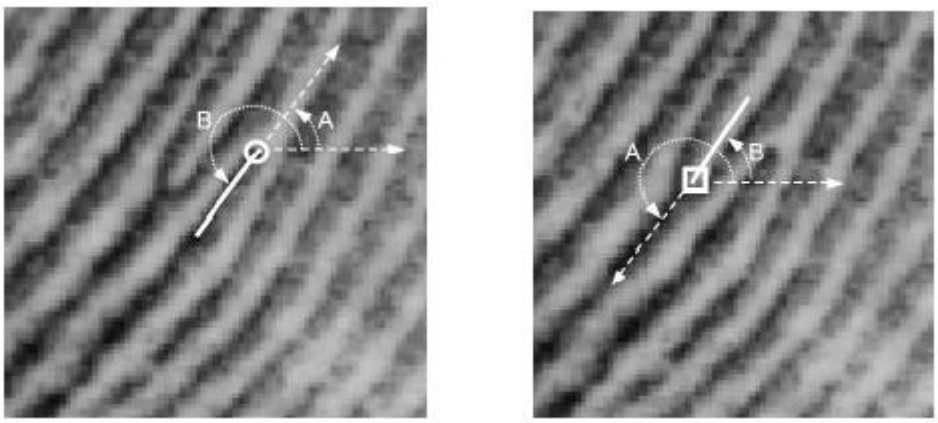


Figure 0.6 Minutiae Orientation

Minutiae points detected using the pixel patterns may comprise of genuine and fake minutiae. The amount of inaccurately discovered minutiae could be reduced in post-processing phase using the aid of quality factor.

Figure 0.7 Genuine and fake minutiae points

2.3. Post Processing

Minutiae points that are discovered in Minutiae extraction phase may contain some false minutiae points. The amount of inaccurately discovered minutiae is dependent upon the standard of the fingerprint. These kinds of fake minutiae must be filtered to eliminate as many fake minutiae as is possible devoid of eliminating genuine minutiae. The unnecessary minutiae within the fingerprint tend to be of the type:

2.3.1.1 Adjacent Minutiae Points

2.3.1.2 Minutiae points near border of the image.

2.3.1.3 Bridges, break, hole, spike as displayed in Fig 2.9.

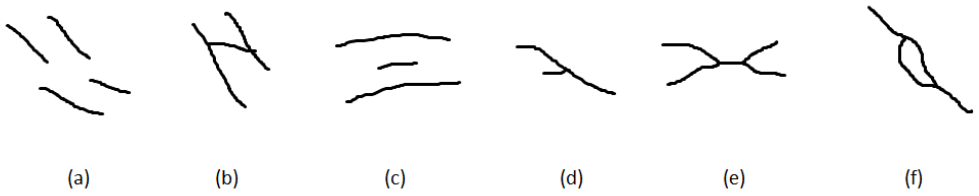


Figure 0.8 Broken ridges, bridges, short ridges, and holes

These kinds of fake minutiae could potentially cause problem in the course of matching. Eliminating all of fake minutiae one by one is time consuming as well as complicated. That is why quality of every minutiae is usually calculated. Initial reliability measure is computed depending on pixel intensity statistics inside the immediate locality of the minutiae point. The dimensions of this

locality are set to some pixels and the reliability of the minutiae point is calculated depending upon this neighbourhood minutiae calculation.

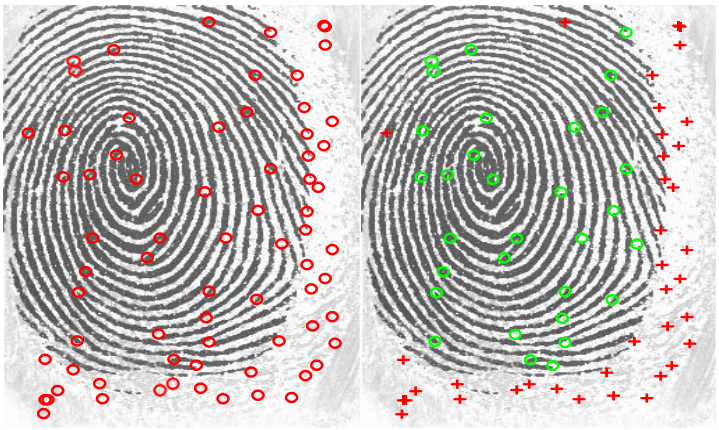


Figure 0.9 Image with false and real minutiae (left), image with read minutiae with green "o" and fake minutiae with red "+" (right)

2.4. Fingerprint Matching

Fingerprint matching can be a challenging method because of quality disparities in the fingerprint image obtained from the identical person over time. All these disparities are usually because of shifting skin situations, disturbance, glitches induced in the course of extraction. A few of the techniques used for fingerprint matching are:

2.4.1 Correlation-based matching

A pair of fingerprint images (usually one is stored in database and other that is query image) are actually superimposed and the relationship (on the intensity stage) among similar pixels is normally calculated for various alignments. This technique is usually good at attaining better outcomes in comparing fingerprint templates during the authentication process. Great matching precision can be acquired using this approach. In this technique grey-level data is obtained to perform fingerprint matching [12].

Correlation dependent technique could be the substitute technique if the fingerprint impression is simply not good, in this particular scenario extracting minutiae might result in glitches or fake minutiae's. Even so, correlation centered technique can't be applied to a variety of applications because of its significant effort required for its computation.

2.4.2 Minutiae-based matching

A Really reliable algorithm is definitely the adaptive elastic string matching algorithm. This algorithm initially picks two similar minutiae point from the stored template as well as the query impressions. This set of minutiae are known as the reference minutiae. The algorithm utilizes three features of the lined-up minutiae to get matching. These features are: the distance from reference minutiae also known as the radius, relative angle to reference minutiae called the radial angle and the local direction of the ridge known as the minutiae direction. This algorithm signifies the source template as a minutiae thread. The string expression is normally acquired simply by using radial angles to impose a linear ordering on a minutiae point. A String matching algorithm is then used to match the ensuing input and the query minutiae string.

2.4.3 Ridge feature-based matching

Ridge feature maps are also utilized for fingerprint matching [13]. This method employs orientation as well as frequency material, eradicates the requirement of minutiae extraction. Although minutiae extraction is usually hard for fingerprint impressions of low quality, various other attributes of the fingerprint related to the ridges like shape of ridge, frequency and local orientation could be extracted a lot more dependably as compared to minutiae. The methods that belong to this category assess fingerprints with regards to characteristics extracted using the ridge pattern.

Chapter 3

Literature Survey

3.1. Minutiae Extraction Techniques

The Technique used for minutiae extraction is usually based upon the quality of the fingerprint images acquired. If quality of a fingerprint is low, we need to enhance the fingerprint image in order to make the extraction process accurate.

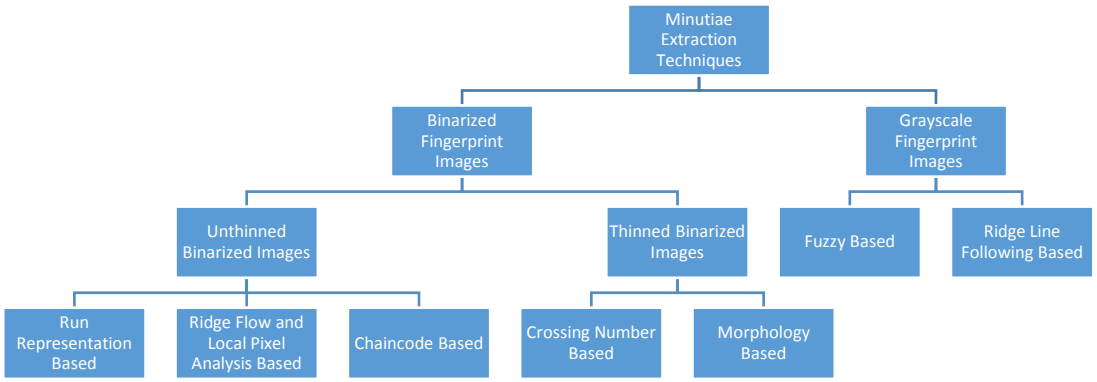


Figure 0.1 Minutiae Extraction Techniques

3.1.1 Unthinned Fingerprint Images

There are three methods of minutiae extraction for Unthinned Fingerprint Images. These are:

3.1.1.1 Chaincode Processing

In this technique, transitions from white background to black foreground are identified by scanning the Binarized fingerprint image from top to bottom and from left to right. These transitions are then expressed as an array of contour elements by tracing the contour counter clockwise and each element represents a pixel on the contour. The chaincode representation of object contours and pixel images can then be recovered from this chaincode of contours. This is done by tracing a ridge line counter clockwise on contour array; a minutia is located when the ridge line takes a large left turn. In the same way, if a trace on the contour array makes a right turn a bifurcation minutia is detected.

3.1.1.2 Run Representation

This method is useful when one wants to quickly extract the minutiae points from the binary fingerprint image without going through the process of thinning. A deluge of runs after the run-length encoding is used to represent the fingerprint images. Characteristic runs are then detected by checking the runs' adjacency. Some of the characteristic runs might not be true points so some kind of geometric constraints are applied while checking the validity of the characteristic runs. The image is first pre-processed in order for its enhancement. The image is then separated from the background by segmentation and normalization in order to get a predefined mean & variance.

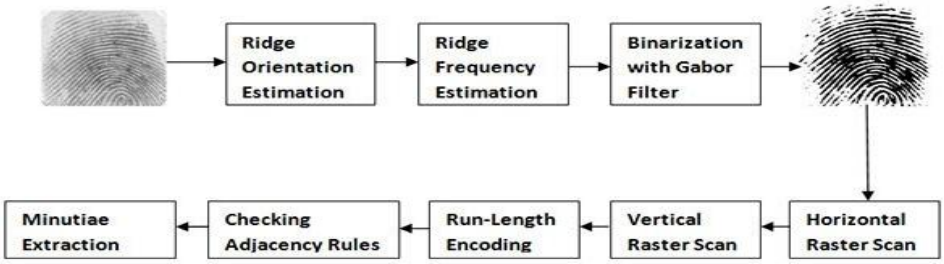


Figure 0.2 Minutiae extraction using run-length encoding

The local orientation and the orientation of the ridge is calculated around each of the pixels and then the gabor filter is applied. This results in contrast between foreground and background as well as noise reduction. These steps are followed by image binarization which is done by selecting a threshold value. After threshold value has been set, pixels with value greater than threshold are considered white and all other pixels are considered black. This method is considered very efficient as it reduces memory space as well as speeds up processing time.

3.1.1.3 Ridge Flow and Local Pixel Analysis

This method is a square based method that is used to extract minutiae images that are binarized but not thinned. This is done by creating a 3X3 mask around each pixel in the fingerprint image. The average of this mask

is then computed. The pixel is treated as an ending if the calculated average is less than .25. Also, the pixel is considered a ridge bifurcation if the calculated average is greater than .75.

3.1.2 Binarized Thinned Images

In this type of Minutiae extraction techniques, the fingerprint image is pre-processed for enhancement. Firstly, segmentation of the image is done which is followed by binarization. The thinning process follows the Binarization. The thinning process iteratively removes pixels hence thinning the ridges until the ridges are just one-pixel wide. Minutiae extraction is then performed on the image which has been enhanced, binarized and thinned. A post processing stage is performed after minutiae extraction to make sure no false minutiae points are selected. Two common categories of Binarized thinned image minutiae extraction are:

3.1.2.1 Crossing Number

Crossing number is the most frequently used minutiae extraction technique in the binarized thinned category. Various techniques for minutiae extraction belonging to this category are available in literature.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure 0.3 Minutiae extraction using Crossing Number

This method is commonly used because of its computational efficiency as well as simplicity [14]. This method uses a skeleton image with eight-connected ridge flow pattern. The local neighbourhood of every ridge pixel is scanned using a 3 X 3 window to extract the minutiae points (fig. 3.3). The Crossing Number (CN) value is then computed:

$$CN = \frac{1}{2}\sum_{i-1}^{8} |P_i - P_{i+1}|$$

The CN number is half the sum of the differences between pairs of adjacent pixels in the eight-neighbourhood.

0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0
0	1	1	1	1	1	1	0	0	0
0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0	1	0

Figure 0.4 Binarized Ridge

0	**0**	**0**
0	**1**	**0**
0	**0**	**0**

Figure 0.5 Isolated Point (CN=0)

0	**0**	**0**
0	**1**	**1**
0	**0**	**0**

Figure 0.6 Ridge Ending Point (CN=1)

0	**0**	**0**
1	**1**	**1**
0	**0**	**0**

Figure 0.7 Connective Point (CN=2)

0	**0**	**1**
1	**1**	**0**
0	**0**	**1**

Figure 0.8 Bifurcation Point (CN=3)

1	**0**	**1**
0	**1**	**0**
1	**0**	**1**

Figure 0.9 Crossing Point (CN=4)

Using the CN Number (Fig 3.4-3.9), the pixel on the ridge is then classified as either an ending, bifurcation or just a non-minutia point.

3.1.2.2 Morphology Based

This technique uses the mathematical morphology with which the image is pre-processed in order to reduce the efforts required in extraction during the post processing stage. Spurs, bridges etc. are removed from the fingerprint image by using Morphological operators and true minutiae points are decided by hit or miss of morphological transform. These morphological operators are shape operators which help in the process of shape manipulation so as to identify and also to compose objects and their

features. This kind of technique helps in developing structuring elements for different minutiae types of a fingerprint image which are again used by hit/miss transform in order to extract valid minutiae points.

3.1.3 Grayscale Fingerprint Images

There are number of techniques to extract minutiae directly from grey fingerprint images without going through the process of thinning and binarization. Advantages of this extraction techniques are:

- Binarization may result in loss of information.
- Binarization and Thinning consume a lot of time.
- Binarization and thinning can add variety of spurious minutiae.
- Binarization techniques are not very useful for low quality images.

3.1.3.1 Ridge Line Technique

This Technique proposes extraction of minutiae points directly from grayscale images by tracking of the ridge lines. This is done by 'sailing' using the local orientation field. At each step, this technique tries to locate, a local maximum which is relative to a section orthogonal to the direction of the ridge. Thus, a ridge line's polygonal approximation can be obtained by connecting the consecutive maxima.

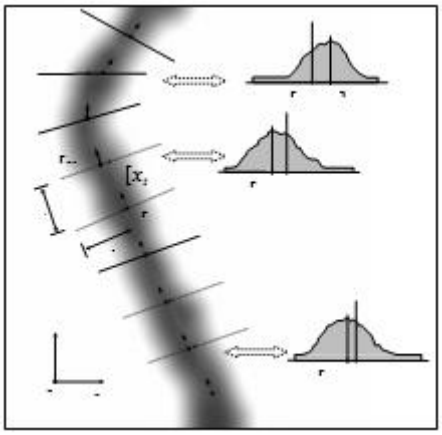


Figure 0.10 Ridge Line Technique

3.1.3.2 Fuzzy Based Technique

A grayscale image is observed to have two distinctively different levels of grey pixels. The pixels with darker levels constitute ridges while the lighter pixels constitute valleys or furrows. These levels are modelled

using fuzzy logic and appropriate fuzzy rules are applied to extract the minutiae accurately.

3.2. Fingerprint Template Protection

With the proliferation of biometric recognition systems, an attacker's benefit in staging a system compromise is also increasing and thus is the need to ensure system security and integrity. The techniques to defend the biometric templates are categorized into two primary groups: biometric cryptosystems and Template transformation techniques. While bio- metric cryptosystems permit restricting a protected key to the biometric information to acquire a secure sketch from which no data in regards to the biometric information or the key can be recouped, Template transformation techniques non-invertible trans-form the biometric template with the client's password. Two main examples of Biometric crypto-systems are: Fuzzy vault and Fuzzy commitment. In fuzzy vault systems, the fingerprint templates are stored in the form of a set of points whereas in fuzzy commitment systems binary vectors are used to store fingerprint templates. Linear error correcting codes are used in fuzzy vault as well as fuzzy commitment methods. Consider a linear error correcting code of length ℓn (number of symbols in the codeword) and rank ℓk (number of symbols in the secret key). Any combination of errors e and g erasures can be corrected by a linear error correcting code as long as it satisfies $(g+2e+1) \leq D_{min}$, where D_{min} represents the minimum distance between code-words, when a biometric cryptosystem uses such a code the secure sketch can be decoded as long as $(\ell n - D_{min} + 1)$symbols in the biometric feature vector can be guessed correctly and the remaining $(Dmin- 1)$ symbols are treated as erasures. If the selected error correcting code is maximum distance separable (i.e., it satisfies the Singleton bound), then $(D_{min}- 1) = (\ell_n - \ell_k)$.

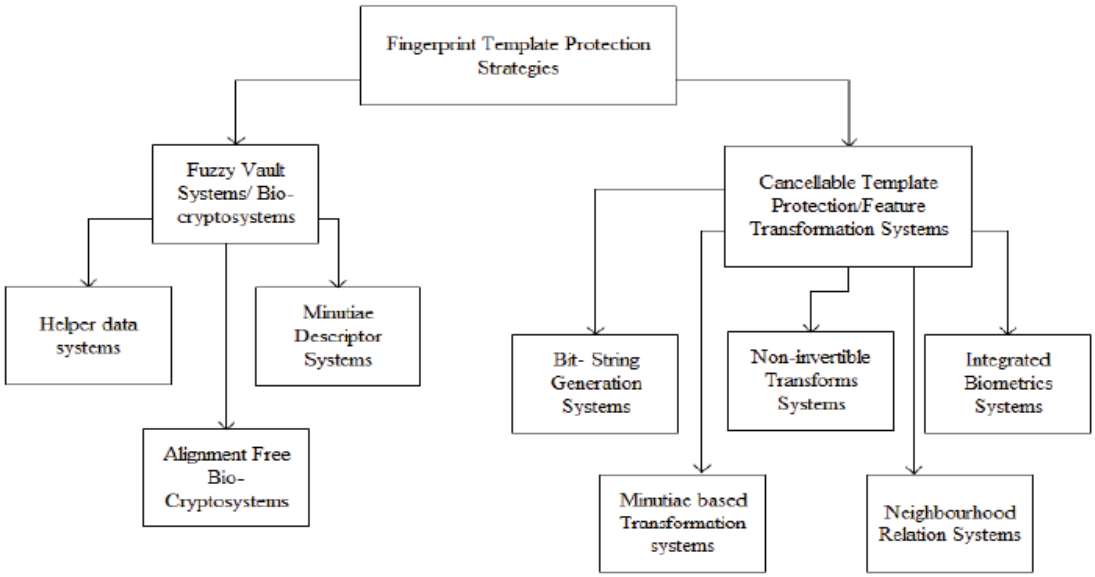


Figure 0.11 Fingerprint Template Protection Techniques

3.2.1 Fuzzy Vault Systems

In Systems such as Fuzzy vault, templates are not actually stored in any database. Instead, the original template is first transformed and then this transformed version is saved by using cryptography (See Fig. 3.12 and Fig. 3.13). [15] Describes such biometric cryptosystems as well as their issues and challenges. The brief introduction about fuzzy system is given by [16].

3.2.2 Helper Data Systems

Systems such as helper data were first proposed by J. Linnartz[17] which was modified to [16] which include a higher degree polynomial to the template whose input would include just minutiae points which are from the genuine set of minutiae points.

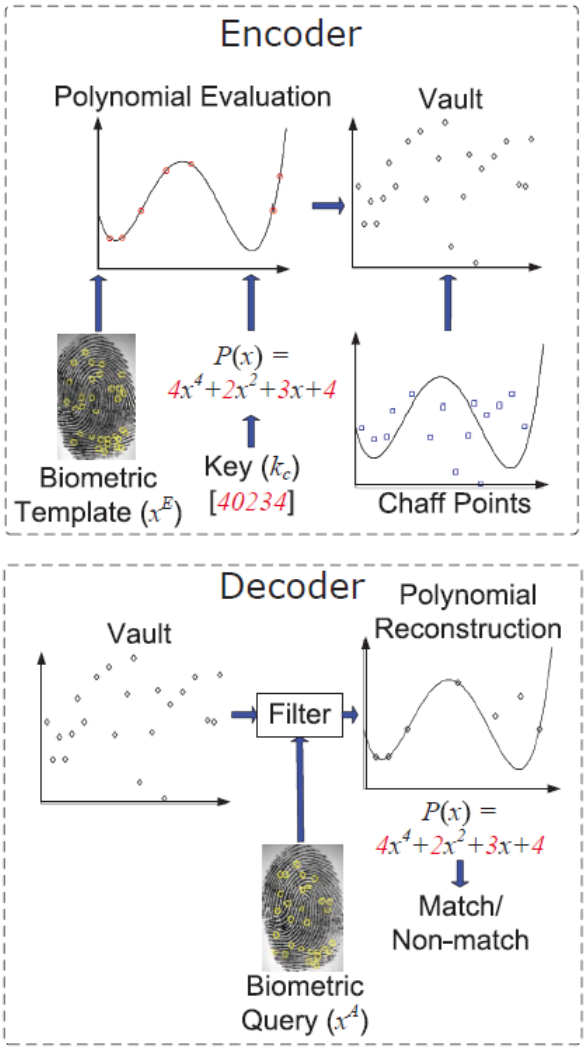
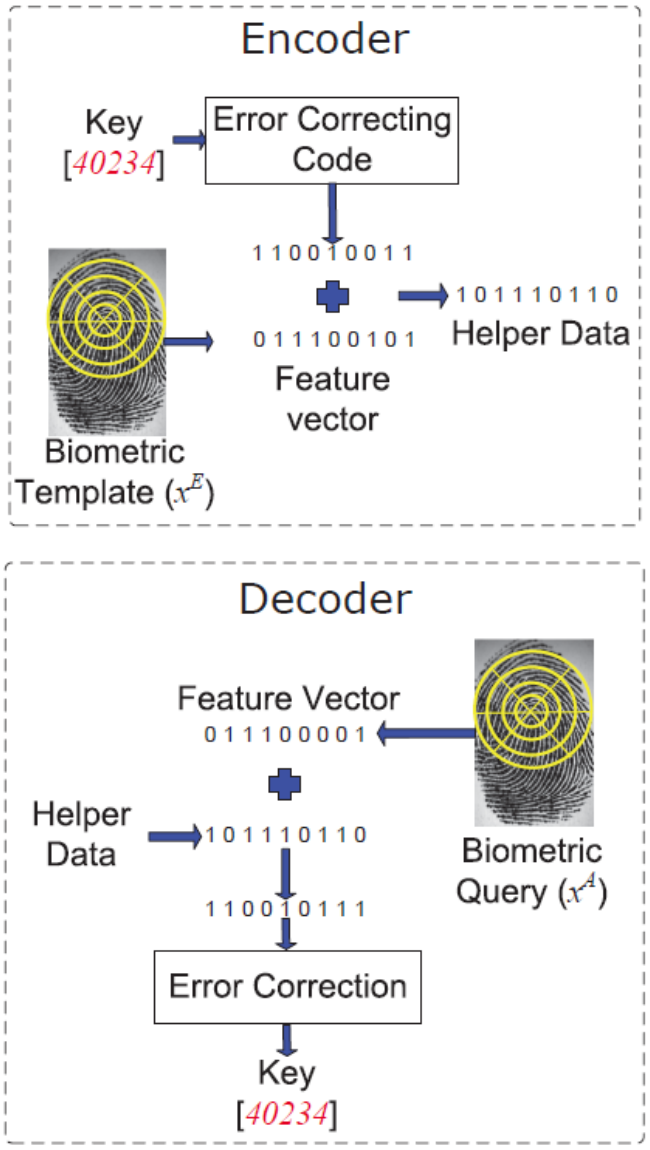


Figure 0.12 A schematic diagram illustrating encoding and decoding of a typical fuzzy vault scheme.

Using the work already done, Uludag [18] successfully proposed a way to implement the methods of Juels et al [16] with the help of helper data [19] and described that the helper data can successfully prevent information leakage. The system comprises of three main parts, i) encoding and decoding – Type of data that is being locked defines the size of the secret key S. In this implementation, 128-bit symmetric AES encryption key was used. Numerous candidate keys are created with the help of Cyclic redundancy code (CRC). During decoding CRC is used check errors and once it is

assured that the templates are identical, curvature estimation is used to obtain orientation field flow curves (OFFC) by analysing the points at maximum as well as minimum curvature of the OFFC.

Figure 0.13 A schematic diagram illustrating encoding and decoding of a typical fuzzy commitment



scheme.

The last phase is ICP. ICP stands for Iterative Closest Point Registration and is just a minor modification of [38]. In which, they have shown that proposed architecture can be used to secure AES keys.

	Fuzzy Vault	Fuzzy Commitment
Representation	Point-set	Binary string
Main advantage	Ability to secure fingerprint Minutiae	Compact size of the sketch
Main limitation	Difficult to generate chaff that are indistinguishable from genuine points	Lack of perfect codes for desired codelengths
Parameters	Polynomial degree (k), size of the template set (r), and number of chaff points(q)	Key length L, length of codeword N, and error correcting capacity of the code
GAR- Security Trade-offs	Higher values of (k/r) and q lead to lower GAR, but higher security and vice versa	Higher values of (L/N) lead to lower GAR, but higher security and vice versa
Implementations	Fingerprint	Fingerprint

Table 2 Comparison of Fuzzy vault and Fuzzy Commitment

3.2.3 Fuzzy Logic with Minutia descriptors

Descriptors are used to improve [16]. J.Feng [20] proposed a matching algorithm that is useful for solving two of the major problems: similarity computation and correspondence. Polynomial evaluations are used to encrypt biometric data by using the method of Fuzzy commitment schemes.

Nagar et al [21] suggested a minutiae descriptor based fuzzy vault system. The vault is encrypted in such a way that makes it harder to decode even when the selected set of minutiae is correct. In this system, minutiae descriptors were used to capture orientation & information of the frequency of the ridge in the neighbourhood of a minutia. Firstly, the helper data is enrolled using fuzzy vault encoder with the help of CRC error checker. The security of the vault is improved by encrypting the ordinate values so that polynomial cannot be reconstructed even if the genuine minutiae points are selected. Chaff point descriptors are picked from the database. Then the two of the templates are matched by anauthentication system by applying XOR operations between the query and enrolled minutiae features.

3.2.4 Cancellable biometrics

Cancellable biometrics are generated by systematic and repeated distortion of the biometric features to secure user-specific data. If any biometric template

is stolen or compromised, the same biometric can be mapped to a new template by changing the distortion characteristics. This technique is used subsequently in [22].

3.2.5 Non-Invertible Transforms

In the paper "Privacy Weaknesses in Biometric Sketches", K. Simoens et al. [23] indicated towards weaknesses in privacy where they proposed an objective "whether one can undermine a user's privacy given access to biometrically encrypted documents", and they further tested and found "if an attacker can determine whether two documents were encrypted using the same biometric". They also deduced the required conditions for ideal distinguishability and perfect irreversibility from bounds on the adversary's advantages.

Y. Sutcu et al.[24] suggested a method in which he fused 1 way transformation of the template with a cryptographic hash function which is more secured. It is composed by merging different Gaussian functions into a single function as "robust hash". The templates in the database are secured by using this cryptographic hash. ORL face database was used for testing the algorithm and the results showed that this method provides a way towards eliminating the weaknesses in terms of privacy and security.

The cancellable domain and the algorithms that were discussed so far come had some demerits like the biometric feature distribution which was either avoided all together or was inefficient to match the features. As such, these algorithms had privacy and security threats. Thus, Nagar et.al [25] proposed an efficient method for transformation of non-invertible fingerprint templates. This system takes into account "coverage effort curve" for calculating the number of estimates that are needed by an intruder to retrieve some part of the biometric template. Keeping this in mind, the non-invertible measure is determined through the following three stages: i) pre-image identification – This step includes calculation of the pre-images to obtain transformed minutia, ii) computation of minutiae likelihood – This step includes kernel density estimation for estimating the relative probability of the previously transformed minutiae, and iii) computation of non-invertible

measure: This step focuses on pre-images sort. This is done on the basis of their likelihood and then calculation of the coverage which includes the number of pre-image guesses that are true. This leads to decrease in security risks as well as improvement in performance during matching.

3.2.6 Minutiae based transforms

This technique is a cancellable template scheme that is concerned with minutiae based transforms. Chen et al. [26] proposed a way in which the application does not have control over the transform so that templates once created cannot be reused. This technique has 3 stages. The first stage includes construction of a circular region in which each and every minutiae is circled. Only a few minutiae points among these are encrypted and the resulting template was obtained in a distorted form. The second stage includes the encryption of the circular region. This is done with the help of above stated non-invertible transformation algorithm. The algorithm encrypts all of the circular region and results in transformed template which is then stored. The third stage includes performing matching of the encrypted regions. This done by one of the following untransformed matching algorithms: Hong. et al.,[27] (Point Pattern Alignment), Jea and Govindaraju [28], (partial fingerprint matching) and Chen et al [29] (Algorithm used for constructing minutia-centred circular regions).

3.2.6.1 Bit String Generation

Over the years, different researchers have proposed a vast number of methods for the protection of biometric templates. Yet a method to satisfy the conditions viz. diversity, performance, non-invertibility and revocability stated by Teoh, Goh and Ngo [30] was not easy to design. After analysing these conditions, Z. Jin et al. [31] introduced an application for the generation of revocable fingerprint template. This template included bit-string that used polar grid based 3-tuple quantization technique. This system includes four phases. The first phase consists of polar transform based reference minutiae, other minutiae points can also be transformed and rotated based on the chosen reference. The second phase includes a 3-tuple based quantization viz. polar grid quantisation

that is performed on all minutiae. The third phase consists of bit-string generation and user specific tokenized permutation - bit-string: it has value 1 for one or more minutiae on polar grid and 0 otherwise. The result is obtained in the final phase that intersects the two bit-strings. This method provides advantages like alignment-freeness and performance.

3.2.6.2 Integrated Biometrics

Integrated Biometrics use a kind of template that is generated by blending two or more impressions of a finger in order make a single mosaic. It can also be done by integration of the feature sets (viz., Information of Minutiae points) that are related to these impressions that has been explained in [32].

Chin et al. [33] proposed an algorithm that had biometric features obtained from multiple biometric data are fused to obtain an integrated template using a hybrid template protection method. This method includes two techniques: i) random tiling and ii) equal-probable discretization scheme.

The whole process proceeds as follows: i) feature level fusion, ii) random tiling and iii) feature discretization. In the beginning, fingerprint and palm-print of a user is registered. The data captured is then merged at the feature level. Depending upon a user-specified key, with the help of random tiling, a random set pf features is generated. At last, the bit strings are generated by discretizing the random features. The hamming distance is compared between the query bit-string and the template bit-string to verify the query. This process is done by matching module.

3.2.6.3 Neighbourhood Relation

Another method of template protection is by using the data obtained by the neighbourhood relation which are projected in a plane that is used for generating string which is then encrypted using user's specified key. In [34], they have contributed by constructing X rectangles and generation of multi-line neighbouring relation. They suggested generation of cancellable template that are alignment free by constructing X rectangles which have

different orientations around each of the reference minutiae which is followed by translation and rotation invariant neighbouring relation. Also, plane based quantization for bit string generation is performed by using the neighbour minutiae that are found in the X rectangles in order to generate multi-line neighbouring relation for every minutiae. In previous methods only the minutiae points with distance greater than a certain threshold value were selected for generation of the template [35] which was followed by the matching process. This method has all the qualities to fulfil necessary conditions which are required of a cancellable template design.

Proposed By.	Methodology Used	Database Used	Success Rate(GAR)	Success Rate (FAR/FRR)	Error Rate
Nagar, A., and Star, A. (2008) [21]	Helper Data Extraction Authentication	FVC2002 DB2.	95%	0.01%	-
Uludag, U. et al (2006) [18]	ICP based Alignment, Constructing Helper Data, and Fuzzy Fingerprint Vault.	DB2 database of FVC 2002.	72.6%	0% FAR	-
Nagar, A., and Jain, A. K. (2009). [25]	Non-invertibility measures, Minutiae template transforms.	FVC2002	92%	10%	-
Yang, W., Hu, J.Wang, S., and Stojmenovic, M.(2014) [36]	Encrypted Matching, Formation of VNSs, Generation of modified VNSs, Generation of fixed-length bit-string representations.	FVC2000DB1, all of the 4 databases) of FVC 2002, and FVC2004DB2.	-	-	14.30% 11.84% 10.38% 16.52% 15.63% 20.61%
Chen, H., and Chen, H. (2011) [26]	Construct circular Regions, Encrypt circular regions, Matching using encrypted Regions	FVC2002 DB1 and DB2.	96.5%, 98.5% num level 18.	2%- DB1 2%- DB2	-
Chin, Y. J. Ong, T. S.et al (2014) [33]	Feature level fusion, Random tiling, Feature Discretization.	2 fp & 2 palm print databases. [47]	-	-	<5%
Prasad, M. V. NK., and Santhosh C (2014). [35]	Plane based quantization and bit string generation, Multiline neighbouring relation generation, Cancellable template generation, Matching.	FVC 2002 DB1, DB2 and DB3.	-	-	0.62% 1.33% 2.64%
Jin, Z., Jin Teoh, A. B. et al(2014).[31]	Tuple based quantization. Bit-string generation and User-specific tokenized permutation, (PGTQ): Reference minutia based polar transform, Matching.	FVC2002 DB1& DB2, FVC2004 DB1& DB2.	-	-	1.19% 6.94% 16.35% 8.66%

Table 3 Evaluation of various fingerprint template protection techniques [37]

Chapter 4

Research Gap and Problem Statement

In the last chapter, various techniques that are available for minutiae extraction from binarized as well as grey scale images were discussed. Various methods that are present for the protection of fingerprint templates were also discussed. This chapter includes the problem statement as well as the objective of this thesis.

4.1. Gap Analysis

Biometric security symbolizes innovations in electronic security systems and more businesses as well as associations are adopting it. But with the increasing use of biometrics especially fingerprints in security systems, it has become very important for an individual to keep his biometric signature secure. In order to do this, a person can keep be extra cautious but there are more than one ways to obtain a biometric signature of an individual.

The major problem is to protect the signatures that are saved on a system in which the user has been enrolled. As discussed in chapter 1 of this thesis, if an intruder gains access to such a database of signatures, the result could be disastrous not only for the individual but for system as well as the organization too. Many techniques like fuzzy vaults, template transformations and encryption have been discussed in chapter 1 and further elaborated in chapter 3 of this thesis. Such techniques are helpful in securing biometric information from the intruder but not all of them are perfect. Each of the techniques has its advantages as well as disadvantages.

The fuzzy vault technique does not store the actual fingerprint template but rather a modified version by applying a polynomial function to the minutiae. A secret key S is used to create this polynomial function that is generated. This modified template known as a vault is saved to the database. During matching, the query template and the vault is compared and the result is compared with the secret key S. If the keys match, access is granted to the system. In encryption technique, some kind of encryption technique is used to actually

encrypt the fingerprint template and store it in the database. During matching, this encrypted fingerprint is used to determine the authenticity of the fingerprint.

4.2. Problem Formulation

The template protection techniques defined in the above section both have some limitations. The Limitation of the encryption techniques are that the keys that are used for encryption or will be used for decryption need to be stored for the system to work. The limitation of the fuzzy vault system is that the likability of the stored template and the query template need to be perfect. This means that both the templates need to have similar number of minutiae points or else the computations needed for comparing the templates may not be practical (if possible at all). A method can be proposed that makes use of both the approaches to provide best results in all situations.

4.3. Objectives

The main objectives of this thesis are:

4.3.1 To study the existing techniques available for protection of fingerprint templates.

4.3.2 To propose a technique for fingerprint template protection that is based on both fuzzy vault and encryption.

4.3.3 To implement the proposed technique.

4.3.4 To evaluate the performance and reliability of the proposed algorithm.

Chapter 5

Proposed Solution and Implementation

The Advanced Encryption Standard, or AES, is a symmetric key encryption algorithm that can be used to secure data. A symmetric key algorithm is the one that encrypts and decrypts data using a single key. This kind of encryption is mainly used for communication between two parties. Both of these parties have the key and data is encrypted before transferring to other party. At the receiving end, the data is encrypted using the secret key.

A Fuzzy vault for fingerprints [19] is a method to secure the fingerprint template in which a new template (vault) is created that is based on a polynomial function created using a secret key and the original template. The vault as well as the secret key are stored in the database for fingerprint matching stage. During fingerprint matching, this vault is compared to the query template (note: both vault and query template must have same minutiae points to reduce complexity). This comparison results in the key that is used to create the vault from the fingerprint template. This key is matched with the stored key, if matched, access is granted to the user.

5.1. AES Encrypted Fuzzy Vault

This proposed work is based on the work of [19] along with other fingerprint recognition techniques that are used for fingerprint matching. This method involves saving the fingerprint template in an encrypted form as well as generation of fuzzy vault.

5.1.1 Methodology

During enrolment, the fingerprint image is acquired from the user. This fingerprint image is enhanced using the methods explained in section 2.1 of this thesis. After enhancement, the fingerprint image is binarized to make the image a true grey-scale image. This binarized image is then thinned to make all the ridges one-pixel wide. This step is necessary for minutiae detection. Once the image is binarized and thinned, it is ready for minutiae extraction. Minutiae are extracted using the method of crossing number explained in section 2.2. The extracted minutiae points are saved in the form of a fingerprint template Ts. Once the process of minutiae extraction is complete,

a secret key S is generated. Using this secret key S, AES algorithm is used to encrypt the fingerprint template Ts to create encrypted template Te. This encrypted template Te is stored in the database. Alongside the encryption, secret key S is used to generate a polynomial P. All the minutiae points from fingerprint template Ts are evaluated onto this polynomial to generate a polynomial template Tp. This polynomial template is stored into the database.

During matching, the query fingerprint is acquired from the user. This fingerprint image is enhanced using the methods explained in section 2.1 of this thesis. After enhancement, the fingerprint image is binarized to make the image a true grey-scale image. This binarized image is then thinned to make all the ridges one-pixel wide. This step is necessary for minutiae detection. Once the image is binarized and thinned, it is ready for minutiae extraction. Minutiae are extracted using the method of crossing number explained in section 2.2. The extracted minutiae points are saved in the form of a fingerprint template Tq. Once the process of minutiae extraction is complete, the encrypted template Te and polynomial template T_p for the corresponding user is fetched from the database. Using Polynomial Lagrange Form LF, the polynomial template T_p and query template T_q are compared. If the set of minutiae points in the query template T_q is similar to the minutiae points of original template Ts, the secret key S will be reconstructed. This key S is then used to decrypt the encrypted template Te and the decrypted data is stored into a decrypted template T_d. Once the process of decryption is complete, a fingerprint matching algorithm based on minutiae points is used to compare the query template T_q to the decrypted template Td. The result of the match decides whether access can be granted to the user or not.

5.1.2 Algorithm

This section describes the algorithms used in the proposed method.

5.1.2.1 Enrolment

Input

Fingerprint Image

Initialization

1.Initialize "$\boldsymbol{F}$" as an empty Buffered Image

2. Initialize "$\boldsymbol{T_s}$" as an empty Double array

3. Initialize "$\boldsymbol{T_e}$" as an empty Double array

4. Initialize "$\boldsymbol{T_p}$" as an empty Double array

5. Initialize "$\boldsymbol{S}$" as an empty Key

Extract Minutiae Points

6. Load fingerprint image $\boldsymbol{F}$

7. Binarize $\boldsymbol{F}$

8. Perform thinning of $\boldsymbol{F}$

9. Generate fingerprint template

10. $\boldsymbol{T_s}$ = ExtractMinPoints($\boldsymbol{F}$)

11. **Generate secret key $\boldsymbol{S}$.**

Encrypt fingerprint template

12. Encrypted Template $\boldsymbol{T_e}$

13. $\boldsymbol{T_e}$=AES.encrypt($\boldsymbol{T_s}$, $\boldsymbol{S}$)

14. Save($\boldsymbol{T_e}$)

Create Fuzzy Vault

15. Generate Polynomial

16. $\boldsymbol{P}$=PolynomialFunction($\boldsymbol{S}$)

17. Evaluate Polynomial

18. FOR each minutiae in $\boldsymbol{T_s}$

19. Populate Polynomial Template $\boldsymbol{T_p}$

20. $\boldsymbol{T_p}$=$\boldsymbol{P}$.value(T_s)

21. Save(T_p)

Output

Encrypted Template (T_e), Polynomial Template (T_p)

5.1.2.2 Matching

Input

Query Fingerprint Image (Q), Encrypted Template (T_e), Polynomial Template (T_p)

Initialization

1. Initialize "$\boldsymbol{Q}$" as an empty Buffered Image
2. Initialize "$\boldsymbol{T_q}$" as an empty Double array
3. Initialize "$\boldsymbol{T_e}$" as an empty Double array
4. Initialize "$\boldsymbol{T_d}$" as an empty Double array
5. Initialize "$\boldsymbol{T_p}$" as an empty Double array
6. Initialize "$\boldsymbol{S}$" as an empty Key

Extract Minutiae Points

7. Load query fingerprint image $\boldsymbol{Q}$
8. Binarize $\boldsymbol{Q}$
9. Perform thinning of $\boldsymbol{Q}$
10. Generate fingerprint template
11. $\boldsymbol{T_q}$ = ExtractMinPoints($\boldsymbol{Q}$)

Fetch Files

12. Load Encrypted Template into $\boldsymbol{T_e}$
13. Load Polynomial Template into $\boldsymbol{T_p}$

Unlock Fuzzy Vault

14. Using Lagrange Form Function, Compare $\boldsymbol{T_q}$ with $\boldsymbol{T_p}$
15. $\boldsymbol{S}$=Lagrange Form($\boldsymbol{T_q}$, $\boldsymbol{T_p}$)

Decrypt Template

16. Using key $\boldsymbol{S}$, decrypt $\boldsymbol{Te}$ to $\boldsymbol{T_d}$
17. $\boldsymbol{Td}$ = AES.decrypt($\boldsymbol{T_e}$)
18. IF
19. Decryption successful
20. THEN
21. Match($\boldsymbol{Tq}$,$\boldsymbol{Td}$)
22. IF
23. Match>Threshold
24. THEN
25. Fingerprint Match

26. ELSE
27. Fingerprint Mismatch
28. ENDIF
29. ELSE
30. Display Error
31. ENDIF

Output

Vault key, Match Percentage

5.1.3 Work Flow Diagrams

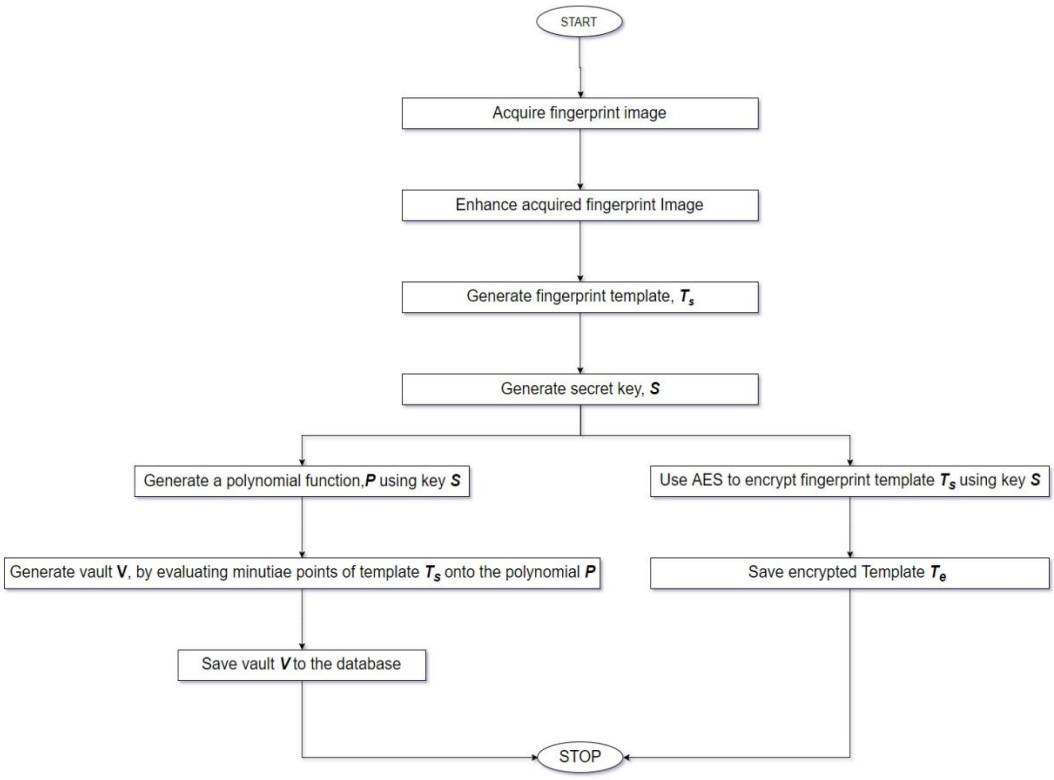


Figure 0.1 Work Flow of enrolment process

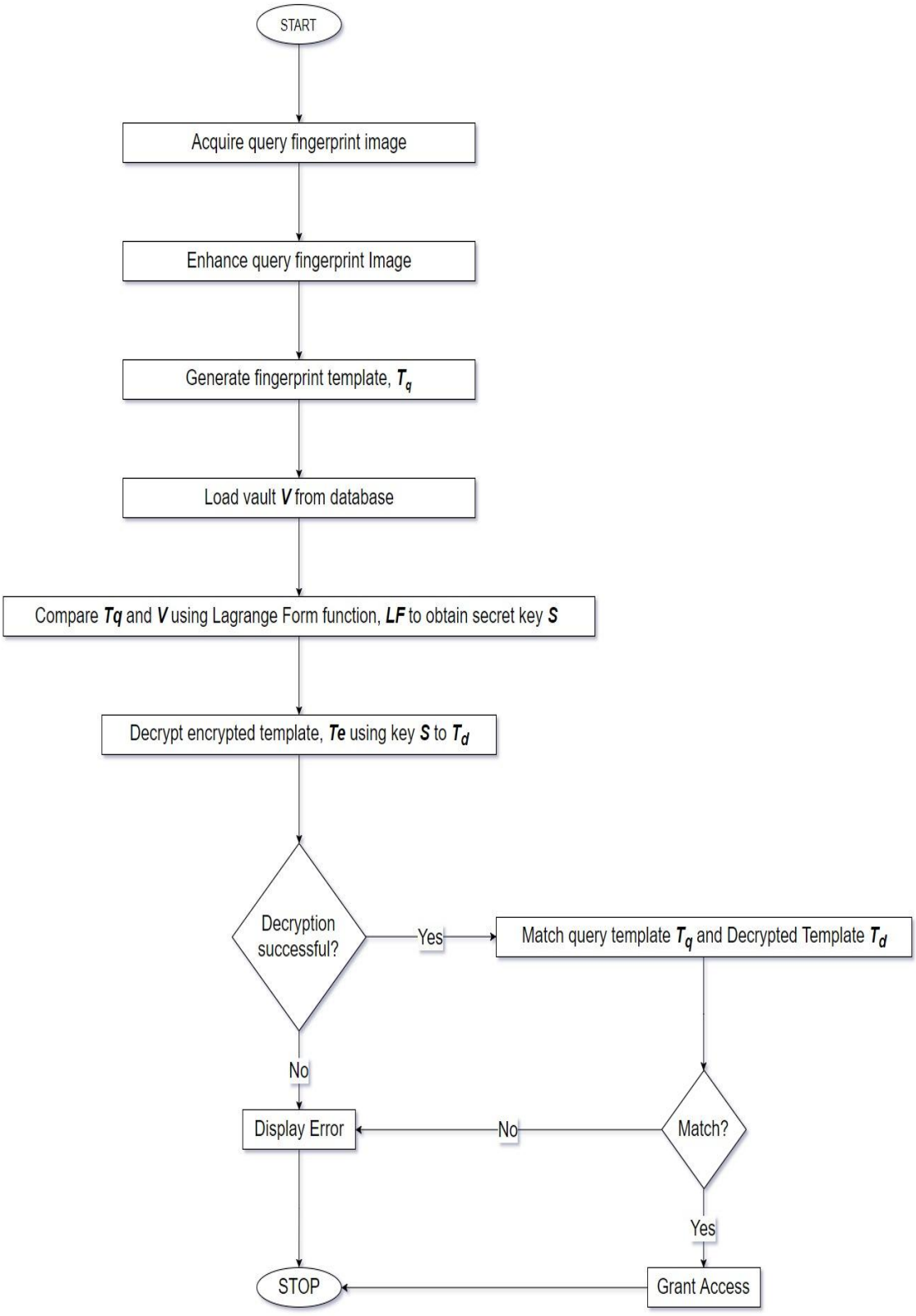


Figure 0.2 Work Flow of matching process

5.2. Implementation

The proposed solution has been implemented in Java using NetBeans IDE.

5.2.1 Java

Java is an object-oriented, concurrent, class-based language particularly built to possess as few implementation dependencies as it can. It is actually meant to enable software programmers "write once, run anywhere" (WORA), which means that created Java code can operate on just about all platforms which support Java without the necessity of recompilation. Java programs are generally compiled to bytecode which could operate on virtually any Java virtual machine (JVM) irrespective of computer architecture.

5.2.2 NetBeans IDE

NetBeans is an open-source, free framework for development of software written in Java. NetBeans can easily operate on just about any platform that works with a suitable JVM.

5.2.3 Java Packages

A few of the java packages used in the implementation of the proposed method are:

5.2.3.1 PolynomialFunction

org.apache.commons.math3.analysis.polynomials.PolynomialFunction

This package is used for representation of a real polynomial function with real coefficients. In implementation, it is used in the generation of the fuzzy vault for creating a polynomial function of which the minutiae points are evaluated.

5.2.3.2 PolynomialFunctionLagrangeForm

org.apache.commons.math3.analysis.polynomials.PolynomialFunctionLagrangeForm

This package is used for representation of a polynomial in lagrange form. In implementation, it is used to obtain the secret key by giving the input minutiae and the polynomial template (vault). The langrange polynomial is constructed using the abscissas (Query minutiae template) and function values (Polynomial template).

5.2.4 Interface and Results

Figure 0.3 Default Interface

Figure 5.3. displays the default interface of the system. The default fingerprint image is loaded on the system. Figure 5.4 shows the events after "Find Minutiae Points" button has been clicked. Center Image displays the thinned image while the image on the right displays the minutiae points detected on the thinned image.

Figure 0.4 Thinning and Detected Minutiae Points

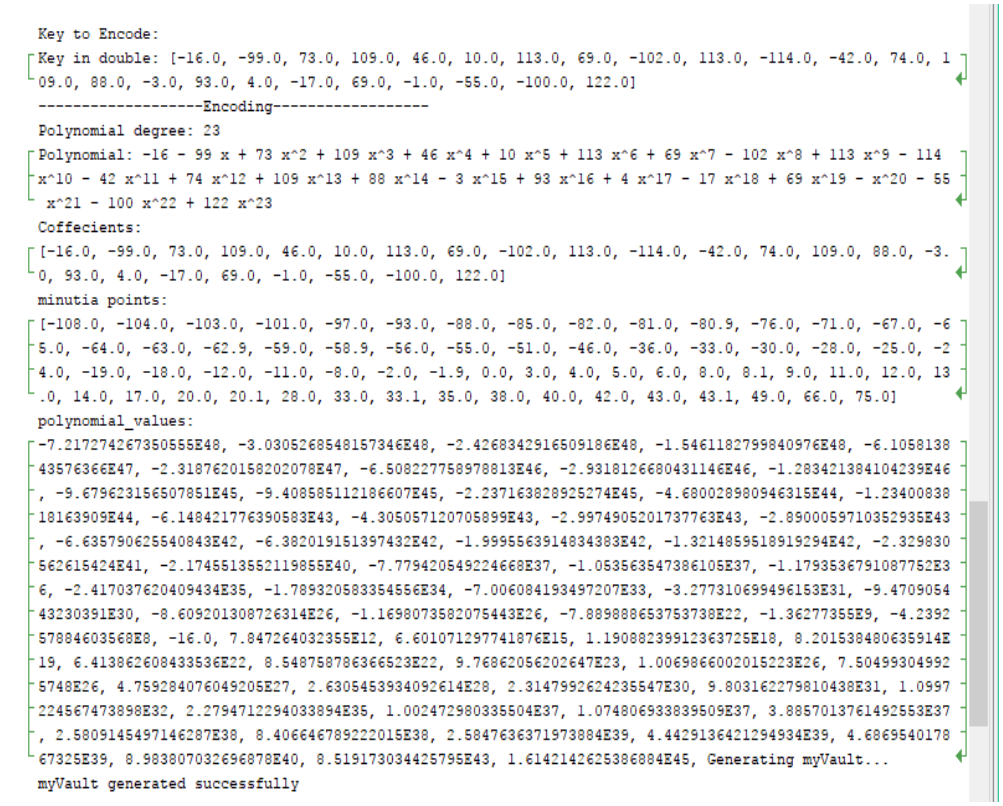


Figure 0.5 Fuzzy Vault Generation Output

In figure 5.5, the output when the vault is generated is displayed. This output contains the key that has been generated and used to generate polynomial, the coefficients of the polynomial as well as the final polynomial values that have been calculated by evaluating the minutiae points over the generated polynomial.

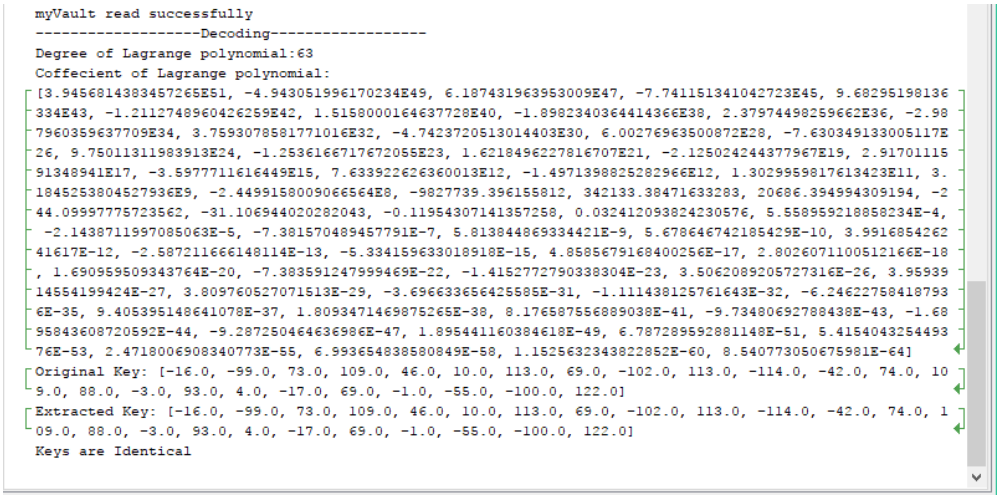


Figure 0.6 Fuzzy Vault Matching

Figure 5.6. displays the result when a query image is matched with the fuzzy vault generated in the previous step. At the end of this step, new key is generated by comparing the query template to the fuzzy vault. This key is compared with the original key used to encrypt the data. If the keys match, the fuzzy vault is said to be unlocked and result is given as a Match.

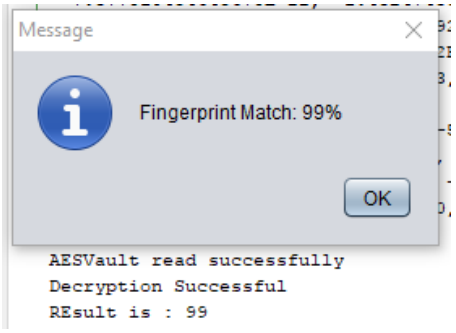


Figure 0.7 Fingerprint Matching Result

Figure 5.7. displays the result of the traditional fingerprint matching that uses the data from the stored fingerprint template and the query fingerprint to compare them. If the data of these fingerprints match above a threshold value, the query fingerprint image is said to be a match and access is granted to the user.

Chapter 6

Conclusion and Future Scope

6.1. Conclusion

With the expansion of biometric recognition systems in industrial market, protection of the kept biometric data is becoming increasingly essential. As discussed in this thesis, existing biometric systems possess a variety of weaknesses and a committed adversary may bring about serious harm to a biometric system along with the end users signed up for the system. Moreover, because of the permanent character of biometrics of a person its thievery and misuse could be irreparable. In case someone's fingerprints or perhaps iris patterns are compromised and are wrongly related to high susceptibility of a dreadful illness, the individual could be struggling to receive a health care insurance. The thought of biometric can devoid an individual of virtually any advantages provided by the biometric systems because of the worry to be easily impersonated by making use of spoof biometrics. Although these kinds of threats might not seem to be imminent, the rate in which biometric systems are booming, the value of information one could possess by setting up high level biometric data theft would certainly definite encourage the con men. By means of this thesis, we have proposed a method which we expect would be significant in securing biometric information stored in the biometric systems.

This thesis specifics different elements of biometric system security. It describes various components of the biometric systems and the attacks that may harm a biometric system. A developer of a biometric system could use this information as useful resource while developing a biometric system which is robust to every theft or sabotage. It also provides an introduction to the fingerprint recognition systems. It explains the various processes and stages that are included in the process of fingerprint recognition. In this thesis, we have discussed the work that has been carried out in the fields of minutiae extraction as well as biometric template security. It also includes the comparison of these techniques along with the reliability of these techniques by specifying the False acceptance and Genuine acceptance rates. Then, we present the problems with the existing methods of fingerprint template protection while expressing the problem statement for the

thesis. Finally, we explain the method that has been proposed in the thesis. It also contains the methodology and the implementation of the proposed method. The results and the interfaces of the implemented method have also been included at the end.

6.2. Future Work

In this thesis, we have proposed a method that incorporates encryption techniques into the fuzzy vault for enhanced security of the biometric systems. In future, such a technique can also be generalized into a fuzzy commitment as well. This technique would also improve the security of the biometric systems. Also, in our work we have incorporated AES encryption into the fuzzy vault, other kinds of encryption methods can also be implemented according to the requirements of the system. Additionally, instead of combining encryption mechanism into the simple fuzzy vault system, a method can also be proposed to incorporate encryption techniques into hardened fuzzy vaults. The methods of template transformation discussed in chapter 1 of this thesis can also be merged with encryption techniques which would essentially make the system a two-level authentication.

References

[1] Galton, F. "Personal identification and description." *Nature*, 1888: pp 201–202.

[2] Herschel, W. "Skin furrows of the hand." *Nature*, 1880: pp 23:76.

[3] Faulds, H. " On the skin-furrows of the hand." *Nature*, 1880: pp 22:605.

[4] Bock, A. C. O. *Automatic fingerprint machine.* New York: Fingerprint Machine Corporation, 1925.

[5] French., W. K. *Automatic recognition of fingerprints by sensing the skin surface.* New York: International Business Machine Corporation, 1966.

[6] Bledsoe, W. W. *Man-machine facial recognition: Report on a large-scale experiment.* Technical Report 22, Palo Alto, California: Panoramic Research, Inc., 1966.

[7] Altman, N. G. "Palmprint identification system." 1971

[8] Daugman, J. "Biometric personal identification system based on iris analysis." 1994

[9] Privaris inc. http://www.privaris.com/ [Online]

[10] National Bureau of Standards, "Advanced Encryption Standard." U.S. Department of Commerce, Washington D.C., November, 2001.

[11] Ratha, Nalin, Ruud Bolle, " Automatic fingerprint recognition systems.", 2004.

[12] Sainath Maddala, Sreekanth Rao Tangellapally " Implementation and Evaluation of NIST Biometric Image Software for Fingerprint Recognition", September 2010

[13] http://www.biometrics.dod.mil (visited 150309) [Online]

[14] A.Senior. A Hidden Markov Model Fingerprint Classifier. Proceedings of the 31 st Asilomar conference on Signals[C]. Systems and Conputers. 1996, pp.1587-1597

[15] U. Uludag, S. Member, S. Pankanti, and S. Member, “Biometric Cryptosystems: Issues and Challenges,” vol. 92, no. 6, 2004.

[16] A. Juels and M. Sudan, “A fuzzy vault scheme,” Proc. IEEE Int.Symp.Inf. Theory, p. 408, 2002.

[17] J. Linnartz and P. Tuyls, “New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates,” pp. 393–402, 2003.

[18] U. Uludag, “Securing Fingerprint Template: Fuzzy Vault with Helper Data ,” 2006.

[19] U. Uludag, S. Pankanti, and A. K. Jain, “Fuzzy Vault for Fingerprints,” pp. 1–10,2005.

[20] J. Feng, “Combining minutiae descriptors for fingerprint matching,” Pattern Recognit., vol. 41, no. 1, pp. 342–352, Jan. 2008.

[21] A. Nagar and A. Star, “Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors,” pp. 2–5, 2008.

[22] Cancellable Biometrics, Andrew Teoh Beng Jin and Lim Meng Hui (2010) [Online]. Available: http://www.scholarpedia.org/article/ Cancelable_biometrics.

[23] K. Simoens, P. Tuyls, and B. Preneel, “Privacy Weaknesses inBiometric Sketches,” 2009 30th IEEE Symp.Secur. Priv., pp. 188–203,May 2009.

[24] Y. Sutcu, H. T. Sencar, and N. Memon, “A secure biometric Multimedia authentication scheme based on robust hashing,” Proc. 7th Work. Secure. – MM & Sec ’05, p. 111, 2005.

[25] A. Nagar and A. K. Jain, “On the security of non-invertible fingerprint template transforms Abhishek Nagar and Anil K . Jain Department of Computer Science and Engineering Michigan State University,” pp. 81–85, 2009.

[26] H. Chen and H. Chen, “A novel algorithm of fingerprint encryption using minutiae-based transformation,” Pattern Recognit. Lett., vol. 32,no. 2, pp. 305–309, Jan. 2011.

[27] L. Hong and E. Lansing, “On-Line Fingerprint Verification,” pp. 596–600, 1996.

[28] T.-Y. Jea and V. Govindaraju, “A minutia-based partial fingerprint recognition system,” Pattern Recognit., vol. 38, no. 10, pp. 1672–1684,Oct. 2005.

[29] H. Chen, H. Sun, and K. Lam, “A fast and elastic fingerprint matching algorithm using minutiae-centered circular regions,” pp. 211–215, 2007.

[30] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, “Random multispacer quantization as an analytic mechanism for Bio Hashing of biometric and random identity inputs.,” IEEE Trans. Pattern Anal. Mach. Intell., vol.28, no. 12, pp. 1892–901, Dec. 2006.

[31] Z. Jin, A. B. Jin Teoh, T. S. Ong, and C. Tee, “Fingerprint template protection with minutiae-based bit-string for security and privacy preserving,” Expert Syst. Appl., vol. 39, no. 6, pp. 6157–6167, May2012.

[32] A. Ross, S. Shah, and J. Shah, “Image versus feature mosaicing : A case study in fingerprints,” no. April, 2006.

[33] Y. J. Chin, T. S. Ong, a. B. J. Teoh, and K. O. M. Goh, “Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion,” Inf. Fusion, vol. 18, pp. 161–174, Jul.2014.

[34] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and M. K. O. Goh, “Multi modal biometrics based bit extraction method for template security,” 2011 6thIEEE Conf. Ind. Electron. Appl., pp. 1971–1976, Jun. 2011.

[35] M. V. N. K. Prasad and C. Santhosh Kumar, “Fingerprint template protection using multiline neighbouring relation,” Expert Syst. Appl., vol.41, no. 14, pp. 6114–6122, Oct. 2014.

[36] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, “An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbour structures,” Pattern Recognition., vol. 47, no. 3, pp. 1309–1320, Mar.2014.

[37] Pradheeba, Ravi Subban. “Fingerprint Template Protection Techniques - A Survey and Analysis.” IEEE International Conference on Computational

Intelligence and Computing Research, 2014.

[38] G. C. Sharp, S. Member, S. W. Lee, and D. K. Wehe, “ICP Registration Using Invariant Features,” vol. 24, no. 1, pp. 90–102, 2002.

List of Publications

[1] Shamsher Singh Dhillon and Vinod K. Bhalla, ***"A Survey on Fingerprint Template Protection",*** *International Journal of Research in Computer Science (IJRCS) ISSN: 2349-3828,* Volume 04, Issue No. 02 (2017):-100-107[Published].

Fuzzy Vault Encryption

ORIGINALITY REPORT

%7	%3	%7	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ijritcc.org Internet Source	%2
2	Pradheeba, , and Ravi Subban. "Fingerprint template protection techniques — A survey and analysis", 2014 IEEE International Conference on Computational Intelligence and Computing Research, 2014. Publication	%1
3	Bansal, Roli. "Minutiae Extraction from Fingerprint Images - a Review", International Journal of Computer Science Issues (IJCSI)/16940784, 20110901 Publication	%1
4	Chakraborty, Bodhi, Sanjay Singh, and Debanjan Sadhya. "A Review of Key Binding Based Biometric Data Protection Schemes", IET Biometrics, 2016. Publication	<%1
5	jpinfotech.org Internet Source	<%1

6	Maltoni. "Fingerprint Analysis and Representation", Handbook of Fingerprint Recognition, 2009 Publication	<%1
7	www.ijcsmr.org Internet Source	<%1
8	Shi, Z.. "A chaincode based scheme for fingerprint feature extraction", Pattern Recognition Letters, 20060401 Publication	<%1
9	Chillarige, Raghavendra Rao, Mulagala Sandhya, and Munaga V.N.K. Prasad. "Generating cancellable fingerprint templates based on Delaunay triangle feature set construction", IET Biometrics, 2015. Publication	<%1
10	Lecture Notes in Computer Science, 2003. Publication	<%1
11	ijarcsse.com Internet Source	<%1
12	shodhganga.inflibnet.ac.in Internet Source	<%1
13	thinkmind.org Internet Source	<%1
14	Prasad, Munaga V.N.K., and C. Santhosh	

	Kumar. "Fingerprint template protection using multiline neighboring relation", Expert Systems with Applications, 2014. Publication	<%1
15	Indrawan, G., B. Sitohang, and S. Akbar. "Parallel processing for Fingerprint feature extraction", Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, 2011. Publication	<%1
16	Lecture Notes in Computer Science, 2014. Publication	<%1
17	K.L. Ng. "A secure card system with biometrics capability", Engineering Solutions for the Next Millennium 1999 IEEE Canadian Conference on Electrical and Computer Engineering (Cat No 99TH8411) CCECE-99, 1999 Publication	<%1
18	Jin, Z.. "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving", Expert Systems With Applications, 201205 Publication	<%1
19	Chin, Y.J., T.S. Ong, A.B.J. Teoh, and K.O.M. Goh. "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion", Information Fusion, 2013.	<%1