Introduction

With the proliferation of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of computer security. Many cryptographic algorithms are available for securing information [2]. In general, data will be secured using a symmetric cipher system, while public key systems will be used for digital signatures and for secure key exchange between users. However, regardless of whether a user deploys a symmetric or a public key system, the security is dependent on the secrecy of the secret or private key, respectively. Because of the large size of a cryptographically strong key, it would clearly not be feasible to require the user to remember .This encrypted key can be stored on a computer's hard drive. To retrieve the cryptographic key, the user is prompted to enter the passcode, which will then be used to decrypt the key. There are two main problems with the method of passcode security. First, the security of the cryptographic key, and hence the cipher system, is now only as good as the passcode. Due to practical problems of remembering various passcodes, some user tend to choose simple words, phrases, or easily remembered personal data, while others resort to writing the passcode down on an accessible document to avoid data loss. Obviously, these methods pose potential security risks. The second problem concerns the lack of direct connection between the passcode and the user. Because a passcode is not tied to a user, the system running the

cryptographic algorithm is unable to differentiate between the legitimate user and an attacker who fraudulently acquires the passcode of a legitimate user. In order to overcome this problem, some biometric feature-based encrypting/decrypting algorithms have been developed.The palmprint is relatively new biometric feature [8, 9, 10, 11, 12, 13] and has several advantages compared with other currently available features [14] palmprints contain more information than fingerprint, So they are more distinctive palmprint capture devices are much cheaper than iris devices palmprints also contain additional distinctive features such as principal lines and wrinkles, which can be extracted from low-resolution images a highly accurate biometrics system can be built by combining all features of palms, such as palm geometry, ridge and valley features, and principal lines and wrinkles, etc. Therefore, it is suitable to use palmprints to implement a cryptosystem. Up to now, we failed to find any literature to discuss palmprint encryption. In this thesis, we will use error-correcting theory to design a palmprint cryptosystem. When palmprints are captured, the position and direction of a palm may vary so that even palmprints from the same palm may have a little rotation and translation. Furthermore, palms differ in size. Hence, palmprint images should be orientated, normalized before feature extraction, and matching.

Chapter1

Biometrics System

A biometric has defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of biometrics. These days, biometric technologies are typically used to analyze human characteristics for security purposes. Security applications (especially cryptographic systems) need certain private information to authenticate a person's privilege. In the science of biometrics, this private information is replaced by personal information filtered out of human characteristics. These human characteristics are acquired with adequate apparatuses, analyzed and distinct features are extracted. So-called enrollment process a user registers with the system by presenting biometric data to it. The system generates a so-called biometric template for the user and stores it in a database. At the time of authentication, another biometric input is acquired, processed, and compared with the previously stored template in the matching process. This form of authentication provides considerable advantages over simple password-based authentication. As a consequence of this, biometrics are combined with cryptography to enhance security. In the following chapter first the merge of both cryptography and biometrics is pointed out. Then several commonly used biometric characteristics are listed. Afterwards potential variations of these biometric characteristics are explained (section. Then the fundamentals of a so-called biometric authentication system are explained in detail (Section1.3). Subsequently

the terms biometric key (Section 2.5), biometric template (Section 2.6) and biometric hash (Section 2.7) are declared.

1.1 Biometric Characteristics

There are several biometric characteristics for various applications. However, each of these biometrics has its strengths and weaknesses and therefore the choice of the biometric depends on the application [47]. Furthermore, to make use of these biometrics one must figure out which human characteristics are the most suitable for the required application and how to use the features these characteristics provide. Each of these biometrics are acquired using different apparatuses [29]. Therefore the matching process of a biometric authentication has to be adapted to the biometric characteristic. Additionally, the choice of the biometric input has an influence on several magnitudes such as the performance of the whole system

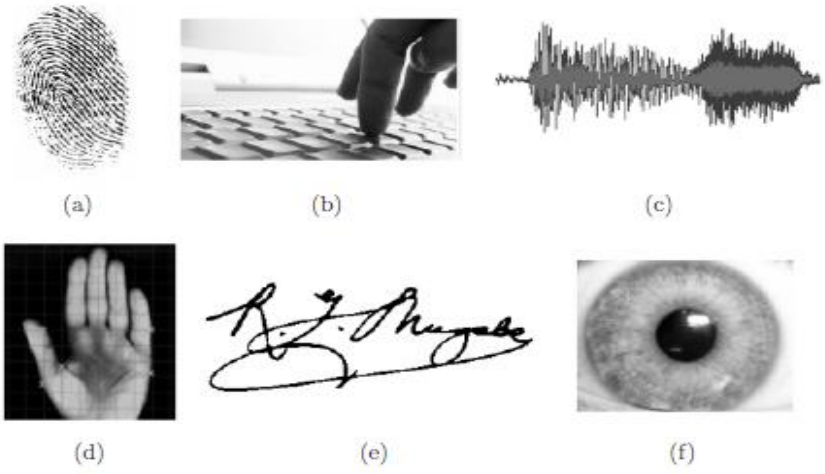


Figure 1.1: Examples of physiological (static) and behavioral (non-static) biometrics fingerprints (b) keystroke dynamics (c) voice (d) hand geometry (e) signature (f) iris.

Over the years several characteristics have been established, which can be classified as follows:

Physiological (static) characteristics: These are characteristics related to the nature of the human body such as fingerprints, face, hand geometry or the iris. In other words, a person can hardly influence these characteristics. Furthermore, these characteristics do not change over time. These characteristics only change under special circumstances, for example, injuries could change a person's hand geometry.

Behavioral (non-static) characteristics: These are characteristics related to the behavior of a person such as signature, voice, or keystroke dynamics. These characteristics do change slightly over time, for example, the signature of a person could change over the years. One can imagine that behavioral characteristics are more easily to forge, for example, an imposter could learn to imitate a person's signature. In the following subsections, the properties of some physiological as well as behavioral characteristics are outline. Most commonly used biometrics is shown in Figure 1.1. Subsequently, the way of how these biometric characteristics are acquired, and which features of these characteristics can be extracted is explained.

1.1.1 Fingerprint Recognition

To start with, physiological characteristics, fingerprints are the oldest traits, which have been used for more than a hundred years. In fingerprint authentication systems, mostly friction minutiae-based features are used while systems are rarely designed to use an entire image of a fingerprint [48, 42]. Therefore, the result of a common fingerprint authentication system's data acquisition (scan) would be a set of minutiae points. These

so-called minutiae are skin ridge impressions of fingers, which only slightly change over time. These minutia points serve as biometric features and are compare to each other in the matching process. This means there is a whole set of features which has to be compared to another set of features while it is not sure if during the capturing of a person's fingerprint the whole set of features is recorded or just a small subset due to bad quality of the fingerprint. The main difficulty within fingerprint biometrics is the inability to show normalizes fingerprint data, for example, by finding specific fingerprint orientation and its center. If fingerprint data is not normalized, then all calculations resulting out of minutiae are destined to be orientation/position-dependent. The way to overcome this difficulty is to have the matching algorithm deal with transformations of fingerprint data. Much work has to be done to solve the problem of aligning fingerprint images including the use of high curvature points and orientation lines. Another challenge is to deal with low quality images of fingerprints, which in the worst case do not include distinct features (minutiae points) necessary for the matching process. Enabling a system to authenticate a person if only a subset of features is capture during the acquisition of the fingerprint is still a topic of research.

1.1.2 Iris Recognition

Another physiological characteristic is a person's iris, the sphincter around the pupil of a person's eye. Data acquisition is performed with a special camera (iris scanner) which is able to capture the iris of a person's eye [7]. Thus, one disadvantage of using iris scans for authentication is that all persons to be authenticated have to fully cooperate with the system. Breakthrough work to create iris recognition algorithms required for image

acquisition and matching were developed by J. G. Daugman [18, 19], University of Cambridge Computer Laboratory. Daugman's algorithms for which he holds key patents are the basis of all todays commercially used iris recognition systems. The algorithm of filtrating information out of such an image of a person's eye involves several steps, which can be summarized as follows:

First, the iris has to be extracted out of the whole image of the person's eye. Therefore, the center of the iris and the inner and outer boundaries has to be detected. This detection has to be performed carefully because of the dynamic dimension of the pupil and dilation of the person's eyelid. To solve this problem Daugman proposed a method called exploding circles" The main idea of this concept is that there are strong changes of brightness in the image at these boundaries, which can be detected using circular integrals. In the beginning, an initial center of the pupil is approximated. Then circular integrals are calculated. The derivation of such integrals is very high at the boundaries where the brightness changes drastically. So applying this method for an approximated center, radii to the boundaries between the pupil and the iris and between the iris and the sclera are calculated. These radii are then used to compute a new center of the pupil and the whole method is applied again until convergence is achieved. In the next step so-called analysis bands" are defined for the extracted iris (in form of a ring). These bands are used to position points, which are, then explored using 2D Gabor filters. These 2D Gabor filters are designed to denoise the acquired signal. This process must not be confused with the smoothing of a signal. Then iris ring is unwrapped by mapping polar coordinates to Cartesian-coordinates, which results in a rectangular image. In the

rectangular image the radii of the previously defined analysis bands is fixed and every explored point is a center of a 2D Gabor wavelet.

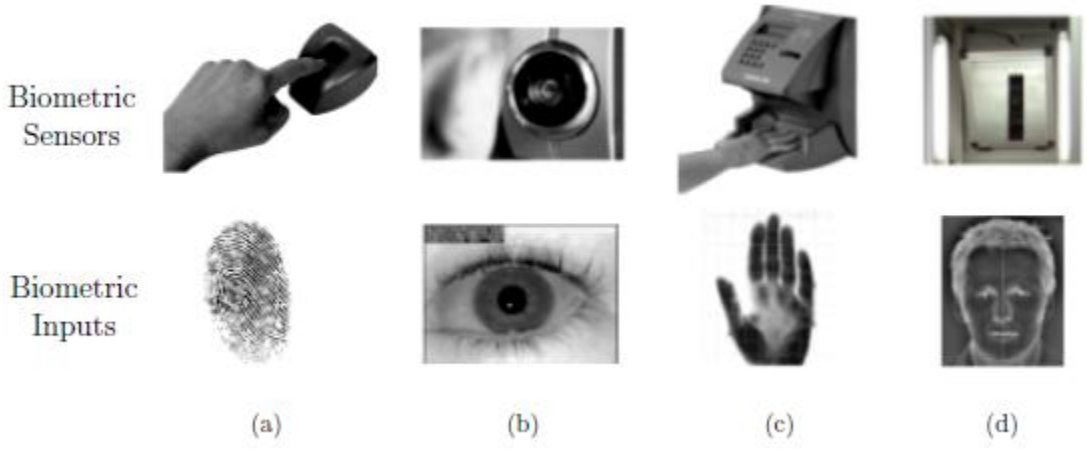


Figure 1.2: Examples of biometric sensor and the according biometric inputs for physiological (static) biometrics: (a) fingerprints (b) iris (c) hand geometry (d) face.

For this wavelet, the coefficients are generated out of which two bits are extracted. This method is applied again until enough bits are extracted. The rectangular image of the iris mostly includes some part of the eyelid and eyelashes. Eyelashes are seen as noise, which have to be detected during the unwrapping of the iris. This is done by calculating a bit-mask where one bit represents a region of the iris and is set to 0 if any noise is detected and otherwise to 1. Other forms of noise could be, for example, camera pixel noise or specular region. The result of the whole procedure is a so-called iris-code (for example 2048-bit long in J. G. Daugman's approach). This iris code serves as a biometric template, which can be stored in a database together with the bit-mask. After the extraction of the iris-code, the matching process can be performed using several metrics, for example, the Hamming distance. This could be easily done by just bitwise XORing two iris-codes and comparing the number of mismatching bits to a specific threshold. In a

face recognition system images of the whole face of a person are captured out of which unique key features are extracted to identify persons reliably [14, 22]. The acquired set of keys features includes relative distances between characteristics such as eyes, the nose, the mouth cheekbones, and the jaw. Using all of this information a unique template is created by applying dimension reduction. In generic face recognition systems, this is done by applying, for example, Eigenfaces [38]. This template may then be compared to databases of facial images to identify a person. While a face-recognition system has high acceptance, its accuracy is low [25]. The problem arises mainly from three factors: insufficient capability of representing features in the feature space and within-class and between-class variations. Most face recognition systems are highly sensitive to variance of a person's face. Unfortunately, there is plenty of variation, for example small movements of the head or changing haircuts. Thus, dimensionality reduction is performed to improve the capability to represent features and harmonizing the image taken.

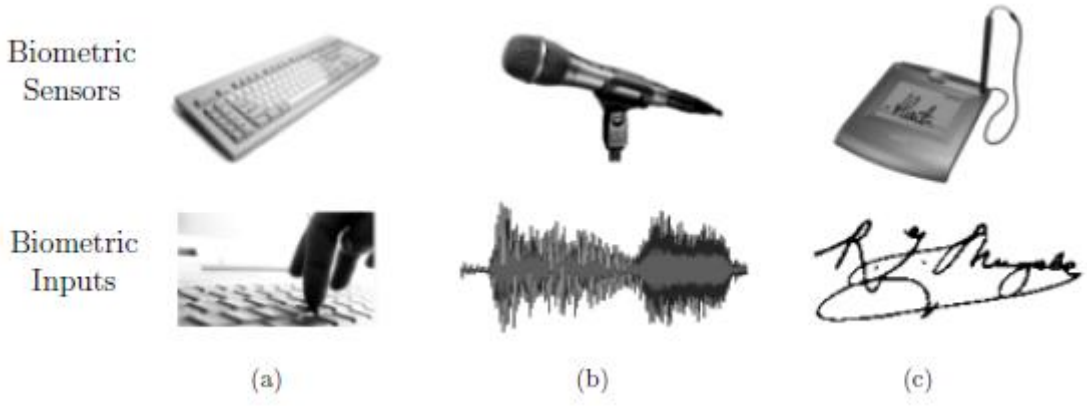


Figure 1.3: Examples of biometric sensor and the according biometric inputs for behavioral (non-static) biometrics: (a) keystroke dynamics (b) voice (c) on-line signatures.

1.1.3 Hand Geometry

Hand geometry is a biometric that identifies users by the shape of their whole hand. For data acquisition, so-called hand geometry readers are used to measure a user's hand along many dimensions [26, 36]. These measurements serve as features, which are used to authenticate a user comparing these against previously stored ones. Since hand, geometry is not thought to be as unique and widespread as fingerprints, remains the preferred technology for high-security applications due to various forgery opportunities such as changing lengths of fingers with caps. Thus, it is advisable using hand geometry combined with fingerprints to form a so-called two-factor authentication system.

1.1.4 Speaker Recognition

One biometric characteristic, which tends to be very difficult to handle is voice. On the one hand, voice biometrics is behavioral characteristics because it depends on the way a person talks (pronunciations, volume of speech). On the other hand, the voice can be seen as a physiological characteristic of a person as well. Data acquisition is first performed during the enrollment process where a person utters a password or passphrase to a device (usually a microphone) when prompted to do so. This signal is digitalize with an analog to digital converter and subsequently analyses resulting in a so-called voice model of a person [10]. In the authentication process, the repeated utterance of the same password by the same person should authenticate a legitimate user. If a correct password is necessary, the whole system is called token-based [49, 50]. Uttering an incorrect password (token) the user will be rejected. Solving this difficulty voice authentication would offer many facilities, for example, a person could be identified during a phone call. However, a

forgery could still attempt to record a person to gain possession of a password. Voice is one human characteristic where the temporal order of the feature is important which is typical behavioral biometric characteristics.

1.1.5 Signature Verification

Speaking of signatures as a biometric characteristic of a person one has to distinguish between so-called off-line" and on-line" signatures: Off-line signatures are for example signatures on documents where nearly only spatial information" such as features of curves can be analyzed to identify a specific person, which is very unsatisfying. This is because off-line signatures refer to the result of a complete writing process. In other words, there is no information but the raw image of the signature. This image can be modified with the technique of dynamic time warping to correlate the result with other acquired off-line signatures [26]. Furthermore, shape matching can be performed. On-line signatures are signatures, which are acquired using a palm or tablets. Therefore, access to signals during the writing process, so-called temporal information, is demanded [9, 32, 45]. This means using on-line signatures the physical activity of signing measured and analyzed. By doing so many additional signals are offered which can be analyzed to identify a person. These signals include the position of the pen, the time, the angle of the pen and the pen pressure. Additionally the analog- digital conversion is performed. Some important features calculated out of these signals are for example the number of pen-ups/downs, the average of absolute writing acceleration in y-direction, the effective average writing velocity in x-direction and the time it took the person to sign . Thus there are plenty more features to analyze with on-line signatures.

1.1.6 Keystroke Dynamics

Keystroke dynamics is another behavioral biometric characteristic, which could be additionally used to identify a person. For data acquisition the keyboard serves as biometric sensor with which two events, the key down" and key release" event, are measured. Every user develops a specific timing pattern when typing a password called keystroke dynamics. Duration and latencies of a user's keystroke dynamics are measured by the authentication system to enhance security. This means the correct password is necessary but does not suffice any more if the keystroke dynamics are measured as well. Very distinctive durations can be measured out of letters often following behind each other such as the “th" in an English password for example. Problems occur within a system, which used keystroke dynamics as a biometric characteristic when keyboards are changed or if a user suffers from a hand injury. The approach of using keystroke dynamics is a simple example for combining the knowledge of something with a biometric characteristic.

1.1.7Hybrid Biometrics

Hybrid biometrics also called multi-factor authentication scheme is an approach to enhance security by combining two or more biometric characteristics. A weighted set of biometric characteristics of a person could be used for identification, for example the image of a person's face and a spoken password could be combined. By doing a forgery attempt, become nearly impossible. Merging features of two or more biometric characteristics still seems to be a tough challenge and even more an intelligent weight age of these characteristics and how a set of authentication processes are combined to form

one hybrid system. Furthermore, hybrid biometrics can be used if one of the biometric characteristics is not available from a person, for example, due to an accidental injury so that there have to be other ways for authentication.

1.1.8 Other Biometric Characteristics

There are plenty more biometric characteristics such as physiological characteristics like a person's retina or DNA or behavioral characteristics like gait or lip movement. However, on these biometric characteristics only little research has taken place in terms of combining these characteristics with a cryptographic authentication system.

1.2 Biometric Authentication Systems

A biometric authentication system is a system, which is able to perform automated authentication of users depending on their physical and behavioral characteristics (Section 1.7.). Such an authentication system consists of several basic entities:

- **Biometric Sensor:** the biometric sensor performs the data acquisition and therefore the analog to digital conversion. The outputs of the biometric sensor are the raw biometric data. The sensor is used at the enrollment of a user and every time a user needs to be authenticated.
- **Feature Extraction:** In the feature extraction, the raw data are processed and analyzed. The result of the feature extraction should be the most distinctive features for every user
- **Database:** In almost all biometric authentication systems, a database is required. This database is used either to store cryptographic keys which are released when an authorized

user represents biometric features to the system or the database could store raw biometric features or a hash value of these.

• **Matcher:** the biometric matcher is responsible for the matching process which should

As mentioned before in some way be tolerant but should not provide any security leakage. Matching is performing whenever a user needs to be authenticated. The two basic processes of biometric authentication system are the enrollment" process and the authentication" process. In the enrollment phase of a biometric authentication system, all Users are registered with the system, and references are stored in the database of the system. On the other hand, the authentication process denotes the process of identity verification or determination. In this phase the authentication system performs a comparison between the presented biometrics and the stored references of the previous enrollment phase.

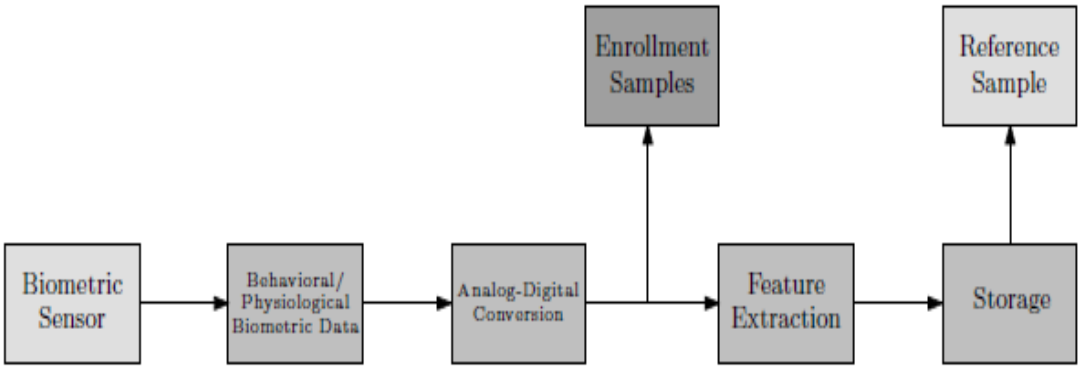


Figure:1.4 Authentication process: collected data is compared to reference data

1.2.1 Enrollment

In the enrollment phase, as shown in Figure 1.3, a user's biometric data is presented to the authentication system for the first time. This analog data, depending on the biometric

characteristic, then needs to be digitalized for further use. The results of this analog-digital conversion are so-called enrollment samples". These samples are then preprocessed, features are extracted and the extracted features are then stored in databases. In most biometric authentication systems not just one but several data acquisitions are performed during the enrollment of a single user. With the help of several biometric sample magnitudes such as standard and mean deviations of biometric features can calculated and thus a more representative sample can calculated or boundaries can be generated for these features. Furthermore, the acquisition of several samples can used to filter out the most stable features where deviation values are small. Thus, common biometric authentication systems demand at least two or three biometric samples of a user during the enrollment process.

1.2.2 Authentication

After a user has been enrolled, the biometric authentication system should be able to authenticate the user as illustrated in Figure 1.3. Once again, biometric data is presented to the system and digitalized. The obtained data, the so-called verification samples" which are of the same (raw) data format as the enrollment samples resulting out of the enrollment phase, are preprocessed and features are extracted. In the matching process, the derived features are then compared to the template resulting from an earlier enrollment process. If the matching succeeds, then the user is authorized, otherwise the user is rejected.

1.2.3 Verification and Identification

There are two modes in which a biometric authentication system can operate, namely verification" and identification". In the first mode a user claims to be someone who needs to be verified and thus only an one-to-one comparison has to be performed by the biometric authentication system while in the second mode a user needs to be identified and therefore a one-to-many comparison has to be performed. Furthermore, the process of identification can be modeled as sequences of one-to-all verification and therefore the fundamental underlying mechanism is always verification.

1.2.4 Performance Measurement

Due to the fuzziness of the matching process of biometric systems several errors occur. In generic biometric verification, systems there are two main types of errors:

- Misrecognizing measurements of two persons to be of the same person, called false acceptance".
- Misrecognizing measurements of the same person to be of two different persons, called false rejection".

The performance of a biometric system is commonly described by its false acceptance rate" (FAR) and false rejection rate" (FRR). The FAR and FRR are commonly accepted and quoted in almost all publications concerning biometric authentication systems.

These two measurements can be controlled by adjusting a threshold, but it is not possible to exploit this threshold by simultaneously reducing FAR and FRR [39]. For example, if an authentication scheme tends to be tolerant with respect to accepting similar biometric

data, the FAR of this system will be very high while the FRR would be satisfying. Another important performance index of a biometric system is its equal error rate" (EER) defined as at the point where FAR and FRR are equal. A perfect system in terms of Accuracy would provide an EER of zero. Unfortunately, however, over several years of investigation, a perfect biometric verification system has not been developed. Additionally the FRR/FAR numbers quoted by biometric vendors are often unreliable. In most cases, these values were calculated under unrealistic circumstances or several presumptions were taken which do not hold in practice. Beyond that, there are some other commonly used measures for technical evaluation of a biometric system including the above measurements and furthermore, False Match Rate False Non-Match Rate, Receiver Operating Characteristic, Failure to acquire Rate and the Failure to enroll Rate.

1.3 Biometric Keys

In the sense of cryptography, a key is a piece of information with which one is able to encrypt a plaintext into a so-called cipher text and vice versa during the decryption process. In biometrics, it is aimed at deriving a cryptographic key from one or more biometric samples during the enrollment phase of the biometric authentication system. This key may later be regenerated using another biometric sample that is close to the original samples. The basic idea of biometric-based keys is that the biometric component performs user authentication, while a generic cryptographic system can still handle the other components of containment such as secure communication .The result of the data acquisition are raw biometric data, which further processed in the feature extraction step. The result of the feature extraction is a set of features called feature vector", denoted by

ϕ. This feature vector ϕ, consists of k features ϕ_i . Such that $\Phi = \{\phi_1, ..., \phi_k\}.$ every ϕ_i represents the value of a measured feature of a user. For generating a cryptographic key of a specific length m out of this set of collected features it requires that there be a way of mapping ϕ to a so-called “feature descriptor" b of length $m: b = (b_1, ..., b_m)$ where $b_i \in \{0,1\}$ and $m \leq k.$ This is mostly done by applying functions which match the ϕ_is of ϕ against some thresholds specified by the system [49, 52]. One very simple way of generating such a feature descriptor would be to obtain the i-th bit b_i of the feature descriptor b by comparing ϕ_i to a fixed threshold and assigning bi to be 1 or 0 depending on either ϕ_i was less than or greater than the threshold. Nevertheless, this simple approach rarely suffices in practice. Once feature descriptors are derived these should separate persons in the sense that descriptors produced by the same user are “sufficiently similar" so that there is a small “intra-class" variation, but ones produced by different users are “sufficiently different" so that there is a large “inter-class" variation. If this property is satisfied, and the features can be reproduced reliably, then the feature descriptor could be a candidate for use as a person's biometric key. Looking at a person's biometric characteristics (see Section 2.2) one can imagine that the variations of these characteristics take a huge influence on this procedure and therefore the challenge in generating such keys lies in finding those features, which are highly consistent from one measurement to another but still, tend to be distinctive for the particular person. Beside the property of separating users, there are other important requirements for creating such a biometric key. The most important requirements can be summarized as follows:

Key Randomness

Key privacy

Key entropy (strength)

Key uniqueness

Key stability

1.4 Biometric Templates

In cryptography, a hash function is a reproducible method of turning some kind of data into a (relatively) small number that may serve as a digital “fingerprint" of the data. Hash functions are designed to be fast and to yield few hash collisions in expected input domains. In hash tables and data processing, collisions inhibit the distinguishing of data, making records more costly to find. A hash function must be deterministic, which means if two hashes generated by the same hash function are different, then the two inputs are different in some way. Hash functions are usually not injective, thus the computed hash value may be the same for different input values. This is because it is usually a requirement that the hash value can be stored in fewer bits than the data being hashed. It is a designated goal of hash functions to minimize the likelihood of such a hash collision. A desirable property of a hash function is the mixing property: a small change in the input should cause a large change in the output. This is called the avalanche effect.The goal of a biometric hash function is to find a function for mapping biometric features into a value space of defined dimensionality, adopting three of the key properties of cryptographic hashes: Mapping from a (very) large value domain to a smaller value space. Infeasibility to find input that maps pre-specified outputs. Infeasibility to find any

two distinct biometric signal inputs originating from any two different users, which map to the same output. Biometric templates (see Section 1.5) do not satisfy security requirements because of several vulnerabilities. According to storing a collection of extracted features of a user's biometrics, this set of features could be transformed by a hash function H into a so-called hash value H(ϕ) .This transformed version of collected features H(ϕ) could be stored as a so-called “private template" during the enrollment process [11]. When a user wants to authenticate to the system, again features are collected, hashed, and compared to a hashed template of an earlier enrollment process. Therefore, the matching process is performed in another space and if a user's template is ever compromised, a new space for the matching process can be issued by just changing the hash function H.

1.5. Security Vulnerabilities of a Biometric System

Biometric systems, especially *one-to-one*, may become vulnerable to potential attacks. Some of those security vulnerabilities include the following:

• **Spoofing.** It has been demonstrated that a biometric system sometimes can be fooled by applying fake fingerprints, face or iris image, etc.

• **Replay attacks,** e.g. circumventing the sensor by injecting a recorded image in the system input much easier than attacking the sensor.

• **Substitution attack**: The biometric template must be stored to allow user verification. If an attacker gets an access to the storage, either local or remote, he can overwrite the legitimate user’s template with his/her own in essence, stealing their identity.

• **Tampering:** Feature sets on verification or in the templates can be modified in order to obtain a high verification score, no matter which image is presented to the system.

• **Masquerade attack.** It was demonstrated10 that a digital "artefact" image can be created from a fingerprint template, so that this artefact, if submitted to the system, will produce a match. The artefact may not even resemble the original image. This attack poses a real threat to the remote authentication systems (e.g. via the Web), since an attacker does not even have to bother to acquire a genuine biometric sample. All he needs is just to gain an access to the templates stored on a remote server (this perfectly fits a description of a typical hacker operating from a rat hole).

• **Trojan horse attacks:** Some parts of the system, eg. a matcher, can be replaced by a Trojan horse program that always outputs high verification scores.

• **Overriding Yes/No response:** An inherent flaw of existing biometric systems is due to the fact that the output of the system is always a binary Yes/No (i.e., match/no match) response. In other words, there is a fundamental disconnecting between the biometric and applications, which make the system open to potential attacks. For example, if an attacker were able to interject a false Yes response at a proper point of the communication between the biometrics and the application, he could pose as a legitimate user to any of the applications, thus bypassing the biometric part.

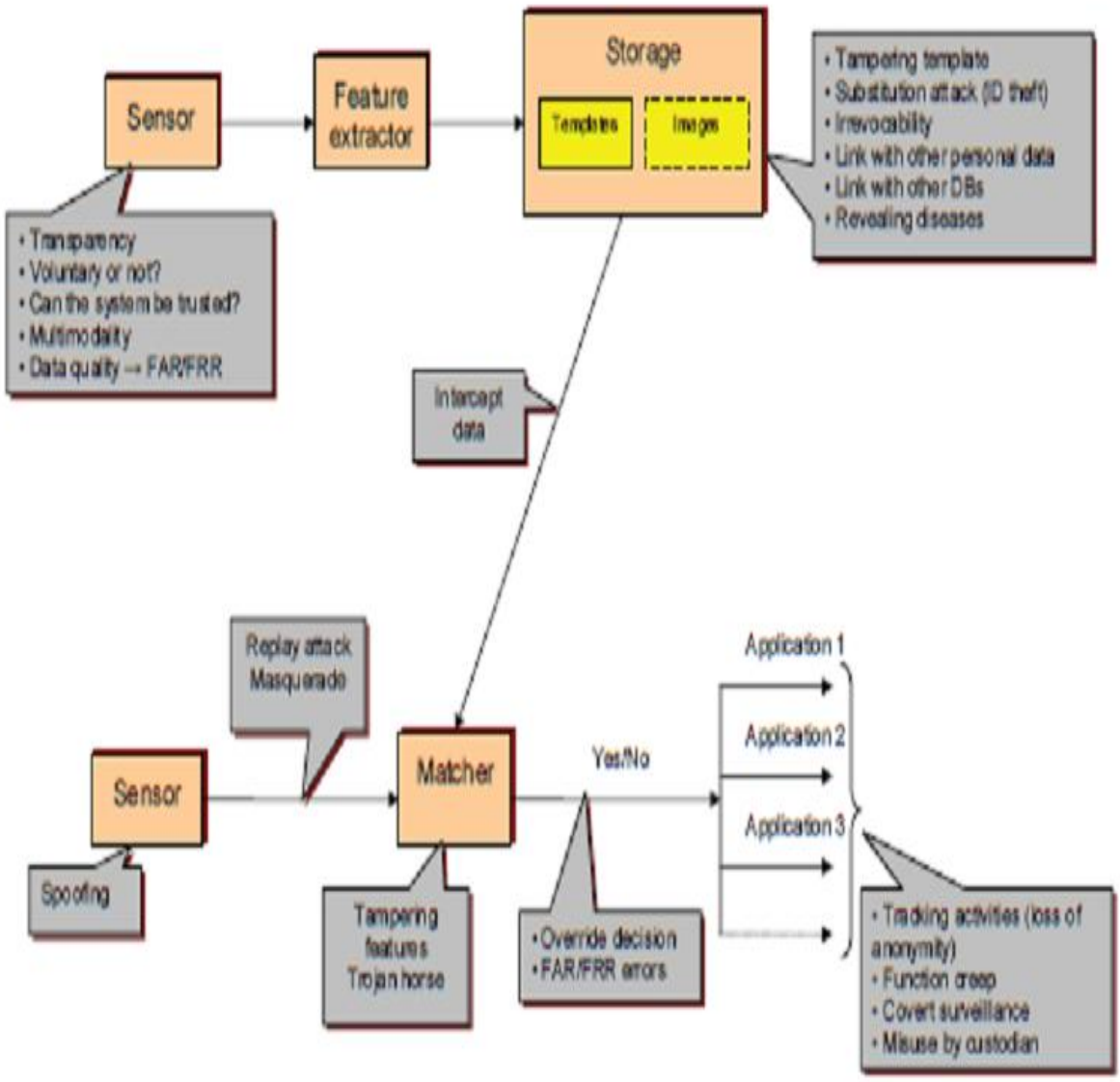


Figure 1.5

Privacy and security issues involving a biometric system

Chapter 2

Merging Biometrics with 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 [52]. Decryption is the reverse, moving from unintelligible ciphertext to plaintext. 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.

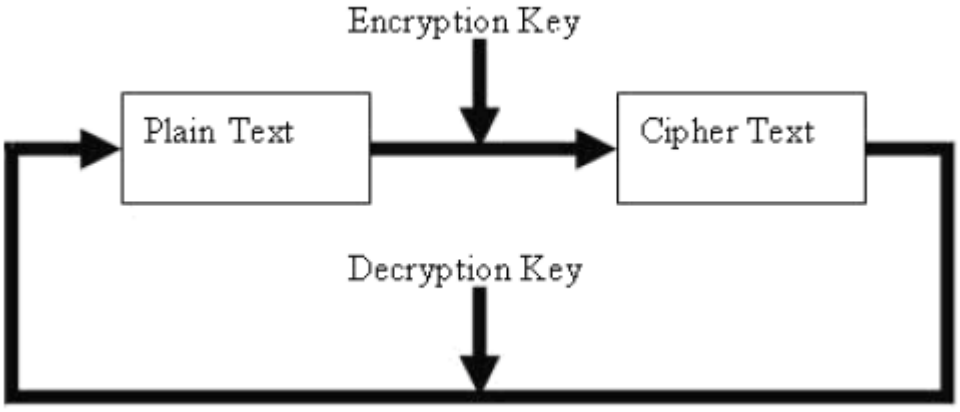


Figure2.1

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.

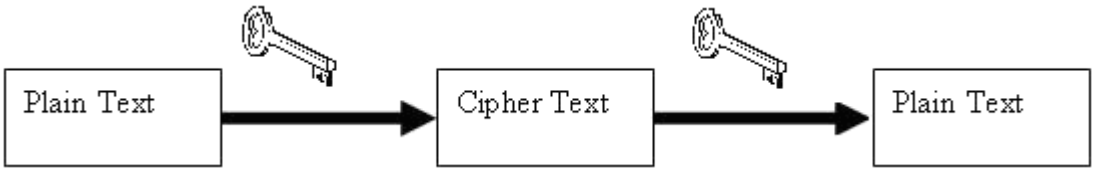


Figure 2.2. (a) Secret Key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

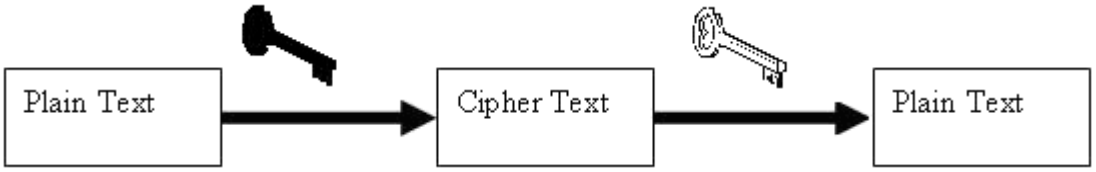


Figure 2.3 (b) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption/decryption

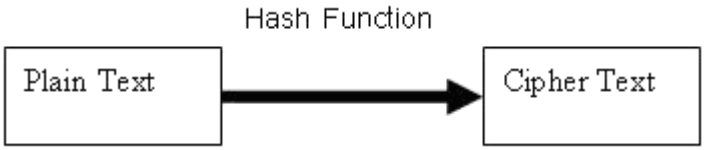


Figure 2.4 (c) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

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

2.1 Biometrics with Cryptography

Cryptography is a very important field in the science of computer security. Many cryptographic algorithms are available for securing any kind of information. For all traditional algorithms, the security depends on the secrecy of the secret or private key when a person deploys a symmetric or a public key system, respectively. The person chooses a password that is used to encrypt the cryptographic key and this key is then stored in a database (these keys are long, random, and thus hard to remember). In order to retrieve the key back, the person enters the password, which will then be used to decrypt the key. This means the authentication (decryption) in such a cryptographic system is possession-based. The possession of the decrypting key ensures that the user is legitimate. This is one security leakage in generic cryptographic systems, which can be avoided by introducing biometric authentication. In general cryptographic systems two different types of systems can be distinguished, namely symmetric systems, where all participants of the secret communication share the same secret key, and public key systems, where pairs of a private key and a publicly available key are used to encrypt and decrypt secret information. While systems of the first category are typically designed for efficient cipher systems, the second type is used mainly in digital signatures or protocols to securely exchange secret session keys. As cryptographically strong keys are rather large, it is certainly not feasible to let users memorize their personal keys. Because of this digital key are typically stored on smart cards or in databases and retrieved through password-based authentication as mentioned previously. Since the password is not directly tied to a person, the system is unable to differentiate between a legitimate person and an attacker. Additionally, the security of the cryptographic key is weak due to

practical problems of remembering various passwords or writing them down to avoid losing data and furthermore, passwords can simply be guessed by attackers (especially those which depend on social circumstances).Thus key management systems are the first field where biometrics can be introduced to enhance security. Several approaches have been made attending to secure password-based storage of cryptographic keys. The authentication procedure can simply be replaced through biometric authentication [35, 36]. Depending on the biometric characteristic that is used to retrieve the key the level of security is increased. Another way of introducing biometrics would be to strengthen the already existing password by means of biometrics to form a kind of two-factor authentication system [49, 52] instead of replacing the password. A biometric input can even be used directly to generate a cryptographic key or a biometric hash out of it. In conclusion, key management is the major point in the science of cryptography where biometrics can be applied to enhance the security of the system. Still there are several ways in which biometrics can be used to build a cryptographic key management system which implies there are many different types of biometric cryptosystems and these use different types of human traits. In the following subchapter, most of these will be discussed in order to give an overview in how to use these different types of human characteristics for security purposes.

2.2 Classification of Biometric Cryptosystems

Over the years, a commonly accepted classification of biometric cryptosystems has been established. Two different types of biometric cryptosystems, namely key release schemes and key generation/binding schemes, can be specified as follows:

2.2.1 Key Release Scheme:

The biometric authentication is completely decoupled from the cryptographic part of the system. Thus, the user's key and the biometric data are independent of each other, which is the major benefit of the key release approach. In the authentication process acquired, biometric data is compared against a reference template acquired during enrollment. If this comparison succeeds with respect to some applied metric, the cryptographic key is given to the user. Therefore this key could easily be modified or updated at any time in case it is compromised, which means key release schemes provide cancellable biometrics.This is an easy approach, which could be for example realized with fingerprint biometrics. A user could present a fingerprint to the system, which matches the acquired samples against a stored fingerprint template and if the matching succeeds, gives a key to the user. Nevertheless, key release schemes are not frequently used although it would be easy to implement a biometric cryptosystem with this approach because of the following vulnerabilities:

(a) The biometric template, which is not secure, has to be stored in a database. This is a very critical subject because biometric templates could be stolen.

(b) Due to the fact that authentication process and the key release are decoupled it would be possible to manipulate the biometric matching process.

(c) The cryptographic key has to be stored as part of the template. Therefore, a biometric cryptosystem based on the key release scheme is not appropriate for high security applications.

2.2.2 Key Generation/Binding Scheme

In the key generation scheme the user's key is directly derived from the user's biometric data (biometric key) and therefore does not have to be stored anywhere. This means a user presents biometric data to the system, which generates a key out of the extracted features. This key is then given to the user who could use it to, for example, encrypt private data. The major problem seems to be that in this approach a key could not be changed if it was compromised once. To achieve the benefits of a biometric cryptosystem with cancellable keys it is common to combine the user's biometric data with the cryptographic key. For example, a reference sample of a user's biometrics combined with this key could be stored as biometric template. During the authentication, process biometric data is presented to the system with which the key can be detached from the stored template. A more secure environment is provided by combining the key and the template together, which on the other hand makes it a bit more difficult to implement with provided that key .It is intelligently mixed with the biometric data. Therefore, it is harder for an adversary to get into the possession of the user's key or the biometric template because these will not appear raw in a database. Additionally the biometric matcher performs authentication and key release in a single step.

2.2.3 Cancellable Biometrics

Unlike simple PINs or passwords, biometric characteristics are permanently associated with a person and cannot be changed. Thus, a great disadvantage comes up with biometric cryptosystems based on the classic key generation scheme. Here the cryptographic key is directly derived from a person's biometrics, which means, if the

biometric data is stolen, for example by capturing images of a person's iris or by recording a person's voice, the biometric data becomes useless and is lost forever. Furthermore, biometric data becomes useless for all applications it was used because a person can potentially be tracked from one application to the next by cross-matching databases. To overcome this disadvantage an intermediate step has to be established, which adds secret information. A commonly used approach is to apply transform functions to the biometric data. If a transformed sample of a person's biometrics is compromised only the transform function, which is either directly applied to the biometric data in the signal domain or later when the biometric features have already been extracted, has to be changed. The most important condition these functions have to fulfill is inevitability so that neither the comparison of transformed data to the raw nor the comparison to another transformed sample reveals any useful information.

2.2.4 Error Correcting Codes

Another way to repress the fuzziness of biometric measurements is to introduce error-correcting codes. The goal of an error correcting code is to transmit a message "m" through a noisy communication channel so that no information is lost [36]. To achieve that, "m" is mapped to a longer string c with the property of correcting single bit errors up to a specific threshold depending on the length of c. With the ability of error correction the receiver can reconstruct c out of a received c' and thus is able to calculate the intact message m for formalized an error correction code contains a large set of codeword's $C \subseteq \{0,1\}^n$. If an l-bit message m has to be transmitted, where l < n is necessary, a function $g: M \to C$ has to be defined. Here $M = \{0,1\}^l$ represents the

message space while g is a one-to- one mapping from messages of M to codeword's of *C*. Furthermore, a decoding function $f : \{0,1\}^n \rightarrow C \bigcup \{\emptyset\}$ is needed which maps a codeword of the received message to it's "nearest" codeword in C or if this is not possible, puts out $\emptyset$ to indicate decoding failed. Error correcting codes can be used to overcome the fuzziness of biometric measures as well: for example, denote $b \in \{0,1\}^n$ a feature descriptor resulting out of a biometric measurement and $k \in \{0,1\}^l$ a cryptographic key with which the feature descriptor should be combined. First the representation of *k* in *C* is calculated, *k'=g* (*k*) and afterwards the bitwise XOR of k0 and the feature descriptor b, $\hat{b} = b \oplus k'$, is computed. The XORing of these two-bit streams represents the binding of the cryptographic key with the user's biometrics. This is first done during the enrollment process and the combination of the user's biometrics and the key is then stored in a database as biometric template. During the authentication process a person presents biometric data to the system, a feature descriptor b' is extracted and $b' \oplus \hat{b} = b' \oplus b \oplus k' = k''$ is calculated. In the end the decryption function *f* is applied and if *f* (*k''*) = *k* the authentication succeeds. Thus, the error correcting code is used to overcome some bit errors, which were produced due to the variance in the captured biometrics. This means, it is assumed that if two biometric measurements are from the same person, these are sufficiently similar so that only some bit errors occur, which can be corrected with common error correcting codes. One class of most commonly used error correcting codes is so-called "Reed-Solomon" codes [33]. Reed Solomon codes are well-established codes based on polynoms, where message of length *l* to be encoded is represented as the evaluation of a polynom of degree *l*-1. Another class of error

correcting codes are so-called “Hadamard Codes”. These Codes use special kind of matrices to detect/correct single bit errors.

2.3 Advantages of Biometric Cryptosystem

BC technologies can enhance both privacy and security in the following ways:

There is no retention of biometric image or conventional biometric template, and they cannot be recreated from the stored helper data. The BC templates from different applications cannot be linked. The BC template can be revoked or canceled. They can be easily integrated into conventional cryptosystems, as the passwords are replaced with longer digital keys, which do not have to be memorized. They provide improved authentication and personal data security through a stronger Binding of user biometric and system identifier The BE systems are inherently protected from substitution attack, tampering, Trojan Horse attack, overriding Yes/No response, and less susceptible to masquerade attack. They are suitable for large-scale applications, as the databases will store only untraceable, yet sufficient, information to verify the individual claim.

2.4 Possible applications and uses of Biometric Encryption

Three-way check of travel documents Anonymous databases that is, anonymous (untraceable) labeling of sensitive records (medical, financial) Consumer biometric payment systems. Remote authentication via challenge-response scheme Access control (physical and logical) personal encryption products. Local or remote authentication of users to access files held by government and other various organizations Biometric boarding cards for travel

Chapter3

Literature on Biometric Cryptosystems

3.1Biometric Encryption

In the following the first approaches of using biometric together with cryptography, resulting in an algorithm called Biometric Encryption TM are described. The goal of this algorithm is to provide a mechanism for the linking and subsequent retrieval of a digital key using a biometric such as a fingerprint. In this algorithm, a filter function is generated with the use of correlation, which should consistently produce the same output pattern for a legitimate user. This output pattern is linked with a cryptographic key during the enrollment process using a so-called linking algorithm, which generates a look-up table. Furthermore, out of the key an identification codes are generated and stored together with the filter function and the look-up table. If the user wants to retrieve this key the user's biometric is captured, another output pattern is generated and a key is retrieved via a look-up table. Out of the retrieved key, another identification codes are generated and matches against the stored one. The whole process of the Biometric Encryption TM algorithm is displayed in Figure 1.3. The prior idea of generating a personal cryptographic key out of a person's biometrics was presented in a German patent by Bodo [6]. In Bodo's approach a key was directly derived from a person's biometrics, thus this method would function as a pure key generation system including the disadvantage of not being able to update the key, in case a person's biometric was comprised.

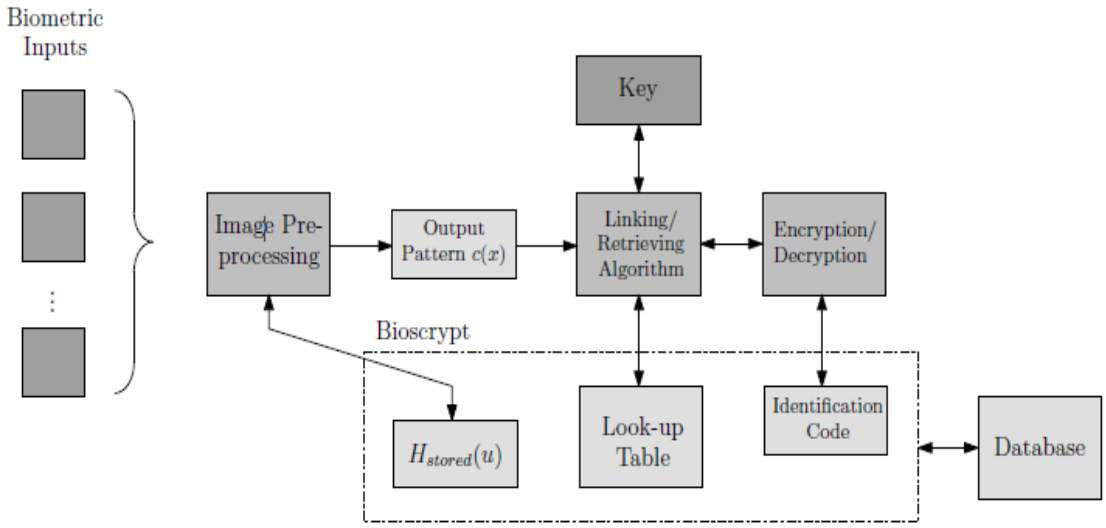


Figure 3.1.The basic operating mode of the Biometric Encryption algorithm

User wants to retrieve these key the users biometric is captured, another output pattern is generated and a key is retrieved via a look-up table. Out of the retrieved key another Identification code is generated and matches against the stored one. The whole process of the Biometric Encryption TM algorithm is displayed in Figure The prior idea of generating a personal cryptographic key out of a person's biometrics was presented in a German patent by Bodo [6]. In Bodo's approach a key was directly derived from a person's biometrics, thus this method would function as a pure key generation system including the disadvantage of not being able to update the key, in case a person's biometric was comprised. This was the first practical approach of generating updateable cryptographic keys out of a unique number and a person's biometrics. Although in the description of the system many things are left open, the elementary idea of applying functions to fuse biometrics with random numbers and just storing these function parameters to regenerate the numbers is presented.

3.2 Private Template Scheme

The objective of a so-called “private template" scheme is to provide user authentication by generating a hash out of user's biometric data which is then matched against a stored hash of this user. With the use of several biometric inputs and a majority decoder, a representative feature vector is generated during enrollment. This vector is then concatenated with an error correction code to overcome the variance in biometric measurements. Afterwards out of the resulting vector and personal information of the user a hash is generated and stored. In the authentication process, again, several biometric inputs are captured and majority decoded. Subsequently the error correction code is used to detect errors and finally a hash is computed and matched against the stored one. The whole process is described in Figure 3.2 Davida et al. [20, 21] proposed the so-called \private template" scheme in which the biometric template itself, or a hashed value of it, are used as a cryptographic key which implies that if a person's biometric data is compromised, it becomes useless and must not be used for authentication purpose.

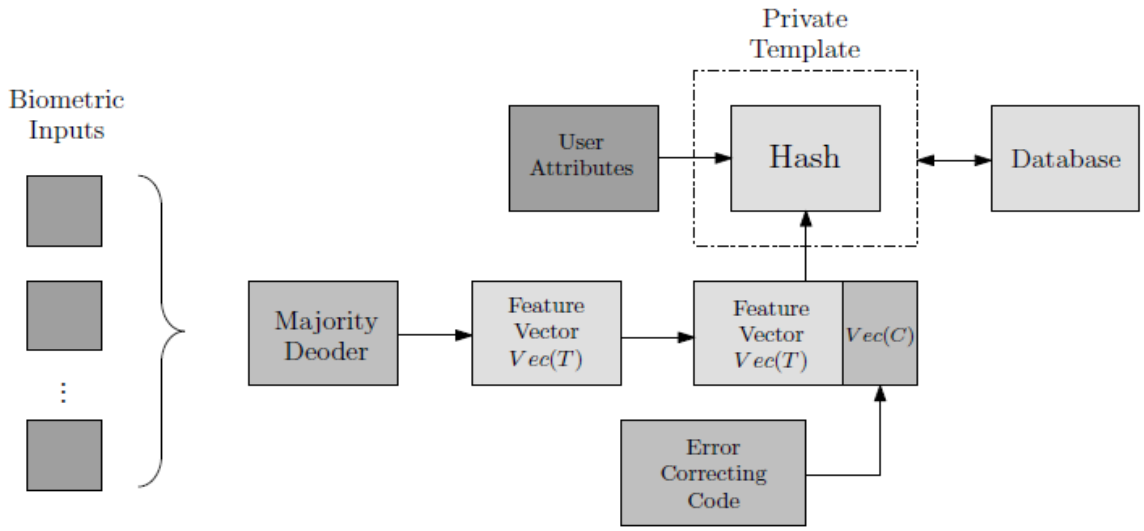


Figure 3.2 The basic operating mode of a Private Temple scheme

3.3 Biometrically Hardened Passwords

In contrast to the above schemes where biometrics are used to create keys or hashes to authenticate legitimate users in a password hardening scheme an existing password is "salted" with biometric data. In the original concept of the password-hardening scheme out of typed password, durations of keystrokes and latencies between keystrokes, are measured. During enrolment out of these measurements, the most distinguishable features are extracted and used to generate an instruction table, which provides information to reconstruct a hardened password. This instruction table is encrypted with the typed password. At the time of authentication, the instruction table is decoded and used to generate the hardened password. Furthermore a history file is stored which is encrypted with the hardened password. This history file includes information about a fixed number of the last successful logins and thus the whole system is capable of adjusting to slight changes of a user's biometrics.

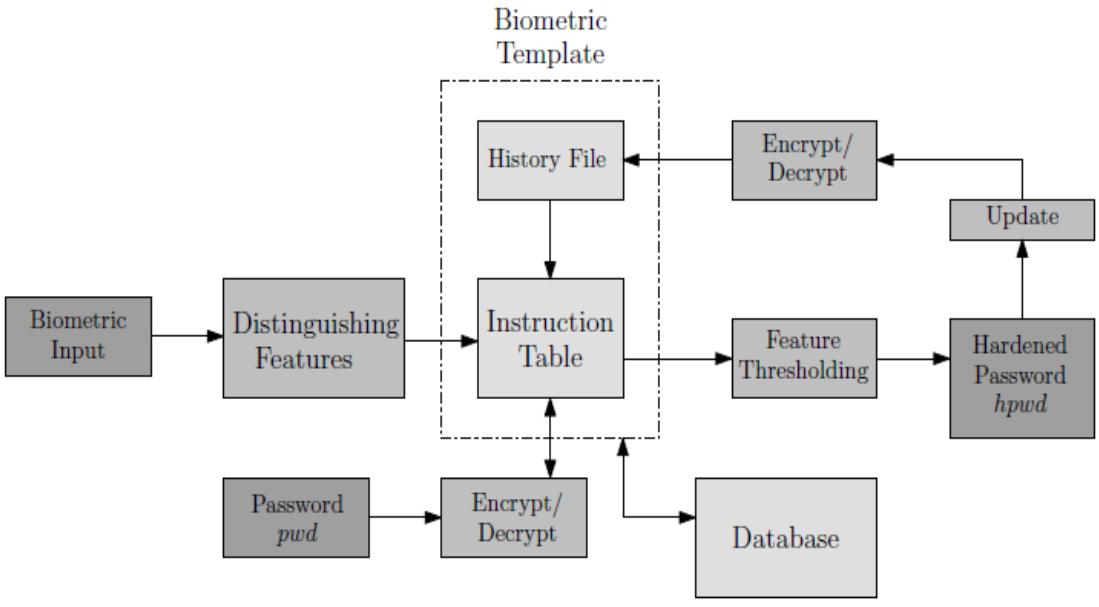


Figure 3.3 basic operating mode of such a system is shown.

3.4 Fuzzy Commitment/Fuzzy Vault Scheme

The objective of a so-called “fuzzy commitment" scheme is to bind biometric features of a user with a key, prepared with an error correction code to overcome the fuzziness of biometric measurements. At the time of enrollment, the extracted features are combined with a codeword of an error correction code. The resulting bit stream is stored in a database together with a hash of the codeword. During the enrollment process, again, biometric features are extracted, combined with the previously stored bit stream and error correction is performed, resulting in another codeword. If the hash of this codeword matched, the stored one authentication succeeds. In Figure 3.4 this process is illustrated Juels and Wattenberg [36] combined well-known techniques from the area of error correcting codes and cryptography to achieve a new type of cryptographic primitive that they refer to as “fuzzy commitment" scheme. Fuzzy commitment is the analog on to “fuzzy logic" in artificial intelligence.

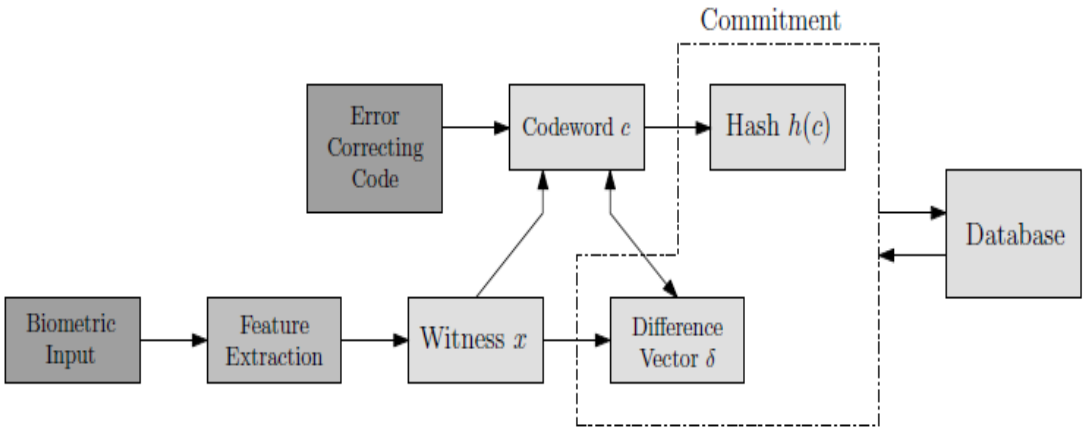


Figure 3.4.The basic operating mode of a Fuzzy Commitment scheme

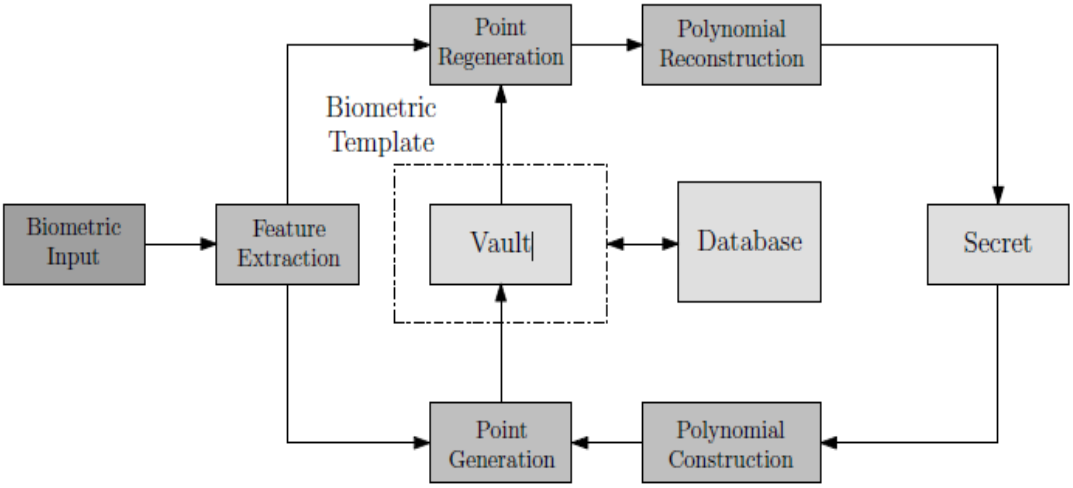


Figure 3.5. The basic operating mode of a Fuzzy Vault scheme

3.4 Cancellable Biometrics

The basic idea of “cancellable biometrics" is to apply transforms to captured biometric data and furthermore perform the matching process in the transformed space. If biometric data is stolen, lost or comprised only the applied transform has to be changed. Furthermore, several different transforms can be used for several applications to prevent imposters from tracking users by cross-matching databases. Figure3.6 illustrates the idea of cancellable biometrics. Ratha et al. [36,27] introduced the concept of “cancellable biometrics".

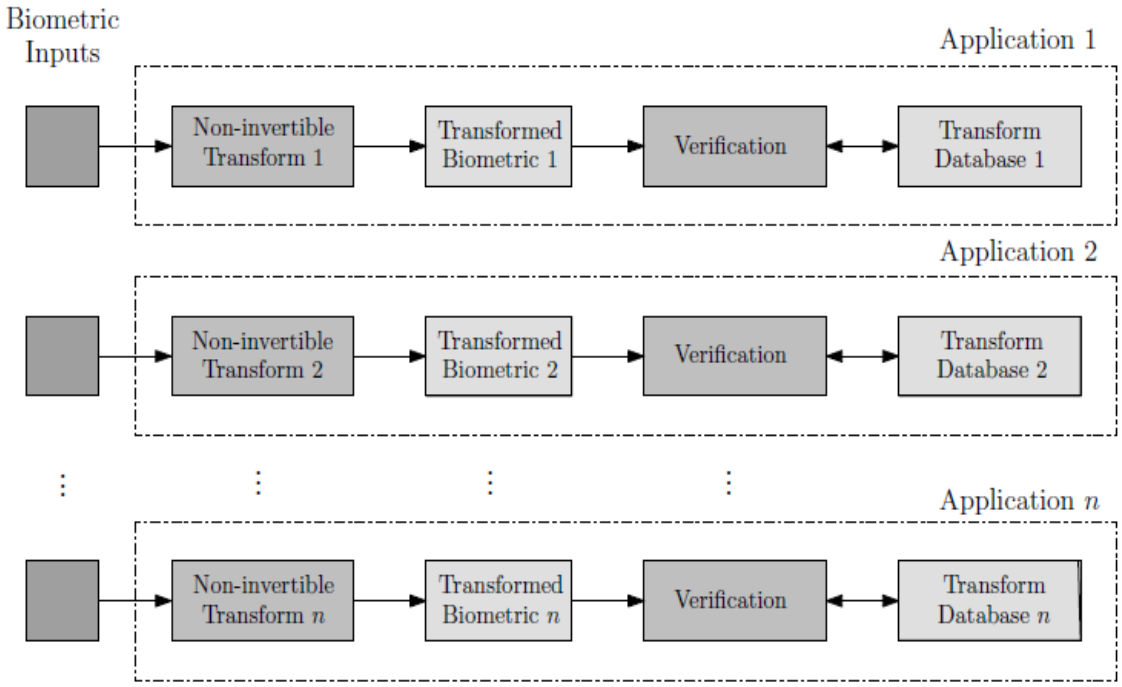


Figure3.6 4 Basis operation of Cancellable Biometrics

Biometric data can be compromised and therefore can become useless because it cannot be modified. The idea of cancellable biometrics consists of intentional, repeatable distortion of a biometric signal based on a chosen transform. These distortion transforms are selected t o be non-invertible, that is the inverse transform is one-to-many. Therefore, the recovering of the original biometric data is not possible if an attacker is in possession of the transform function and the transformed biometric data. Additionally, the correlation of several transformed biometric measurements does not reveal any information about the original biometrics. The distortion of the biometric signal can be performed either in signal domain or in feature domain. Performing distortion in the signal domain means manipulating the raw biometric.

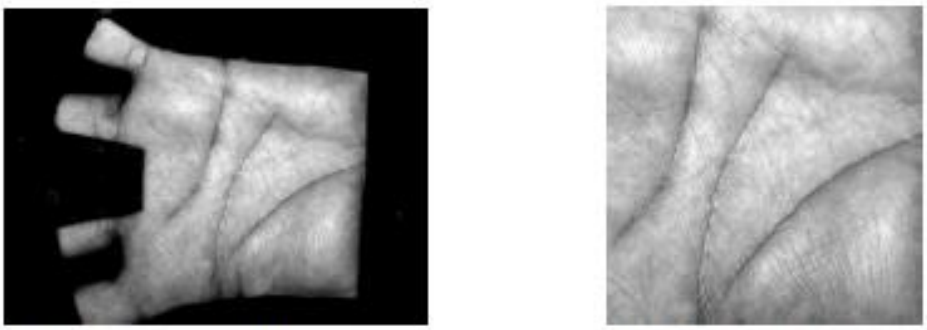
Chapter4

A Proposed Method for Palmprint Based Cryptosystem

In this chapter, we use the preprocessing technique described in [13] to align and normalize the palmprints. After preprocessing, the central part of the image, which is 128×128, is cropped to represent the whole palmprint. Figure. 4.1 .Shows a palmprint and the normalized image. The rest of this thesis is organized as follows. feature extraction and matching ,palmprint cryptosystem. Biometric authentication offers a new mechanism for key security by using a biometric to secure the cryptographic key. Instead of entering a passcode to access the cryptographic key, the use of this key is guarded by biometric authentication. When a user wishes to access a secured key, he or she will be prompted to allow for the capture of a biometric sample. If this verification sample matches the enrollment template, then the key is released and can be used to encrypt or decrypt the desired data. Thus, biometric authentication can replace the use of passcodes to secure a key. This offers both conveniences, as the user no longer has to remember a passcode, and secure identity confirmation, since only the valid user can release the key. Various methods can be deployed to secure a key with a biometric. One method involves remote template matching and key storage [9]. The biometric image is captured and the corresponding template is sent to a secure location for template comparison. If the user is verified, then the key is released from the secure location. This provides a convenient mechanism for the user, as they no longer need to remember a passcode. This method

would work well in a physical access application where the templates and keys may be stored in a secure location physically separated from the image capture device. In this scenario, the communication line must also be secure to avoid eavesdropper attacks.

However, for personal computer use, the keys would likely be stored in the clear on a user's hard drive, which is not secure. A second method involves hiding the cryptographic key within the enrollment template itself via a trusted (secret) bit-replacement algorithm [6]. Upon successful authentication by the user, this trusted algorithm would simply extract the key bits from the appropriate locations and release the



(a) Original Palmprint (b) Cropped Image

Figure 4.1.An example of the palmprint and the normalized image

Key into the system. Unfortunately, this implies that the cryptographic key will be retrieved from the same location in a template each time a different user is authenticated by the system. Thus, if an attacker could determine the bit locations that specify the key, then the attacker could reconstruct the embedded key from any of the other users' templates. If an attacker had access to the enrollment program then he could determine the locations of the key by, for example, enrolling several people in the system using identical keys for each enrollment. The attacker then needs only to locate those bit

locations with common information across the templates. A third method is to use data derived directly from a biometric image.

4.1 Feature Extraction and Matching

4.1.1 DiffCode Extraction

Let I denote a palmprint image and $G\sigma$ denote a 2D Gaussian filter with the variance σ. The palmprint is first filltered by $G\sigma$ as below

$$If = I * G\sigma$$

Where * is the convolution operator. Then the difference of If in the horizontal direction is computed as following:

$$D = If * b$$

$$b = [-1, 1]$$

Where * is the convolution operator. Finally, the palmprint is encoded according to the sign of each pixel of D:

$$C(i,j) = \begin{cases} 1, & \text{if } D(i,j) > 0; \\ 0, & \text{otherwise.} \end{cases}$$

C is called DiffCode of the palmprint I. The size of the preprocessed palmprint is 128×128. An extra experiment shows that the image with 32×32 is enough for the DiffCode extraction and matching. Therefore, before compute the DiffCode, we resize the image from 128×128 to 32×32. Hence, the size of the DiffCode is 32×32. Fig. 2 shows some examples of DiffCode. From this figure, the DiffCode preserves the structure information of the lines on a palm.

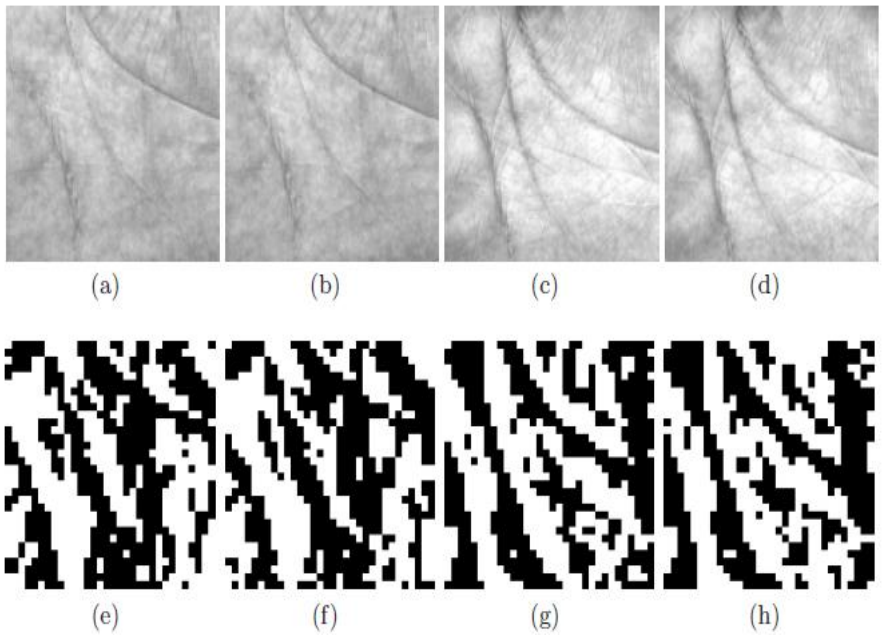


Figure.4.1.some examples of DiffCodes. (a) and (b) are two palmprint samples from a palm; (c) and (d) are two palmprint samples from another palm; (e)(h) are the DiffCodes of (a)-(d), respectively.

4.1.2 Similarity Measurement of DiffCode

Because all DiffCodes have the same length, we can use Hamming distance to define their similarity. Let *C*1, *C*2 be two DiffCodes, their Hamming distance *H* (*C*1, *C*2)) is defined as the number of the places where the corresponding values of *C*1 and *C*2 are different. That is,

$$|H(C_1, C_2) = \sum_{i=1}^{32} \sum_{j=1}^{32} C_1(i,j) \otimes C_2(i,j)$$

Where $\otimes$ is the logical **XOR** operation the matching distance of two DiffCodes *C*1 and *C*2 is defined as the normalized Hamming distance:

$$D(C_1, C_2) = \frac{H(C_1, C_2)}{32 \times 32}$$

Actually, D ($C1$, $C2$) is the percentage of the places where $C1$ and $C2$ have different values. Obviously, D ($C1$, $C2$) is between 0 and 1 and the smaller the matching distance, the greater the similarity between $C1$ and $C2$. The matching score of a perfect match is 0. Because of imperfect preprocessing, there may still be a little translation between the palmprints captured from the same palm at different times. To overcome this problem, we vertically and horizontally translate $C1$ a few points to get the translated C_1^T, and then, at each translated position, compute the matching distance between C_1^T and $C2$. Finally, the final matching distance is taken to be the minimum matching distance of all the translated positions.

4.2 Palmprint Cryptosystem

In general, the palmprints captured from the same hand at different time are not exactly same. However, they are similar enough to distinguish that they are from the same hand. That is, when the matching distance between the DiffCodes $C1$ and $C2$ is less than a threshold T , they should be regarded as being computed from the same hand, and $C2$ should be able to decrypt the information which is encrypted using $C1$. However, in general symmetric cryptosystems (eg.AES), it is impossible to successfully finish the decryption if the encrypting key and the decrypting key are not exactly same. To overcome this problem, we must transform $C2$ to $C1$ before using it for decryption. Since both $C1$ and $C2$ are binary strings with the same length, we can use the error-correct-coding theory to encode $C1$ and get its error-correcting code, which can correct- less than $T \times 1024$ errors, and then use this error-correcting code to correct $C2$. If the matching distance between $C1$ and $C2$ is less than T , which means that $C1$ and $C2$ are from the

same hand, *C*2 can be exactly transformed to *C*1 using the error-correcting code. Then the corrected *C*2 can be used for decryption. The principle of the palmprint cryptosystem is shown in Figure.4 3. In the encrypting phase, the 32×32 = 1024 bits DiffCode is extracted from the palmprints. Then the DiffCode is encoded to a fix length palmprint key (HC) using a Hash function (eg. MD5), and at the same time, an error-correct-code (ECC) of the DiffCode is generated using an existed algorithm (e.g. BCH).Some general encryption algorithms (e.g. AES) use this palmprint key to encrypt the secret information *S*. In decrypting phase, the 1024 bits DiffCode extracted from the input palmprint is first corrected using the ECC. Then the corrected string is encoded to a palmprint key (HC) using the same Hash function. Finally, the corresponding general decryption algorithms use this key to decrypt the information (S).To overcome the translation problem, we can get the 144 × 144 central part of the palmprint in the preprocessing of decryption phase, and then resize it to 36 × 36 to compute DiffCode. That is, in decryption phase, we get a DiffCode.

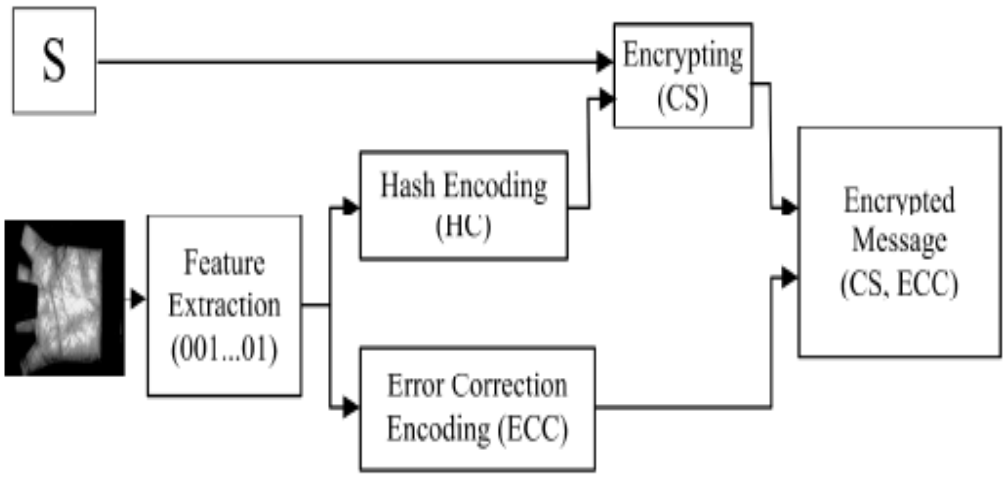


Figure 4.2(a)Encryption Phase

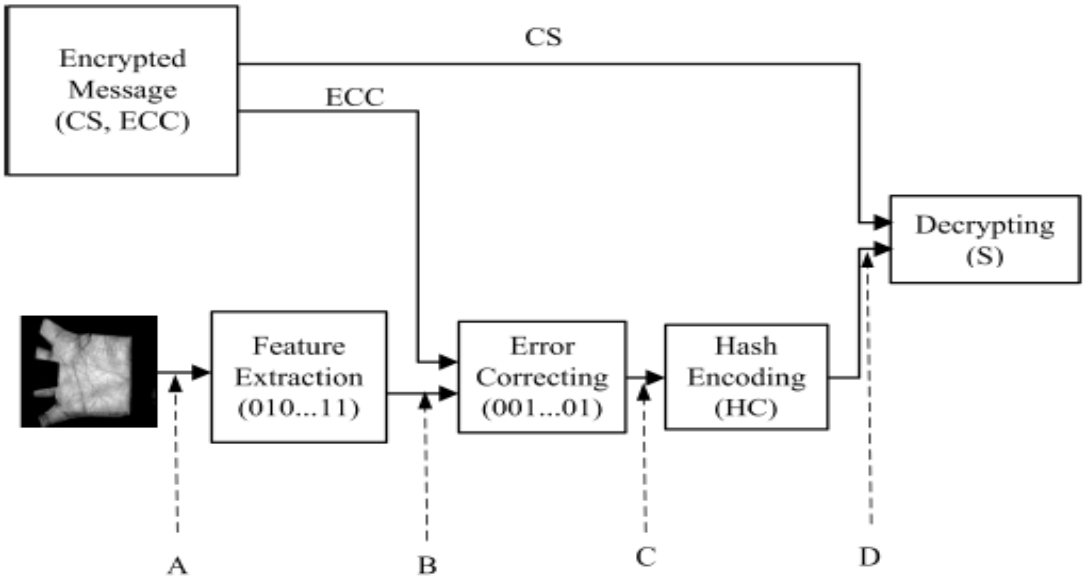


Figure 4.3 (b) Decryption phases

With 36×36 size. From this larger DiffCode, we can get 25 DiffCodes with 32×32, which are used one by one for decryption until success. This process is equivalent to the translation the DiffCode vertically and horizontally from −2 to +2 points.

Chapter 5

Experimental Results and Analysis

These palmprints were used is taken from PolyU PalmprintDatabase [15] to test our system, people of different ages and both sexes and were captured twice, at an interval of around twomonths, each time taking about 10 images from each palm. Therefore, This database contains about 20 images of each palm. The size of the images in the database is 384 × 284. In our experiments, all images were preprocessed using the preprocessing technique described in [13] and the central 128×128 part of the image was cropped to represent the whole palmprint. In the system, the Hash, error-correcting and encrypting algorithms are respectively selected as MD5, BCH and AES. For a (*n, k, t*) BCH code, *n*, *k* and *t* respectively mean the length of the code, the length of the information and the number of the errors which can be corrected by this code. For our system, *t* can be computed using its distance threshold *T* as following.

$$t = 1024 \times T$$

and *k* should satisfy the following conditions

$$k \geq 1024$$

If $k > 1024$, we can append $(k - 1024)$ zeros to the 1024 bits DiffCode to get the message with length *k* and then encode it using BCH encoding. Therefore, to error-correcting encoding, to investigate the relationship between the threshold and accuracy, each sample in the database is matched against the other palmprints in the same database.

The matching between palmprints, which were captured from the same palm, is defined as a genuine matching. Otherwise, the matching is defined as an impostor matching. A total of 30, 042, 876 (7, 752 × 7, 751/2) matching have been performed, in which 74, 086 matching are genuine matching's. The FAR and FRR at different thresholds are plotted in Fig. 4. Some typical FARs, FRRs, the corresponding thresholds, and the numbers of the error bits are listed in Table 1. We can select a threshold according to the requirement of the applications. In our experiments, we choose the distance threshold as 0.2949. According to Table 1, the corresponding FAR, FRR and the number of errors, which should be corrected, are 0.0012%, 3.0169%, and 302. According to the theory of BCH error-correcting-code, (4095, 1412, 302) BCH code can be used in our system. Now we analyze the attacks to this system.If the attack happens at Point A (See Fig. 3), that is, the attacker uses some palmprints to attack the system. In this case, the possibility to successfully decrypt the message is about 0.0012% ≈ 10^{-5}, which means that to decrypt the message, a cracker has to find about 10^5 different palmprints to try, which is very difficult to get so many palmprints in a short time. If the attack happens at Point B (See Fig. 3), that is, the cracker attacks the system by directly generating the DiffCode for the error-correcting. The possibility to successfully decrypt the message in this way is *p*:

$$p = \frac{C_{1024}^{302} + C_{1024}^{301} + \cdots + C_{1024}^{1} + C_{1024}^{0}}{2^{1024}} \approx 2^{-134}$$

If the attack happens at Point C (See Fig. 3), that is, the cracker generates the corrected DiffCode to attack the system, the possibility to success is 2^{-1024}. If the attack happens at

Point D (See Fig. 3), that is, the cracker generates the hashed code to attack the system, the possibility to success is 2^{-128}.

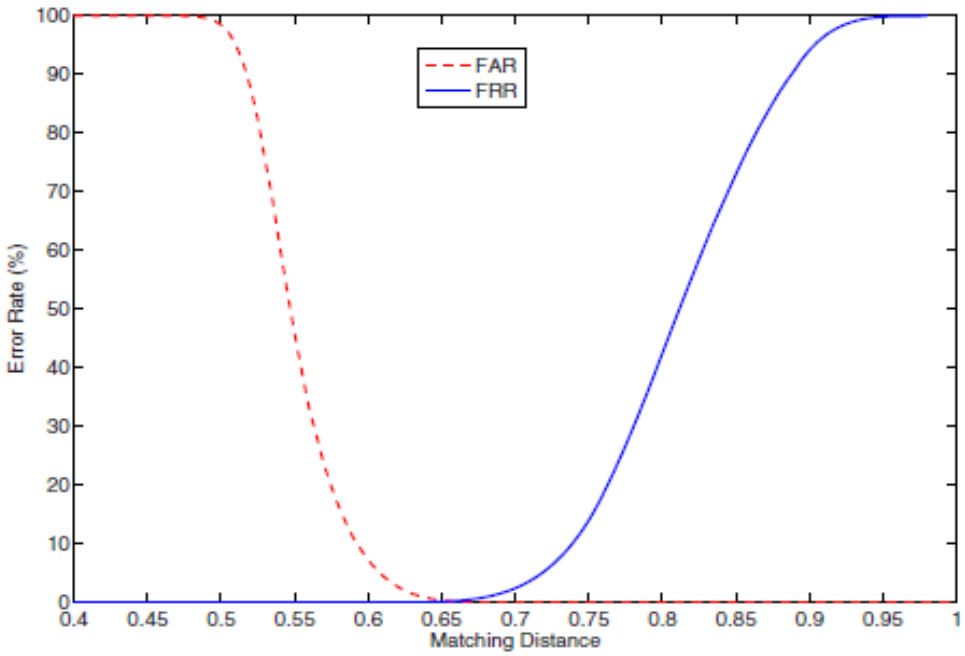


Figure 5.1 The FAR and FRR at Different Threshold

Threshold	Number of Error Bits	FAR (%)	FRR (%)
0.3799	389	2.6862	0.0240
0.3750	384	2.0133	0.0283
0.3701	379	1.4784	0.0382
0.3652	374	1.0976	0.0523
0.3604	369	0.7799	0.0764
0.3555	364	0.5458	0.1018
0.3496	358	0.3786	0.1386
0.3447	353	0.2558	0.2150
0.3398	348	0.1663	0.2899
0.3350	343	0.1092	0.3791
0.3301	338	0.0663	0.4964
0.3252	333	0.0399	0.6973
0.3203	328	0.0238	0.9038
0.3154	323	0.0135	1.2277
0.3096	317	0.0075	1.5445
0.3047	312	0.0042	1.9533
0.2998	307	0.0022	2.4370
0.2949	302	0.0012	3.0169
0.2900	297	0.0006	3.6788
0.2852	292	0.0003	4.4751

Typical FAR, FRR, corresponding thresholds, and number of error bits

Chapter 6

Conclusions and future work

6.1Conclusion

Biometric Cryptosystem technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.This work has explored the possibilities and privacy-enhancing benefits of Biometric Cryptosystem technologies for meeting the needs of businesses and government agencies. We believe that BC technology exemplifies fundamental privacy and data protection principles that are endorse around the world, such as data minimization, user empowerment, and security, better than any other biometric technology solution in existence.Discussions regarding the most appropriate methods to achieve, in a privacy-enhanced manner, strong identification and authentication protocols. While introducing biometrics into information systems may result in considerable benefits, it can also introduce many new security and privacy vulnerabilities, risks, and concerns, as discussed above. However, novel Biometric Cryptosystem techniques have been developed that can overcome many, if not most, of those risks and vulnerabilities, resulting in a win-win, positivesum scenario. A positivesum model, in the form of Biometric Cryptosystem, presents distinct advantages to both security and privacy. 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.

In this work proposed a palmprint cryptosystem. This system extracted binary DiffCode feature from palmprint and used the error-correcting theory to remove the difference between the DiffCodes from the same palms. The system can effectively encrypt and decrypt messages and it is almost impossible to crack it.

6.2Future Work

This thesis addressed some limitations regarding bio crypt technology; there still remaina number of unresolved issues. Therefore, the following solutions could be furtherexplored 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.

- 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.]. Uludag, U., Pankant, S., Prabhakar, S., Jain, A.K.: Biometric cryptosystems: issues and challenges. Proceedings of the IEEE 92, 948–960 (2004)

[2.] Freire-Santos, M., Fierrez-Aguilar, J., Ortega-Garcia, : Cryptographic key generation using handwritten signature. In: Proc. of SPIE, Biometric Technologies for Human Identificatin III (2006)

[3.]Uludag, U., Pankant, S., Jain, A.K.: Fuzzy vault for fingerprints. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 310–319. Springer, Heidelberg (2005)

[4.] Monrose, F., Reiter, M.K., Li, Q.,Wetzel, S.: Using voice to generate cryptographic keys. In:ASpeakerOdyssey,TheSpeakerRecognitionWorkshop, pp. 202–213 (2001)

[5.] Juels, A., Sudan, M.: A fuzzy vault scheme. In: Proc. IEEE International Symposium on Information Theory, IEEE Computer Society Press, Los Alamitos (2002)

[6.] Soutar, C., Roberge, D., Stojanov, S.A., Gilroy, R., Kumar, B.V.K.V.: Biometric encryption. ICSA Guide to Cryptography (1999)

[7.] Monrose, F., Reiter, M.K., Li, Q., Lopresti, D.P., Shih, C.: Towards speechgenerated cryptographic keys on resource constrained devices. In: Proc. 11th USENIX Security Symposium, pp. 283–296 (2002)

[8.] Zhang, D.: Palmprint Authentication. Kluwer Academic Publishers, Dordrecht (2004)

[9.] Wu, X., Zhang, D., Wang, K.: Palmprint Recognition. Scientific Publishers, China (2006)

[10.] Wu, X., Wang, K., Zhang, D.: Fisherpalms based palmprint recognition. Patter Recognition Letters 24, 2829–2838 (2003)

[11] Duta, N., Jain, A., Mardia, K.: Matching of palmprint. Pattern Recognition Letters 23, 477–485 (2001)

[12.] Han, C., Chen, H., Lin, C., Fan, K.: Personal authentication using palm-print features. Pattern Recognition 36, 371–381 (2003)

[13.] Zhang, D., Kong, W., You, J., Wong, M.: Online palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence 25, 1041–1050 (2003)

[14.] Jain, A., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology 14, 4–20 (2004)

[15.] PolyU Palmprint Palmprint Database
(http://www.comp.polyu.edu.hk/biometrics/)

[16] The Center of Biometrics and Security Research, CASIA Iris Image Database, http://www.sinobiometrics.com.

[17] A. Adler, \Vulnerabilities in Biometric Encryption Systems," Audio- and video-based Biometric Person Authentication (AVBPA), pp. 1100{1109, 2005.

[18] S. Agaian, Hadamard Matrix and Their Applications, ser. Lect. notes in math. Springer Verlag, 1985, vol. 1168.

[19] L. Ballard, S. Kamara, F. Monrose, and M. Reiter, \On the requirements of biometric key generators," Technical Report TR-JHU-SPAR-BKMR-090707, 2007, submitted and available as JHU Department of Computer Science Technical Report.

[20] E. Berlekamp, “Factoring Polynomials Over Finite Fields," Bell Systems Technical Journal, vol. 46, pp. 1853{1859, 1967.

[21] A. Bodo, \Method for producing a digital signature with aid of a biometric feature," 1994, german patent DE 42 43 908 A1.

[22] K. Bowyer, K. Hollingsworth, and P. Flynn, \Image understanding for iris biometrics: a survey," Computer Vision and Image Understanding, no. 110, pp. 281{307, 2008.

[23] X. Boyen, \Reusable cryptographic fuzzy extractors," CCS 2004 Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 82{91, 2004.

[24] A. Burnett, F. Byrne, T. Dowling, and A. Du_y, \A Biometric Identity Based SignaturemScheme," Applied Cryptography and Network Security Conference, New York, 2005.

[25] J. P. Campbell, “Speaker Recognition: A Tutorial," Proceedings of the IEEE, vol. 85, no. 9, pp. 1437{1462, 1997.

[26] R. Canetti, “Towards realizing random oracles: hash function which hide all partial information," Advances in Cryptology. proc. of Crypto'97 (LNCS: 1294), pp. 455,469,

[27] A. Cavoukian, A. Stoianov, and F. Carter, \Biometric Encryption: Technology for Strong Authentication, Security and Privacy," IFIP International Federation for In-formation Processing, vol. 261/2008, pp. 57{77, 2008.

28] Y.-J. Chang, W. Zhang, and T. Chen, \Biometrics-based cryptographic key generation," Proceedings of 2004 IEEE International Conference on Multimedia and Expo (ICME-2004), vol. 3, pp. 2203{2206, 2004.

[29] R. Chellappa, C. Wilson, and S. Sirohey, \Human and Machine Recognition of Faces: A Survey." Proceedings of the IEEE, vol. 83, no. 5, pp. 705{740, 1995.

[30] B. C. Chen and V. Chandran, \Biometric based cryptographic key generation from faces," In Proceedings Digital Image Computing: Techniques and Applications (DICTA),

[31] T. C. Clancy, N. Kiyavash, and D. J. Lin, \Secure smartcard-based _ngerprint authentication," Proc. ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45{52, 2003.

[32] T. Connie, A. Teoh, M. Goh, and D. Ngo, \Palmhashing: a novel approach for cancelable biometrics," Inf. Process. Lett., vol. 93, no. 1, pp. 1{5, 2005.

[33] J. Daugman, \The importance of being random: Statistical principles of iris recognition,"Pattern Recognition, vol. 36, no. 2, pp. 279{291, 2003.}

[34] ||, “How Iris Recognition Works," IEEE Trans. CSVT, vol. 14, no. 1, pp. 21{30, 2004.

[35] G. Davida, Y. Frankel, and B. Matt, \On enabling secure applications through off-line biometric identification," Proc. of IEEE, Symp. on Security and Privacy, pp. 148{157,1998.}

[36] “On the relation of error correction and cryptography to an off- line biometric based identication scheme," Proc. of WCC99, Workshop on Coding and Cryptography, pp. 129{138, 1999.

[37] D. L. Delivasilis and S. K. Katsikas, \Side channel analysis on biometric-based key generation algorithms on resource constrained devices," International Journal of Network Security, vol. 3, no. 1, pp. 44{50, 2005.

[38] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, \Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Proc. Eurocrypt 2004 (LNCS: 3027), pp. 523{540, 2004.}

[39] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. Yedidia, \Secure storage of fingerprint biometrics using slepian-wolf codes," in Inform. Theory and Apps. Work. (UCSD), 2007.

[40] S. Y. E. Martinian and J. S. Yedidia, \Secure biometrics via syndromes," in 43rd Annual Allerton Conference on Communications, Control, and Computing, Monticello, IL, USA, 2005.

[41] H. Feng and C. C. Wah, \Private key generation from on-line handwritten signatures," Information Management and Computer Security, vol. 10, no. 18, pp. 159{164, 2002.

[42] M. R. Freire, J. Fierrez, J. Galbally, and J. Ortega-Garcia, “Biometric Hashing Based on Genetic Selection and Its Application to On-Line Signatures," International Conference on Biometrics '07 (LNCS: 4642), pp. 1134{1143, 2007.

[43] A. Goh and D. C. L. Ngo, “Computation of cryptographic keys from face biometrics," in Communications and Multimedia Security (LNCS: 2828), 2003, pp. 1{13.

[44] A. Goh, A. B. J. Teoh, and D. C. L. Ngo, “Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 1892{1901, 2006.

[45] A. Graps,”An introduction to wavelets," IEEE Computational Science and Engineering, vol. 2, no. 2, 1995.

[46] F. Hao, R. Anderson, and J. Daugman, “Combining Cryptography with Biometrics

Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081{1088, 2006.

[47] F. Hoa and C. W. Chan, “Private key generation from on-line handwritten signatures," Information Management and Computer Security, vol. 10, no. 2, pp. 159{164, 2002.}

[48] G. S. I. Reed, “Polynomial codes over certain finite fields," Journal of the Society for Industrial and Applied Mathematics, vol. 8, pp. 300{304, 1960.}

[49] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti, \Filterbank-based Fingerprint matching,"In Proc. of IEEE Transactions on Image Processing, vol. 9, no. 5, pp. 846{859, 2000.

[50] A. Juels and M. Sudan, “A fuzzy vault scheme," Proc. 2002 IEEE International Symp. on Information Theory, p. 408, 2002.

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

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