Security Analysis of Biometric Cryptosystems: Case Study of Fuzzy Vault Approach

Maryam Lafkih[1] , Mounia Mikram[1, 2], Sanaa Ghouzali[1, 3], Mohamed El Haziti[1, 4], Driss Aboutajdine[1]
[1] LRIT, Faculty of Sciences
Mohammed V University, Rabat, Morocco
[2] The School of Information Sciences
Rabat, Morocco
[3] College of Computer and Information Sciences,
King Saud University, Riyadh, Saudi Arabia
[4] Higher School of Technology
Sale, Morocco
maryam.lafkih@gmail.com

ABSTRACT: *Use of biometric systems is becoming an important alternative to replace traditional authentication such as password. Yet most of biometric authentication systems store original biometric features, unfortunately, without any encryption, threatening though the security and privacy of user's identity. When biometric data is compromised, unlike a password, it cannot be changed. Therefore, the security of biometric models is essential in designing an authentication system. To achieve this protection of biometric models, two approaches are used: methods based on transformation of user characteristics and biometric cryptosystems. Although biometric cryptosystems are used in several applications (e.g. smart cards), they include several components that have limitations such as risk of falsification and poor performance. A performance evaluation is then compulsory for comparison between different biometric systems. For this reason we proposed in this paper several criteria to assess the security strength and we defined several measures that facilitate overall security evaluation of biometric cryptosystems.*

In this analysis we considered Fuzzy Vault scheme, a well known approach of biometric cryptosystems, in order to provide security and protection risks associated with this approach. We proposed in this work four distinct classes of attacks against Fuzzy Vault technique, including Intrusion attacks, Correlation attacks, Combination attacks and Injection attacks. Our experimental results indicate that the Fuzzy Vault technique is vulnerable to some proposed attacks because of the easiness to obtain the user model using the elements known to the attacker. This vulnerability is increased especially in the intrusion attacks and correlation attacks where attacker can match multiple helper data generated from the same biometric traits. The proposed attacks can reach a 100% success to access the system, making the Fuzzy Vault based protection approach easily compromised.

Keywords: Biometric Cryptosystems, Fuzzy Vault, Security Analysis, Performance Evaluation

Received: 19 August 2012, Revised 8 October 2012, Accepted 19 October 2012

1. Introduction

With the increasing need to ensure security in several large applications, biometric is presented as an alternative solution that replaces traditional authentication techniques such as the password and other identifiers. It presents simplicity to the user and can also control access to applications. However, biometric systems are vulnerable to several attacks and especially a user template stored in the database can be used by an attacker to view confidential information or to gain access illegitimately to the system [26]. To address these vulnerabilities of biometric systems, two methods of biometric template protection are proposed in the literature. Methods based on the *Transformation of user Characteristics and Biometric Cryptosystems* [22].

The first type of approaches consist of applying a transform function on biometric characteristics to build a model that will be stored in the database (enrollment phase). During authentication, the same function is applied to the bio-metric characteristics of the request. The result model is then compared with stored reference model to allow or deny the access [22]. Biometric cryptosystems use a secret key to wrap the biometric characteristics and generate *Helper data* that will be stored in the database (enrollment phase). The helper data does not reveal significant information about the biometric data or the secret key. During authentication phase the secret key must be generated from the characteristics of biometric query and the stored helper data [23]. Error correcting codes are employed in biometric cryptosystems in order to regenerate the secret key given the biometric query. This message recovery mechanism can be used to allow reconstruction of original message and then to address the problem of intra-class variation.

Although systems using biometric cryptosystem provide high level of security, these systems have on the other hand several gaps and limitations namely the high cost, the possibility of falsification and the low performance [23]. To allow the comparison between different biometric systems that rely on these methods, it is necessary to evaluate their performance and analyze their security. Thus the objective of this work is to propose a set of criteria to evaluate the security of biometric cryptosystems. Hence we have proposed different measures to assess the security strength of *Fuzzy Vault* biometric cryptosystems that considered as a well known and secure approach of biometric cryptosystems. We applied these measurements for the protection of a biometric facial recognition system showing the interest of the proposed criteria. We proposed in this work several attacks against *Fuzzy Vault* technique, that we introduce into four distinct classes of attacks including, *Intrusion attacks, Correlation attacks,Combination attacks* and *Injection attacks*. Our analysis shows that this method is easily compromised by all proposed attacks and then systems based on this approach are not suitable for providing security.

The rest of this paper is organized as follows, biometric systems are described in Section 2, followed by the secu-rity in biometric cryptosystems in section 3. In section 4 Security Analysis in Fuzzy Vault biometric cryptosystems is detailed and the experimental results are illustrated in section 5. Section 6 provides discussion and finally conclusion and perspectives are drawn in Section 7.

2. Biometric Systems

2.1 Biometric systems Principe

Applications like Internet and financial systems have increased need to ensure the security/privacy of the user's identity when using authentication technologies. To this end, biometrics have several advantages compared to classical authentication techniques. Biometric systems are easy to use, reliable and allow more security for applications. They are based on two steps (Figure 1) [22]:

• **Enrollment step:** In this phase biometric characteristics are extracted from the user and stored in the database.

•**Authentication step:** In this phase biometric characteristics of the person who is present to the system are extracted and then compared with the enrollment characteristics stored in the database.

A number of biometric systems are used for different applications and the choice of biometric trait depends primarily on the application. A brief description of some biometric technologies illustrated in literature is given below.

2.2 Biometric techniques

Many different technologies can be used for biometric authentication that differ from one to another in terms of their architecture, modalities and methods used for integration of information (Figure 2).

• **Fingerprints:** Fingerprints are formed by the minutiae which represented by ridges and furrows present on the surface of

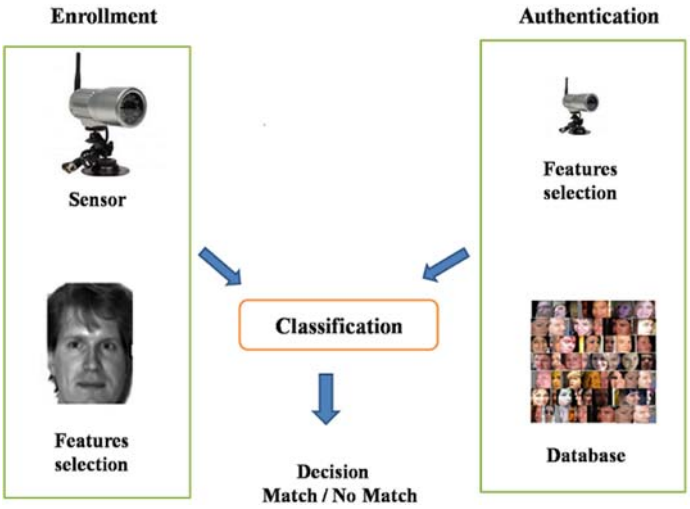

Figure 1. Steps of biometric authentication

finger [18]. We can capture them by traditional technology such as printing finger on a sheet via a layer of ink or the latest technology including: optical (camera takes an image of the finger that is placed on a sensor), capacitive (electric field analysis of the finger by a microprocessor), or ultrasound (the transmission of acoustic waves).

• **Iris Recognition:** Iris is the colored area visible between the white of the eye and the pupil, it the most accurate modality in the identification and authentication. It is used just in critical areas such as nuclear bases because of it's high cost [3]. In this system a camera detects the image of iris and after features are extracted and compared to those that recorded.

• **The retina:** The retina has vessels that are unique for each person. This method requires placing the eye with a short distance from the sensor [4] and uses a light beam which extracts feature points of the retina, despite these performances this method has a problem of health risk, for this reason it's less used comparing to other modalities.

• **Face Recognition:** In this modality several facial features are extracted (for example cheeks, eyes, nose, and mouth) from a photo or video [17]. This modality is very used because it's easy and can be practiced in public places like airports etc...

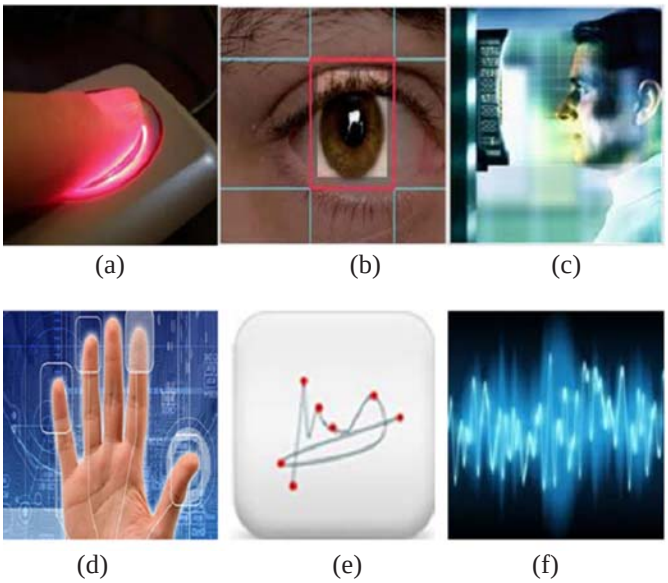

Figure 2. Examples of biometric techniques: (a) fingerprint, (b) iris,(c) face,(d) hand geometry, (e) signature, (f) voice.

Biometric recognition has a number of advantages against classical authentication mechanisms based on passwords or smart cards. Despite these advantages, biometric systems are targeted by several type of attacks.

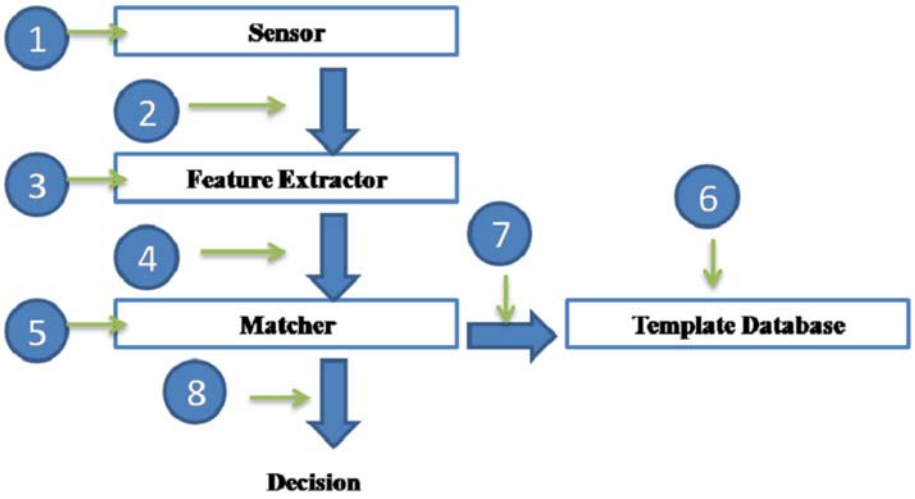

Figure 3. Different levels of attacks

2.3 Attacks on biometric systems

Ratha et al.[26] have identified eight points or levels of attack in a biometric system (Figure 3). The first type of attack named (*Sensor Attack*) consists of presenting a falsified data to the system (as a silicon finger, face mask, etc ...). Using information from a database stolen by the attacker which allows illegitimate access to the system, this attack can be made in several ways such as illustrated by Putte, Keuning [33]. In the case of fingerprints, authors did the falsifica-tion of digital fingerprint with cooperation (with liquid silicon) or without cooperation of the user (creation of dummy finger by casting the finger which filled with silicon). In the first case the falsification is more efficient compared to the case of non-cooperation. Matsumoto et al. [20] have tested fingerprint falsified with the help of real users in 11 biometric systems, their results show that this attack can be performed with a probability of 67%. A falsification data attack is very used because it requires only false biometric traits, for systems that are less secured, attacker can soak the system in the first test, for systems that are more secured access may be after several attempts.

For the second type of attack (*between the sensor and features extractor*) a replay of biometric data is made and sent with an illegally way to the extractor of features. The attacker can have access to the system by sending the falsified data to the features extractor instead of real data. To distinguish between real data and falsified data, a signature must be done before sending data to the features extractor [22].

In third attack (*Features extractor Attack*), the features extractor is replaced by a program chosen by the attacker de-pending on the desired functionality. This program can be a Trojan horse that makes the functionality by its designer to change the internal processing of the extractor. It is necessary that the features extraction module must ensure the not spoofing internal data and also ensure the more security of the entry data.

In fourth attack, the attacker can replace other characteristics by synthetic data (*By pass matcher Attack*) on the channel. The attackers stole biometric characteristics of the real user and submit them to the matcher. This attack has a similar treatment to the second attack, an attacker can give characteristics generated depending on the purpose desired as input to the correspondence. In this context the more known attack system is developed by Soutar who proposed a hill-climbing attack [19] in a facial recognition system using the correlation based on a filter. To have an illegitimate access to the system he changed the input image for obtaining the desired score. This attack can disrupt the system by sending random models, it has the principle of linking the match score in the output. This attack can be considered as type 2 or 4. Adler [1] proposed a synthetic image of face to attack a face recognition system. As a first step, an image was randomly selected, it will be changed using the scores returned by the comparator. The procedure is completed if there is no improvement in score.

In the fifth attack, the attacker can also change the comparator depending on the desired goal (*Attack on comparator*). A system

should normally accept clients and refuse others even if they have close characteristics to real users. Although it's possible to forge signature data, it's possible also to do the same signature for closer data which make another problem. In this attack the attacker used a Trojan horse to change the score of correspondence and then have high score which indicate acceptance or low score for rejecting the real user [32].

The sixth type of attack (*Database Attack*) that can be at the database is where an attacker can make a modification (addition, or deletion) of models registered in the database. If an attacker has stolen a biometric database, he can use it to find the original model of a user [9]. In this type of attack an attacker can have access to user data stored in the database and modify it which allows easy access to the system. In this context we can also mention the possibility of linking data from the same user in multiple databases for illegitimate access in several systems [9].

The seventh attack (Bypass comparator Attack) is made at the transmission medium before the comparison of the model stored in the database and the authentication model. Here an attacker can submit test data generated by these specific characteristics instead of data to be sent from the database. For this purpose it is necessary to ensure that the data comes from the database but not a falsified data submitted by the attacker. For this end, a data must be signed before being sent to the comparator [28] . We consider in this type of attack, another threat where a user can steal the data of another user. The sixth and seventh attacks are the most serious because spoofed data from the database can not only access to the system but also to have information on the identity and privacy of the user [9].

The latest attack may be at the comparison score where an attacker can replace the results (accept / reject). In the case of a beuge at the biometric system application, an attacker can exploit this beuge by modifying the control program for a decision to accept not legitimate or also refused customers.

Although a system can be stolen sing one of these attacks, illegitimate access to the biometric template is the at-tack that can be of a potential damage of the system, since the leak of user information is considered as serious threat security and also for privacy [18]. Despite the solutions proposed to address the mentioned attacks, no method for tem-plate protection is perfect and the choice of protection methods is based on application requirements and influenced by the selection of biometric trait, representation and variation of characteristics.

2.4 Protection of biometric systems

To address the problem of attacks against biometric templates, it is necessary to protect the models stored in the database to prevent any illegitimate access of the impostor. An ideal algorithm for the protection of templates should meet the following three properties:

• **Revocability:** It must be easy to revoke a compromised model and reissue a new identifier based on the same biometric data.

• **Security:** It should be difficult to obtain the original biometric features from secure template. This property prevents an impostor to create an identifier from the stolen model.

• **Performance:** The protection of a model should not degrade the performance of biometric system [10].

In the literature there are two types of methods to protect biometric templates: Methods based on *Feature Transformation* and *Biometric Cryptosystems* [22] (Figure 4).

Feature Transformation method is based on applying a transform function on the biometric characteristics. Instead of the biometric characteristics, the transformed characteristics will be stored in the database as a reference model (Figure 4). The same transformation is applied to the query during authentication and then matched with the stored template [22]. The transformation can be invertible or not:

• **Invertible:** Possibility of recovering the original biometric template from the transformed template.

• **Non-Invertible:** In this type of transformation, it is hard to regenerate the original template from the transformed template.

Biometric cryptosystems are developed in order to produce or retrieve a key from biometric features (Figure 4) without revealing information about the used biometric traits or the used key. Usually, error correction codes [25] are used in these systems to retrieve the enrolled biometric identifiers or key from the biometric characteristics of the application.

Features transformation and *biometric cryptosystems* have their advantages and limitations. For the first method a biometric template is revocable, we can change the model if it is compromised by changing the key, also in this method there is the ability to manage the intra-class variation in the transform domain which gives a lower error rate systems. The problem of the transformation method is its difficulty in measuring the security. Biometric cryptosystems are based on the correction error code that evaluates the security. Hence the performance of biometric cryptosystems is limited by the capacity of error correction code.

3. Biometric Cryptosystems

Security has become increasingly a concern in biometric systems, it ensure confidentiality by providing a robust authentication process against any type of deception and also against the possibility of raising the original biometric characteristics [27]. For this purpose biometric cryptosystems are proposed as cryptography based technology to minimize the vulnerabilities exploited illegitimately to gain access to a system [26]. Several biometric cryptosystems are developed and demonstrated a high security, this security is variable depending on the used technologies and also the variation of biometric characteristics.

Biometric Cryptosystems are considered as techniques that incorporate the benefits of using biometric characteristics and secret key to encrypt the biometric data of the user [7] [16]. The error correction codes are used in such systems to retrieve the key from biometric characteristics at the authentication stage. There are several approaches developed in the field of biometric cryptosystems. These approaches are based on two modes to generate the secret key, *Key binding* and *Key generation* [32]. For *Key binding* binding cryptosystem, biometric template is linked with a secret key in a single entity to build an helper data. This data reveal no information on the key or biometric template. It is therefore difficult to decode the key or the model without any prior knowledge of biometric data of the user. The key is recovered after a successful authentication. This mode is tolerant to variations of biometric data and this tolerance is determined by the ability of associated error correction code word. Using *Key generation*, the key is derived from the biometric data. Authentication is successful if the key is retrieved. During the authentication phase, the biometric data cannot be reproduced exactly. For this purpose a data-derived model called Secure sketch is also stored in the database. This allows recovering the model if the current model and that recorded in the database are close [16]. *Fuzzy Commitment* method, proposed by Juels and Wattenberg [12], is one of the main approaches for biometric cryptosystems. This method, is based on the use of a secret key with the biometric characteristics of the user to construct the helper data that will be stored with the encrypted key in the database instead of the user biometric template. During authentication. The key must be recovered using the auxiliary data and characteristics of the request. This approach requires that the data must have a canonical format which is not the case for some biometric traits (e .g fingerprint).

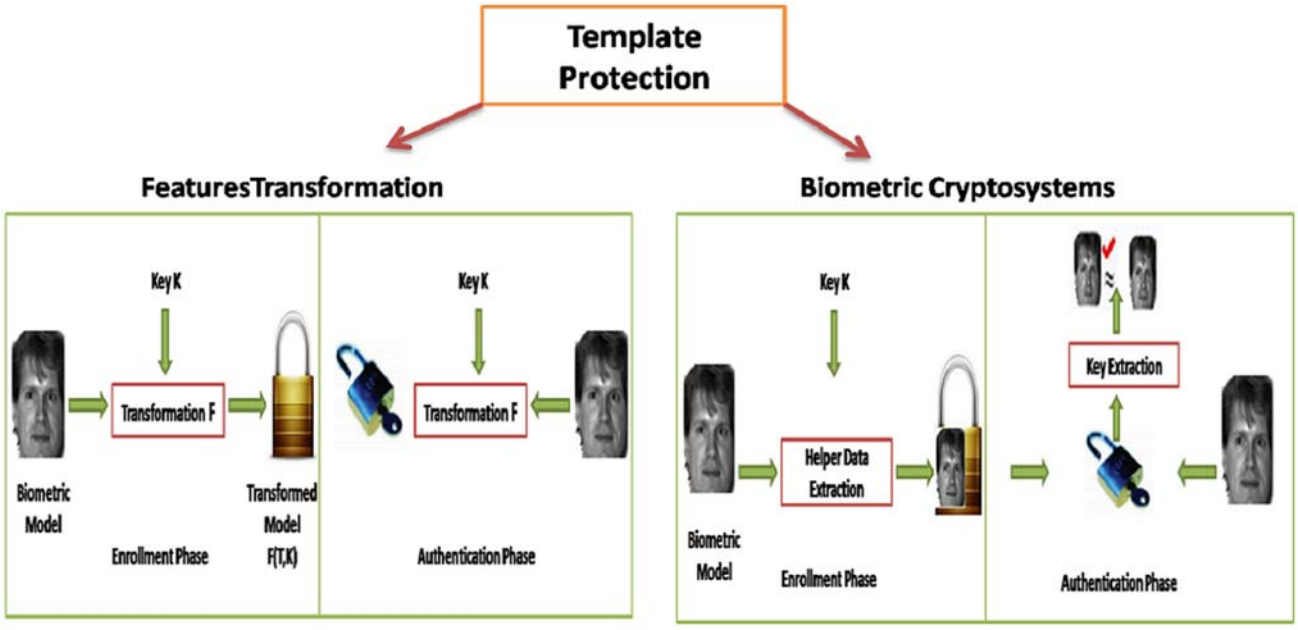

Figure 4. Protection methods of biometric template

To address the weakness of the *Fuzzy Commitment*, another main approach is proposed by Juels and Sudan [11] named Fuzzy

Vault. This method is based on the use of biometrics with a secret key that will be converted into polynomial, after a series of false points added to build a '*vault*'. The '*vault*' will be stored in the database instead of the user biometric template. To have access to the system, the authentication secret key must be retrieved using characteristics of the request and the '*vault*' already stored in the database. For a good illustration of the approach let's consider this example [29], if Alice has a secret *K*, she encodes it using a set *A* and publishes the result to know if someone has the same secret without revealing her own secret. Suppose that Bob uses another set *B*, if *B* overlaps substantially with *A*, then Bob can find the Alice secret, else the secret cannot be revealed by Bob because B not identical to *A*. *Fuzzy Vault* method allows Bob to recover the secret *K* if his set largely superimposes with the set of Alice. In this approach the protection of *K* requires to represent it by a polynomial *P* at first; to generate the set *R* using features *U* and *P* (*U*) at second, and finally to add false points to construct the vault. If characteristics of Bob are approximately close to Alice characteristics, he can find enough real point in *R*, using error correction coding to recover the secret *K*.

To secure the user characteristics $\{X_1, X_2,..., X_r\}$, a random key *K* is generated of length l, and converted into polynomial *P* of degree *d*. Using this polynomial we obtain the set $\{(Xi , P (Xi))\}_{i = 1}$ that is secured by hiding a set of random chaff points $(a_j , b_j)_{j = 1}$where $b_j \neq P (a_j)$ and $a_j \neq X_i$. The resulting set is considered as the vault *V*. In the authentication phase if the characteristics of query X_{query} are approximately close to the abscissas of the vault X_{vault}. The secret can be recovered using the code correcting error with capacity ε.

Fuzzy Vault approach was presented as solution for protecting biometric template and preserving privacy. However the security of several existing *Fuzzy Vault* schemes cannot, always, be valid for biometric systems, where an attacker could link several *vaults* generated from the same biometric trait or submit his own biometric template in the database in order to gain illegitimate access to the system etc... To better illustrate the weakness/strength of this approach against attacks, it is necessary to analyze the security of biometric cryptosystems based *Fuzzy Vault* approach.

4. Security Analysis

In order to compare different cryptosystems in terms of facility, level of the security etc ... the analysis of security is beneficial. To analyze the security of Fuzzy Vault, we are focused on four types of vulnerabilities namely: '*Intrusion Attacks*' , '*Binding Attacks*' , '*Combination Attacks*' and '*Injection Attacks*'. We are based in these types of attacks because they generalize critical vulnerabilities that can affect biometric cryptosystems, when an attacker can falsify the data (with or without help of the user) or link different biometric templates or also inject his data in the database. Proposed attacks can be applicable in all biometric cryptosystems independently to the used modality, system protection approach, parameters setting, etc....

• **Intrusion Attacks:** the attacker appears to the system with fake data for illegitimate access to the system. Liaison

• **Attacks:** the attacker tries to link several vaults of different systems to have the original model.

• **Combination Attacks:** the attacker combines his biometric data with the user data to have access.

• **Injection Attacks:** This attack consists of submitting the data of the attacker in the database to access to the system. This attack is proposed by Scheirer and Boul but without any criterion and any implementation to represent this scenario [29]. So we proposed a criterion for this attack and we visualized the feasibility of this scenario on the *Fuzzy Vault* method.

To evaluate the security and performance of *Fuzzy Vault* we have proposed criteria (1) to measure the performance and analyze the security while considering all previous attacks (2).

4.1 Performance evaluation

To evaluate the performance, our analysis is based on measuring the usability of systems using the False Accept Rate, which shows the number of impostor accepted by the system, and the *False Reject Rate*, which shows the number of users rejected by the system [34]. We distinguish between two cases : before encryption and after encryption.

4.1.1 Before Encryption

Before encryption, we measure the *False Reject Rate* of original system by the probability that the distance between characteristics of the user $X_{(U)}$ and characteristics of the query $X_{Query\,(U')}$ is greater or equal to the threshold ε.

$$FRR_O(\varepsilon) = P(D(X_{(U)}, X_{Query(U')}) \geq \varepsilon) \quad (1)$$

To measure the False Acceptance Rate in original domain, we propose to calculate the probability that the distance between the biometric characteristics of the user $X_{(U)}$ and biometric characteristics of the attacker $X_{Query(A)}$ is lower than ε:

$$FAR_O(\varepsilon) = P(D(X_{(U)}, X_{Query(A)}) < \varepsilon) \quad (2)$$

4.1.2 After Encryption

After encryption, the False Reject Rate is supposed as the probability that the cardinality of intersection between the abscissa of user vault $X_{vault(U)}$ and the characteristic of the query $X_{Query(U')}$ is greater than or equal to the threshold ε as follow:

$$FRR_E(\varepsilon) = P(card(intersect(X_{vault(U)}, X_{Query(U')})) \geq \varepsilon) \quad (3)$$

The False Acceptance Rate in encryption domain is defined by the probability that the cardinality of the intersection between the abscissa of the user vault $X_{vault(U)}$ and the characteristic of the attacker $X_{Query(A)}$ is lower than the threshold ε as illustrated by:

$$FAR_E(\varepsilon) = P(card(intersect(X_{vault(U)}, X_{Query(A)})) < \varepsilon) \quad (4)$$

4.2 Security evaluation

To measure the security we proposed several criteria based on the attacks previously mentioned. Presented criteria was defined based on the intersection of vault abscissas (that contain real characteristics of the user and chaff points added in the enrollment phase following the *Fuzzy Vault* schema) and the query characteristics estimated by the attacker.

4.2.1 Intrusion Attack

In *Intrusion Attack* we consider that the attacker knows the vault and encryption key of the first system *S*1 and he tries to gain access to the second system *S*2. We define this scenario known as *Cryptosystems Intrusion Rate in Different System* (*CIRD*) by the probability that the cardinality of (intersection of the vault abscissas of the user *U* generate using Key K_U in the second system *S*2 (i.e $X_{vault^{S2}(U^{S2}, K_U^{S2})}$)and query characteristics $X'_{query(U^{S1})}$ generated by the attacker using the known elements of first system (the vault and encryption key)) is lower than the threshold ε:

$$CIRD_E(\varepsilon) = P(card(intersect(X_{vault^{S2}(U^{S2}, K_U^{S2})}, X'_{query(U^{S1})}) < \varepsilon) \quad (5)$$

4.2.2 Liaison Attack

In *Liaison Attack or Correlation Attacks* we consider that an attacker tries to link two databases DB of different systems (*S*1 and *S*2) in order to have the original model of the user. We define this criterion by the probability that the cardinality of (intersection between the abscissas of vaults $X_{vaultDB}$ of the user *U* in the first system (i.e $X_{vaultDB^{S1}(U^{S1}, K_U^{S1})}$)) and the abscissas of vaults of the same user in the second system ($X_{vaultDB^{S2}(U^{S2}, K_U^{S2})}$)) is lower than the threshold ε:

$$CR_E(\varepsilon) = P(card(intersect(X_{vaultDB^{S2}(U^{S2}, K_U^{S2})}, (X_{vaultDB^{S1}(U^{S1}, K_U^{S1})})) < \varepsilon) \quad (6)$$

If an attacker tries to link just two vaults of different systems generated using the '*Same*' key i.e, *Correlation Attacks with Same Key*, we propose to calculate the probability that the cardinality of (intersection between the vault abscissas X_{vault} of the user *U* in the first system *S*1 generated using the Key K_U (i.e $X_{vault^{S1}(U^{S1}, K_U^{S1})}$) and the vault abscissas of same user *U* in the second system generated using the same Key K_U (i.e $X_{vault^{S2}(U^{S2}, K_U^{S2})}$) is lower than the threshold ε:

$$CRSK(\varepsilon) = P(card(intersect(X_{vault^{S2}(U^{S2}, K_U)}, (X_{vault^{S1}(U^{S1}, K_U)})) < \varepsilon) \quad (7)$$

We have considered also the case when an attacker tries to link two vaults of different systems generated using the '*different*' Key i.e, *Correlation Attacks with Different Key*. This criterion is defined by the probability that the cardinality of (intersection between the vault abscissas of the user *U* in the first system *S*1 generated using the Key K_U^{S1} (i.e $X_{vault^{S1}(U^{S1}, K_U^{S1})}$) and the vault abscissas of the same user in the second system *S*2 generated using the Key K_U^{S2} (i.e $X_{vault^{S2}(U^{S2}, K_U^{S2})}$)) is lower than the threshold ε:

$$CRDK(\varepsilon) = P\,(card\,(intersect\,(X_{vault^{S2}(U^{S2}, K_U^{S2})}, (X_{vault^{S1}(U^{S1}, K_U^{S1})})) < \varepsilon) \quad (8)$$

4.2.3 Combination Attack

Besides the previous attacks, we propose the scenario when an attacker combines his data with the data of a legitimate user, i.e. the user helps the attacker in order to gain access to the system. This scenario is presented by the probability that the cardinality of (intersection between the vault abscissas of the user U (i.e $X_{vault(U, K_U)}$) and the union of the user characteristics $X_{Query}(U)$ (in the same system) with the characteristics of the attacker $X_{Query}(A)$) is lower than the threshold ε. We explain this criterion as follow:

$$CA(\varepsilon) = P\,(card\,(intersect\,(X_{vault(U, K_U)}, union\,(X_{Query(U)}, X_{Query(A)}))) < \varepsilon) \quad (9)$$

We consider another scenario when the attacker combines his data with data of a legitimate user estimated using the key and the vault of a first system in order to attack a second system, we refer to this attack as Combination Attack in *Different Systems* (CADS). The combination attack is defined by the probability that the cardinality of (the intersection between the vault abscissas of the user U in the second system ($X_{vault^{S2}(U, K_U)}$)and the union of the characteristics of the user in the first system $X_{Query^{S1}}(U^{S1})$ with the characteristics of the attacker $X_{Query}(A)$) is lower than the threshold ε. We explain this criterion as follow:

$$CA_{diff}(\varepsilon) = P\,(card\,(intersect\,(X_{vault^{S2}(U, K_U)}, union\,(X_{Query^{S1}(U^{S1})}, X_{Query(A)}))) < \varepsilon) \quad (10)$$

4.2.4 Injection Attack

We present the case when the attacker submits his data in the database to gain access to the system. We represented this criterion by the probability that the cardinality of the(intersection of the abscissa of the stored vaults $X_{vault(U+A, K_U)}$ (using the characteristics of the user U and the characteristics of the attacker A) and the characteristics of the attacker $X_{Query}(A)$) is lower than the threshold ε as defined in this equation:

$$IA(\varepsilon) = P\,(card\,(intersect\,(X_{vault(U+A, K_U)}, (X_{Query(U)}, X_{Query(A)})) < \varepsilon) \quad (11)$$

After having proposed different criteria for security analysis, the second aim of our study is to apply these criteria on *Fuzzy vault* to evaluate the performance and analyze the security of this method. Hence the results are linked to each biometric cryptosystems (i.e. the results are depended on expression setting: feature extraction method, used modality, database size, and also used correcting code error, etc...).

5. Experiment Results

5.1 Experimentation Setting

In order to achieve the security analysis of biometric cryptosystems, we used biometric facial recognition systems. Thus, we need two biometric systems [21] using two different methods for features extraction of the face images (Figure 5) and a technique to protect the authentication scheme.

At first we created two biometric systems. One is based on the recognition of faces using *Laplacian Smoothing Transform* (LST) [6] for feature extraction followed by *Linear Discriminant Analysis* (LDA) [15]. In the second system LST is used for feature extraction and for selection of the most relevant, we used SVM-LDA (or SVDA) technique [5]. SVDA technique presents the advantages of both LDA and *Support Vector Machines* (SVM) [8]. We evaluated the performance these biometric systems using YALE database [2] that contains faces images taken from 10 different conditions: a normal image, with or without glasses, images taken with different light sources, and different facial expressions (Figure 6), we separated this base into basic training and test database. Then we calculated the distance between the user of the test and the reference. Practically, we have used face recognition systems and *Fuzzy Vault* as method for template protection based on Reed Solomon as error correcting code.

Fuzzy Vault can be constructed based on any error correcting code. In our implementation we have used Reed Solomon codes (R-S), this code is based on Galois Filed and considered a systematic way to correct and detect multiple symbol errors. $R-S\,(n, k)$ encoder takes as input k data symbols and then adds parity symbols to resulting n symbol codewords. $R-S\,(n, k)$ decoder takes as input the n symbols and tries to recover original data, the decoder is able to correct as many as $(n-k)/2$ errors in codeword depending on the characteristics of R-S code [14] [13] .

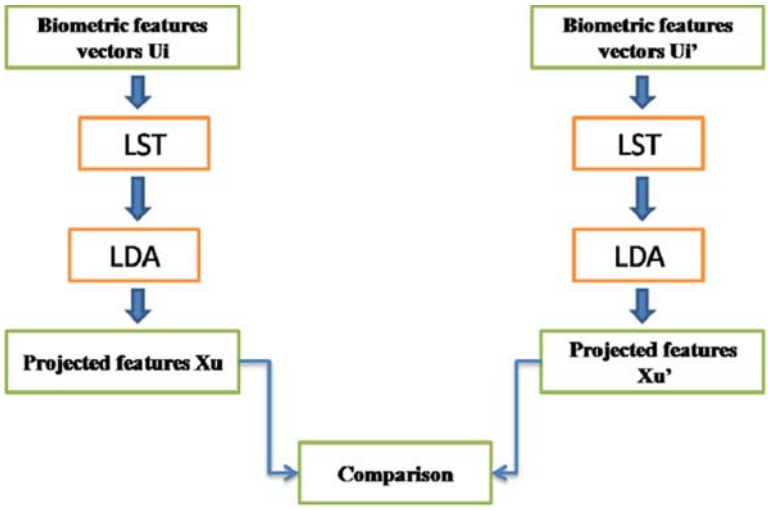

Figure 5. Facial recognition system (LST and LDA)

Figure 6. Example of samples in YALE database

Error correcting code EEC is used in many techniques of biometric cryptosystems to match the reference date and the query data and then user can authenticate despite the intra-class variation (feature variation of the same user). Hence error correcting code has important impact on systems performance. Amioy Kumar and Ajay Kumar have used Reed Solomon code to performance evaluation, they have presented the *Receiver Operating Characteristics* (*ROC*) curve (designed for performance evaluation and obtained by calculating different values of FAR and FRR for each value of the threshold) based on tolerance variation to achieve minimum false acceptance and rejection rates values [14] . Therefore we often compute performance of systems in multiple operating points based on variation of *False Accept Rate* and *False Reject Rate* with tolerance value of the code corrector error (i.e. we considered capacity of R-S code as decision threshold). To obtain complete *ROC* curve, several operating points must be generated to attain the corresponding combination for false acceptance and false rejection rates [24] . Yagiz Sutcu and Qiming Li [30] have represented the *ROC* curve based on variation of quantization step size that can be determined in different ways such as tolerance of noise level and in [31] they have illustrated *ROC* curves of fingerprint and face features by varying detection parameters.

In [13] Kelkboom and Zhou have used Cyclic Redundancy Check (CRC) to decode correct secret and they have illustrated an example of corresponding correction number and the error rate. In our study the goal is not defined the threshold to have minimum error rate, but to show the variation of the rate of proposed attacks according to several threshold and then make a decision of the system in term of security and performance.

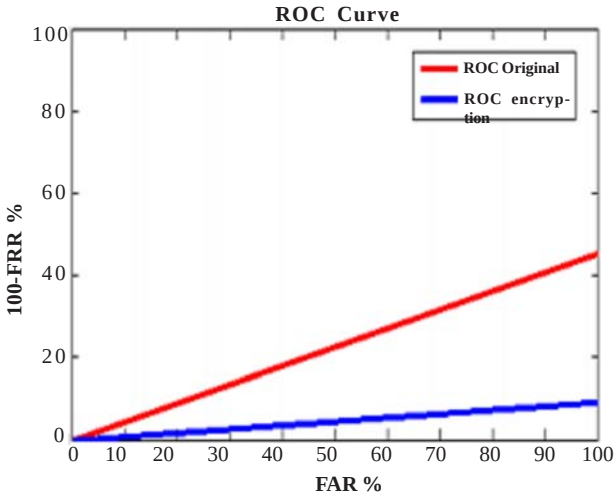

Figure 7. $ROC_{original}$ and $ROC_{encryption}$ curves

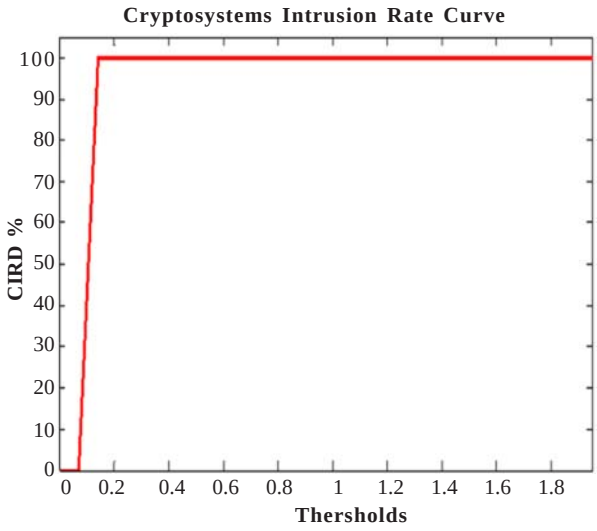

Figure 8. CIRD Curve

5.2 Performance Evaluation

In this work we used the *Receiver Operating Characteristics* curves *ROC* to visualize the performance of the biometric system before and after encryption. Figure 7 shows the ROC curves of the biometric system, at first without the protection scheme ($ROC_{original}$) and then with the protection scheme ($ROC_{encryption}$). We remark the degradation of the performance after using protection scheme of the user template explained by the use of error correcting codes where the number of errors that can be corrected has a strict threshold.

5.3 Security Evaluation

5.3.1 Intrusion Attack

In the *Intrusion Attack*, an attacker tries to use the information of the first system to have access to a second system. The attacker knows the key and the vault stored in the first system and use them to gain access to the second system. Figure 8 shows the results of this attack, with a threshold of 0:14 or larger the attacker can successfully access to the second system using the helper data and the encryption key of the first system which means that only the intra-class prevents the access to the system. The threshold value plays a very interesting role in the system. When the threshold is high we can accept more dissimilarity between user and request characteristics.

5.3.2 Liaison Attack
Attacker here wants to link the two databases of both systems to get user characteristics and keys. As shown in Figure 9 (a), correlation rate increases from 0 to 50% then we have a binding rate that equals 100% depending on the thresh-olds. When the threshold is high the two databases are linked and then more dissimilarity is accepted into the system.

Figure 9 (b) shows the results when an attacker attempts to link two vaults of different systems using the same biomet-ric trait and the *Same key*. We have 2:25% as binding rate of vaults when the threshold is null. We notice an increase of binding rate depending on the thresholds to reach a 100 % success when the threshold is greater or equal to 1.

Figure 9 (c) shows the results of linking two vaults generated using two *Different keys*. The binding rate is increased from 20% to reach a correlation rate of 100%.

As a comparison of the three correlation attacks we have presented the results in Figure 9 (d). We notice that an attacker can easily link two vaults generated by the same key than two vaults generated by two different keys.We remark also that the correlation rate is very high for connecting two databases. This can be explained by the fact that the attacker has several samples of legitimate users and uses them to launch easily the attack.

5.3.3. Combination Attack
In *Combination Attack*, the attacker will build a single data from his characteristics and of the legitimate user char-acteristics to gain access to the system. This attack can reach a 100% success as shown in Figure 10 (a). It can be considered as falsification of data where a user of the system helps the attacker to have an illegitimate access. Figure 10 (b) shows the results of combination attack in a second system. The probability of success is null for thresholds less than 0035, and increase to a 100% for a threshold above 0.1. In Combination Attack in Different System, the attacker has difficulty compared to the Combination Attack in Same System as illustrated by CA curve because in *Combination Attack* in *Different System* the attacker use the element of the first system to gain access in second system that use the same trait of the user (both system are different) when in the case of *Combination Attack* in *Same System* the attacker use the element of the first system in order to gain access in the same system(one system is used).

5.3.4 Injection Attack
In *injection Attack*, instead of combining his data with the user, the attacker injects his data in the user's database in order to be accepted by the system. In this case even a user can be considered as an attacker by the system and hence we can have users that are rejected while the attacker can be considered as legitimate user.

Figure 11 illustrates the injection rate according to thresholds, for a threshold less than 1.04 we have low injection rate which will increase with the given threshold. In this scenario, the vault stored in the database contain user data and attacker data, hence in the user authentication case, the data of the user may be considered as chaff points, which imply that the user can be rejected by the system. In the case of attack the system can accept the attacker because the vault contains attacker data and then attacker data was considered as genuine points.

6. Discussion

Biometric cryptosystems aim to integrate the benefits of using a secret key (encryption) and biometric features in a security system. Biometric Cryptosystem schemes can be evaluated in terms of performance and security analysis. There is no formal metrics to calculate the performance of biometric cryptosystems, therefore we have proposed formal criteria to calculate the FRR and FAR and then to evaluate the conviviality of the system practically the *Fuzzy Vault* Cryptosystem. Moreover, we have proposed four types of vulnerabilities that can be staged against biometric cryptosystems. According to the proposed tests we make decision in terms of the performance and security of this biometric cryptosystem approach.

The first type of vulnerabilities defined in this study is *Intrusion Attack* when the attacker presents fake data for illegitimate access to the system. In this attack we suppose that attacker has access to vault and key of the first system and tries to attack the second system that uses same biometric traits of user. We called this criterion *Cryptosystems Intrusion Rate in Different Systems*. The authentication system is vulnerable to this type of attack and attacker can easily decode the vault and gain access to the system.

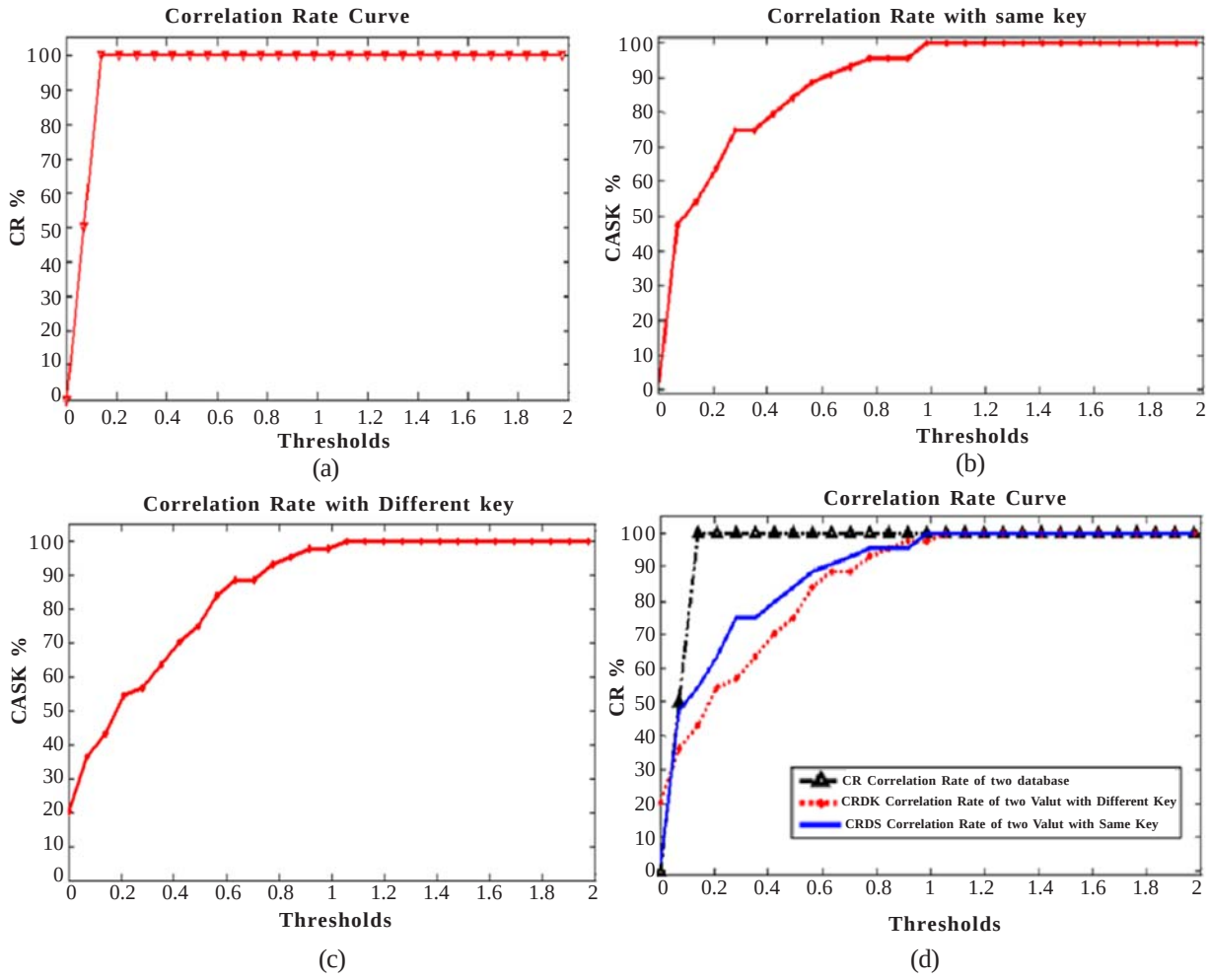

Figure 9. (a) CR (Correlation Rate of two databases) Curve, (b) CRSK (Correlation Rate with Same Key) Curve, (c) CRDK (Correlation Rate with Different Keys) Curve, (d) Comparison of the different Correlation Attacks

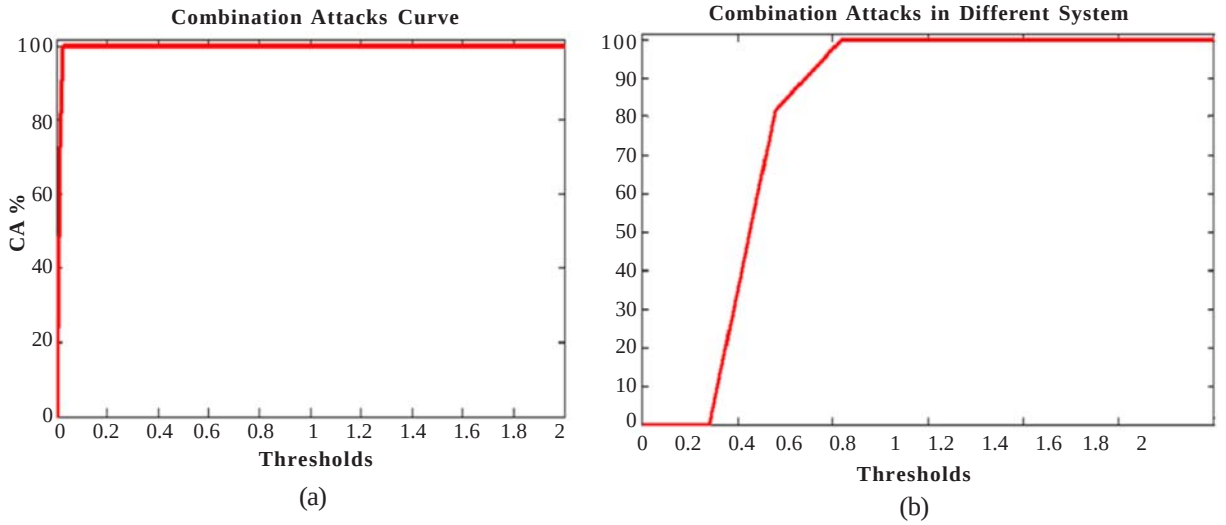

Figure 10. (a) CA (Combination Attack in the Same system), (b) CAdiff (Combination Attack in the Different system)

The second type of proposed vulnerabilities is *Liaison Attack* when attacker has access to different vaults generated from the

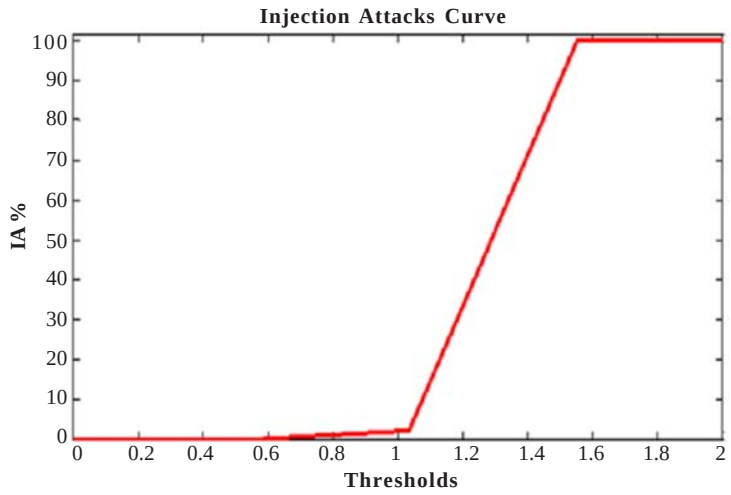

Figure 11. Injection Attacks

same biometric traits of the same user (for example from different applications), thus multiple scenarios are proposed. In the first scenario we suppose that attacker tries to link two databases of both systems. In the second scenario, attacker tries to link two vaults of the same user generated using the same key (*Liaison Attacks with Same Key*) and stored in two different systems that use the same biometric trait of the user. In the last scenario attacker tries to link two vaults of two systems using different keys (*Liaison Attacks with Different Key*).

The attacker can easily identify the genuine points by linking two databases compared to the liaison of two different vaults. This vulnerability can be explained by the fact that attacker uses several samples of legitimate users (stored in the database) and then he can recover more information about the real user to initiate easily the attack.

Besides the previous attacks, we proposed *Combination attacks* that can be considered as falsification attacks when user helps attacker to gain access to the system. We have considered two scenarios, the first case when attacker tries to gain access to the same system, the second case when attacker tries to gain access to the second system using the same biometric traits of the user *Combination Attack in Different Systems* (CADS). In this combination the attacker has difficulty compared to combination attack in the same system (first case). The last type of proposed attacks is *injection attack* when attacker injects his own biometric data in the vault to gain access to the system, then both, user and attacker can be authenticated using same vault.

After launching previous attacks on *Fuzzy Vault* method, we note that this method does not allow high level of security. Indeed this approach is vulnerable to intrusion attacks where an attacker can access to the same system or also use data of one system to access to another system that uses same feature of user. Only the intra-class variation which reduces the rate of this attack because the attacker can estimate the original features using the known elements (helper data and encryption key). *Fuzzy Vault* is also vulnerable to liaison attack when attacker can easily link different database or make connection between two generated vaults using the same key in a first scenario or generated from a different key in a second scenario. In both scenarios of combination attack, attacker has a difficulty to access illegitimately to the second system compared to accessing the same system. This difficulty can be explained by variability between query generated by the attacker and features of the legitimate user. Over these previous attacks, *Fuzzy Vault* is also vulnerable to injection attacks when the attacker injects his data into the vault of legitimate user. In this attack user and attacker can be authenticated using the same vault and then the system can accept the attacker and reject legitimate user. Even if *Fuzzy Vault* technique has been developed in order to secure data of legitimate user, this method has several limitations and does not allow a high level of security and privacy protection as we have shown in the experimental results section of the present work.

7. Conclusion

Biometric cryptosystems are developed in order to enforce protection and address the vulnerabilities in biometric models. In this paper, we have focused our work on four types of attacks: *Intrusion, Liaison, Combination* and *Injection attacks*. We have introduced different measurements and applied the proposed criteria on biometric facial recognition system protected by *Fuzzy*

Vault approach to assess the security strength of this scheme. In our analysis we used different values of thresholds depending on error correcting code. We have proposed some criteria that allow evaluation of the security of this method and also make the difference between security and conviviality of the system. Regardless, the limitation of the security of this approach enables us to conclude that *Fuzzy Vault* does not provide security for biometric systems or protection of user's privacy. The obtained results show that *Fuzzy Vault* method is vulnerable to the proposed attacks. The experimental field in the future will be extended to include different criteria to assess the security of the protection schemes of biometric systems. As future work, we plan to offer other attack scenarios to evaluate the strength of different template protection approaches.

References

[1] Adler, A. (2003). Sample images can be independently restored from face recognition templates. *In*: Electrical and Computer Engineering. IEEE CCECE 2003. Canadian Conference on, 2, 1163–1166. IEEE.

[2] Belhumeur, P. N., Hespanha, J. P., Kriegman, D. J. (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection, *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19 (7) 711–720.

[3] Daugman, J. (2003). The importance of being random: statistical principles of iris recognition. *Pattern Recognition*, 36 (2) 279–291.

[4] Gonzales Barron, U., Corkery, G., Barry, B., Butler, F., McDonnell, K., Ward, S. (2008). Assessment of retinal recognition technology as a biometric method for sheep identification. *Computers and Electronics in Agriculture*, 60 (2) 156–166.

[5] Gu, S., Tan, Y., He, X. (2010). Discriminant analysis via support vectors. *Neurocomputing*, 73 (10) 1669–1675.

[6] Gu, S. C., Tan, Y., He, X. (2010). Laplacian smoothing transform for face recognition. *Science China Information sciences*, 53 (12) 2415–2428.

[7] Hao, F., Anderson, R., Daugman, J. (2006). Combining crypto with biometrics effectively, *IEEE Transactions on Computers*, 55 (9) 1081–1088.

[8] Hearst, M. A., Dumais, ST., Osman, E., Platt, J., Scholkopf, B. (1998). Support vector machines. *Intelligent Systems and their Applications*, IEEE, 13 (4) 18–28.

[9] Jain, A. K. (2006). Biometric system security. *In*: 4th Int Symp Comput Media Stud Biom Authentication Symp Kyoto 2006, p. 120–131.

[10] Jassim, S., Al-Assam, H., Sellahewa, H. (2009). Improving performance and security of biometrics using efficient and stable random projection techniques. *In*: Image and Signal Processing and Analysis. ISPA 2009. *In*: Proceedings of 6th International Symposium on, p. 556–561. IEEE.

[11] Juels, A., Sudan, M. (2006). A fuzzy vault scheme. Designs, Codes and Cryptography, 38 (2) 237–257.

[12] Juels, A., Wattenberg, M. (1999). A fuzzy commitment scheme. *In*: Proceedings of the 6th ACM conference on Computer and communications security, p. 28–36. ACM.

[13] EJC Kelkboom, Zhou, X., Breebaart, J., RNJ Veldhuis, Busch, C. (2009). Multi-algorithm fusion with template pro-tection. In Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on, p. 1–8. IEEE.

[14] Kumar, A., Kumar, A. (2008). A palmprint-based cryptosystem using double encryption. *In*: Proc SPIE *Conf Biometric Technology for human identification*, 6944, 69440D–1.

[15] Li, J., Janardan, R., Li, Q. (2004). Two-dimensional linear discriminant analysis. *Advances in Neural Information Processing Systems*, 17, 1569–1576.

[16] Li, Q., Sutcu, Y., Memon, N. (2006). Secure sketch for biometric templates. Advances in Cryptology–ASIACRYPT 2006, p. 99–113.

[17] Li, S. Z., Jain, A. K. (2011). Handbook of face recognition. Springer.

[18] Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. (2009). Handbook of fingerprint recognition. springer.

[19] Martinez-Diaz, M., Fierrez-Aguilar, J., Alonso-Fernandez, F., Ortega-Garcia, J., JA Siguenza. Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. *In*: Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, p.151–159. IEEE.

[20] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S. (2002). Impact of artificial gummy fingers on fingerprint systems. *In*: Proceedings of SPIE, 4677, 275–289.

[21] Moujahdi, C., Ghouzali, S., Mikram, M., Abdul, W., Rziza, M. (2012). Inter-communication classification for multi-view face recognition. *In*: The 4th *International Conference on Multimedia Computing and Systems* (ICMCS), Tangier, Morocco.

[22] Nagar, A., Nandakumar, K., Jain, A. K. (2010). Biometric template transformation: a security analysis. *In*: Proc. *SPIE, Electronic Imaging, Media Forensics and Security* XII.

[23] Anil K. Jain Nagar, Karthik Nandakumar. (2010). A hybrid biometric cryptosystem for securing fingerprint minutiae models. Elsevier *Pattern Recognition Letters*.

[24] Nandakumar, K. (2008). Multibiometric systems: fusion strategies and template security. ProQuest.

[25] Peterson, W. W., Weldon, E. J. (1972). Error-correcting codes, Revised. MIT press.

[26] Ratha, N., Connell, J., Bolle, R. (2001). An analysis of minutiae matching strength. *In*: Audio-and Video-Based Biometric Person Authentication, p. 223–228. Springer.

[27] Ross, A., Jain, A. (2003). Information fusion in biometrics. *Pattern Recognition Letters*, 24 (13) 2115–2125.

[28] Ross, A., Shah, J., Jain, A. K. (2005). Towards reconstructing fingerprints from minutiae points. *In*: Proc. SPIE, Biometric Technology for Human Identification II, 5779:68–80.

[29] Scheirer, W. J., Boult, T. E. (2007). Cracking fuzzy vaults and biometric encryption. *In*: Biometrics Symposium, p. 1–6. IEEE.

[30] Sutcu, Y., Li, Q., Memon, N. (2007). Protecting biometric templates with sketch: Theory and practice. *IEEE Transactions on Information Forensics and Security*, 2 (3) 503–512.

[31] Sutcu, Y., Li, Q., Memon, N. (2007). Secure biometric templates from fingerprint-face features. *In*: Computer Vision and Pattern Recognition. CVPR'07. IEEE Conference on, p. 1–6. IEEE.

[32] Uludag, U., Pankanti, S., Prabhakar, S., Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. *In*: Proceedings of the IEEE, 92 (6) 948–960.

[33] Van der Putte, T., Keuning, J. (2000). Biometrical fingerprint recognition: don't get your fingers burned. *In*: Proc. IFIP, p. 289–303.

[34] Wayman, J. L. (2002). Technical testing and evaluation of biometric identification devices. *Biometrics*, p. 345–368.