Security Analysis of Key Binding Biometric Cryptosystems

Maryam Lafkih[1], Mounia Mikram[1,2], Sanaa Ghouzali[1,3], and Mohamed El Haziti[4]

[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. The use of biometric systems is becoming an important solution to replace traditional authentication. However, biometric systems are vulnerable to attacks. When biometric data is compromised, unlike a password, it can't be changed. Therefore, the security of biometrics models is essential in designing an authentication system. To achieve this protection of biometric models, two categories of approaches are proposed in the literature, namely, methods based on transformation of characteristics and biometric cryptosystems. For the first type of approaches, a study is made to assess the security of biometric systems. In biometric cryptosystems the realized works are hampered by the lack of formal security analysis. Hence the purpose of this paper is to propose standard criteria for a formal security analysis of biometric cryptosystems. The proposed measures take into account the specific effect of key binding cryptosystems. The security analysis is illustrated by experiments on the techniques of *Fuzzy Commitment* and *Fuzzy Vault* which we use in this work for the protection of biometric face recognition system. Our analysis indicates that both techniques are vulnerable to intrusion and binding attacks because of the ease of obtaining the user's model using the elements known to the attacker.

Keywords: Security analysis, Biometric cryptosystems, Performance evaluation, Models transformation.

1 Introduction

Today, the need for security systems is becoming a necessity in the world. To better meet this need, biometrics is presented as a real alternative to passwords and other identifiers. It ensures that the user is who he claims to be, thereby reducing the risk of theft, loss or forgetfulness. However, biometric systems are not protected against attacks and a template stored in a database can be stolen by an attacker for an illegitimate access. This would mean that legitimate users should not be able to use the compromised model to authenticate [1]. To overcome this problem, one idea would be to secure biometric authentication scheme.

A. Elmoataz et al. (Eds.): ICISP 2012, LNCS 7340, pp. 269–281, 2012.

In the literature there are two types of methods to protect biometric templates: Methods based on the transformation of biometric features and biometric cryptosystems [2]. The first type of methods consists on applying a transform function on the biometric characteristics to build a model that will be stored in the database (enrollment phase). During authentication, the same function is applied to the biometric characteristics of the query template to obtain a model that is then compared to the stored reference model to allow or deny the access [2]. Biometric cryptosystems use a secret key to wrap the biometric characteristics and generate an auxiliary data that will be stored in the database (enrollment phase). In the authentication phase the secret key must be extracted from the biometric characteristics of the query and the auxiliary data stored [3].

However, these biometric technologies include several components that have weaknesses and limitations such as high cost, risk of tampering and poor performance. To this end a performance evaluation is a necessity for comparing different systems. In the case of characteristics transformation methods, a study is made by Nagar et al. [4] for the security evaluation of biometrics systems. Although cryptosystems are used in the real world (e.g. smart cards) [5], their practical applicability is hampered by the lack of a formal security analysis. Thus, the objective of this work is to propose a set of standard criteria to evaluate the overall security of biometric cryptosystems.

In the rest of this article, biometric cryptosystems are described in Section 2, and then in Section 3 the analysis of the security of cryptosystems is detailed. In Section 4, experimental results illustrate how the proposed measures can be used to evaluate biometric cryptosystems. Conclusion and perspectives are drawn in Section 5.

2 Biometric Cryptosystems

Biometric cryptosystems are techniques that aim to integrate the benefits of using a secret key (encryption) and biometric features in a security system [6] [7]. A several approaches developed in the field of biometric cryptosystems are based on two modes of generation of the secret key. Thus, we can distinguish between two types of cryptosystems along the two modes (1) *Key binding biometric cryptosystems* [5]: where the biometric template is linked with a secret key in a single entity to build an auxiliary data. This data reveal no information on the key or the biometric template and (2) *Key generation biometric cryptosystems* [8]: where the key is derived directly from the biometric data. Authentication is successful if the key is retrieved.

In the literature there are two main approaches to perform key binding biometric cryptosystems: *Fuzzy Commitment* and *Fuzzy Vault* [9]. The first approach, proposed by Juels and Wattenberg [10], consists on using biometric features and secret key to generate a helper data. The pair that contains the helper data and the secret key encrypted is then stored in the database. In the authentication phase the key must be regenerated from the helper data stored in the database and biometric features of the query template. The second approach, proposed by Juels and Sudan [11], aims to generate a polynomial p from a secret code and biometric characteristic and then add false points to construct a Vault V that will be stored in the database. During

authentication it must find the secret code from the Vault stored and the biometric features of the query in order to succeed the access.

However, these biometric cryptosystems include several components that have gaps and limitations such as the high cost, risk of falsification and poor performance. To this end, a performance evaluation is a prerequisite for comparison between different biometric systems. To ensure the security and protection against the risks associated with these systems, the security analysis of biometric cryptosystems consists of measuring these risks according to the probability or frequency of their appearance and their possible effects. Nagar and al [4] have made a study for security analysis of biometric systems. In the case of biometric cryptosystems the studies are made specifically for each approach; there is no formal analysis to analyze the security of all biometric cryptosystems. In next section we propose a set of generalized criteria to evaluate the overall security of biometric cryptosystems.

3 Security Analysis of Biometrics Cryptosystems

The security analysis plays an important role to evaluate the performance of biometric systems; it can test several components such as the ease of the system, the security … etc. To analyze the security of biometric cryptosystems, we focused on vulnerability to intrusion attacks and binding attacks. The term "*Intrusion"* is the access to a biometric system by submitting fake authentication data for the system. "*Binding"* attacks involve the mapping of multiple biometric models generated from different encryption parameters to find the original model. To cope with these attacks, it is important to analyze the probability of their success in a cryptosystem.

To describe the security measures of biometric cryptosystems, we used the following notation: X_U and X_U' represent the model of the user and biometric characteristics of the request for the same user, X_A the biometric characteristics of the attacker, H is the auxiliary data, K_U and K_U' are two different keys of the user and K_A *is* the key of the attacker. D_O (respectively D_E) is a function of distance between the original models (respectively auxiliary data in encrypted domain). The user will be accepted by the system if the distance between the model and biometric characteristics of the query is below a threshold ε.

We have proposed criteria for (1) measure of the usability of the system, (2) measure of the security for intrusion threats evaluation and (3) measure of the security for binding threats evaluation.

3.1 Measure of the Usability of a System

Measuring the usability of a system is made in terms of False Rejection Rate "*FRR"*. The *FRR* is the percentage of the users rejected by the system out of the total number of users in the database [12]. Therefore we distinguish two cases; before encryption and after encryption.

The False Rejection Rate of the biometric system in Original domain i.e. before the encryption, "FRR_O" is expressed by the probability that the distance between the biometric characteristics of the user X_U and the biometric characteristics of the request X_U' is greater than or equal to the threshold ε.

$$FRR_O(\varepsilon)=P\ (\ D_O\ (\ X_U\ ,\ X_U')\geq \varepsilon) \quad (1)$$

The *False Rejection Rate of the biometric system after the application of encryption*, i.e. False Reject Rate in encrypted domain, "FRR_E" is expressed by the probability that the distance between the helper data of the user and the helper data of the request is greater than or equal to the threshold ε as given by the following equation:

$$FRR_E(\varepsilon) = P\ (DE\ (H_U\ (X_U,\ K_U),\ H_U\ (\ X_U',\ K_U))\geq \varepsilon) \quad (2)$$

3.2 Measure of the Security of Intrusion Threats

The measure of the security of intrusion threats is defined as the probability of a successful attack, assuming that the model stored in the database and encryption parameters are available to the attacker attempting to usurp the identity of a trusted user. The probability of successful intrusion threats is given by the *False Acceptance Rate* "*FAR*". The *FAR* gives the percentage of accepted attackers among the number of attackers who come to the system [12]. We have proposed criteria for both cases; before encryption and after the encryption.

False Acceptance Rate of original biometric system before encryption "FAR_O" is given by the probability that the distance between the biometric characteristics of the user X_U and the biometric characteristics of the attacker X_A is lower than the threshold ε as it is illustrated in the following equation:

$$FAR_O(\varepsilon)=P(D_O(X_U,\ X_A\ )<\varepsilon) \quad (3)$$

For the case after encryption, the attacker is required to submit biometric characteristics with a set of encryption parameters for authentication. Therefore, there are two possibilities; the case where the parameters are '*Unknown*' to the attacker and the case where the parameters are '*known*' to the attacker. Suppose that the attacker doesn't know the encryption parameters for the specific user. We calculate in this case the *False Acceptance Rate with Unknown encryption parameters* "FAR_{UP}" given by the following equation which expresses the probability that the distance between the helper data of the user and the helper data of the attacker generated by its own key K_A is lower than the threshold ε.

$$FAR_{UP}(\varepsilon)=P\ (D_E\ (H_U(X_U,K_U),\ H_A(\ X_A\ ,K_A)<\varepsilon) \quad (4)$$

If the attacker knows the encryption parameters of the user, the *False Acceptance Rate with Known encryption parameters* "FAR_{KP}" is defined by the probability that the distance between the helper data of the user and the helper data of the attacker generated by the same key of the user K_U is lower than the threshold ε, as indicated in the following equation:

$$FAR_{KP}(\varepsilon)=P\ (D_E\ (\ H_U\ (\ X_U\ ,\ K_U),\ H_A\ (X_A\ ,\ K_U)\ )<\varepsilon) \quad (5)$$

In addition to the False Acceptance Rate, we considered other probabilities of intrusion after encryption where the stored model and the encryption parameters are

available to the attacker to gain an illegitimate access to a '*Different*' biometric system which uses the same biometric characteristics. Suppose that the attacker knows also the encryption parameters of the second system. In this case, he will try to retrieve the biometric model using the model encrypted and the encryption parameters of the second system. The probability of success of such attack is called the *Cryptosystem Intrusion Rate of Different system with known Parameters* "$CIRD_{KP}$" and is defined by the Equation 7 that expresses the probability that the distance between the helper data of the user stored in the second system H_U^{S2} and the helper data of the attacker H_A (generated by the feature X'_U estimated using the two keys of the user (the key of the first system and the key of the second system) and the helper data of the user stored in the first system) is lower than the threshold ε:

$$CIRD_{KP}(\varepsilon) = P(D_E (H_U^{S2}(X_U,K_U), H_A (X'_U,K'_U)) < \varepsilon) \quad (6)$$

If the attacker knows the helper data and the encryption parameters of the user in the first system without knowing the encryption parameters of the second system, the attack performed in this case is called the *Cryptosystem Intrusion Rate of Different system with Unknown Parameters* '$CIRD_{UP}$'. The success of this attack can be expressed by the probability that the distance between the helper data of the user stored in the second system H_U^{S2} and the helper data of the attacker H_A (generated by the feature X'_U, estimated using the key of the user in the first system and both helper data of the user stored in the first and the second systems, and his key K_A) is lower than the threshold ε as specified by

$$CIRD_{UP}(\varepsilon)=P(D_E (H_U^{S2}(X_U,K_U), H_A(X'_U,K_A))<\varepsilon) \quad (7)$$

3.3 Measure of the Security of Binding Threats

The measure of the security for the evaluation of binding attacks is defined as the probability of a successful attack to link different models of the same biometric trait of the user and different parameters encryption. Suppose that the two sets of encryption parameters are known to the attacker. The *Cross Rate in the Encrypted* fields "CR_E" can be defined by the probability that the distance between the helper data of the user in the first system $H_U^{S1}$and the helper data of the user in the second system H_U^{S2} is lower than the threshold (ε equation 8):

$$CR_E(\varepsilon)=P(D_E (H_U^{S2}(X_U,K_U), (H_U^{S1}(X_U',K'_U)<\varepsilon) \quad (8)$$

Besides these attacks, we assume the case where the attacker will attempt to combine the helper data of the trusted user and his own helper data H_A (generated from his biometric data and his own key K_A) which we named the *Combination Attack;* '*CA*'. To illustrate this scenario we consider the following criterion which consists of the probability that the distance between the result of combination and the helper data of the user is lower than the threshold ε.

$$CA(\varepsilon)=P(D_E (H_U(X_U,K_U), (H_U(X'_U,K_U)+ H_A(X_A,K_A))<\varepsilon) \quad (9)$$

We also proposed another criterion, *Combination Attack in a 'different' system* "CA_{diff}", fin which we assume that the attacker has the encryption parameters and the helper data of the user in the first system and tries to have access to a second system. We expressed this criterion by the probability that the distance between the helper data of the user stored in the first system H_U^{S1} and the result of combination (of the helper data of the user in the first system and the helper data of the attacker generated by the key of the user K'_U) is lower than the threshold ε by

$$CA_{diff}(\varepsilon)=P(D_E (H_U^{S2}(X_U,K_U), (H_U^{S1}(X'_U,K'_U)+ H_A(X_A,K'_U)) < \varepsilon) \quad (10)$$

4 Experiments

In order to evaluate the proposed security analysis framework of biometric cryptosystems, we considered the example of biometric systems based on face recognition. Thus, we need two biometric systems using two different methods for extracting features of the face images and a technique to protect the authentication scheme.

4.1 Experimental Settings

At first we created two biometric systems, the first biometric system is based on "*Laplacian Smoothing Transform, LST*" [13] method used for feature extraction followed by "*Linear Discriminant Analysis, LDA*" [14]. The second biometric system [15] uses *LST* for feature extraction followed by Support Vector-Discriminant Analysis (*SVDA)* technique [16] for dimensionality reduction. We evaluated the performance of biometric systems using the *YALE face* database [17] separated into training and test subsets. Then we calculated the *Hamming distance* between the user of the test and the reference for matching. In a second step we used the *Key binding* biometric cryptosystems (*Fuzzy Commitment* and *Fuzzy Vault*) to secure the two biometric systems. We used *Reed Solomon error correcting code* that allows recovering the data even in the case of error transmission [18]. The hash function *SHA-1* [19] has been used in this work to encrypt the secret key in Fuzzy Commitment scheme. In a third step we applied the criteria proposed in Section 3 to analyze the security of these systems.

To evaluate the performance of biometric systems, there are several important components to test such as the system reliability and performance. We measured the performance of biometric systems using a false acceptance rate set correspondence with a false rejection rate. To view the performances of biometric systems when the threshold varies, we used the *ROC* (Receiver Operating Characteristics) [20] curves representing the *FAR* from *1-FRR*. The "ROC_{orig}"(*FARo* from *1-FRRo*) curve present the original system i.e. before encryption, the system after encryption in case the attacker knows the encryption parameters and the case where the attacker does not know the encryption parameters is presented by "$ROC_{Unknown}$"(FAR_{UP} from $1\text{-}FRR_E$).

4.2 Security Analysis Results of Fuzzy Commitment Technique

Figure 1 (a) shows the different *ROC* curves of the first system. We notice performance degradation compared to the original model in case the encryption parameters are unknown and increased degradation in the case that the attacker knows the encryption parameters as indicated by the curve ROC_{known}. As it is shown, the original system ROC_{orig} is better than the system after encryption, in case where the attacker has just his biometric traits and attempts to gain illegitimate access to the system as expressed in $ROC_{Unknown}$ curve, we notice that the system accepts up to 47% of the attackers and in the case where the attacker knows also the encryption parameters of the system we notice less performance compared to the previous scenario (as indicated by the ROC_{known} curve).

In the second system represented by Figure 1 (b), we note that there is always a degradation of performance compared to the original model in the case of intrusion with unknown parameters as shown by the $ROC_{Unknown}$ curve, and the degradation of the performance increases if the attacker knows the encryption parameters as it is indicated by the curve ROC_{known}. ROC_{orig} curve shows also that the original system is better than the system after encryption; we note that the system accepts a maximum of 11.36% of the attackers in the case of unknown parameters ($ROC_{Unknown}$).

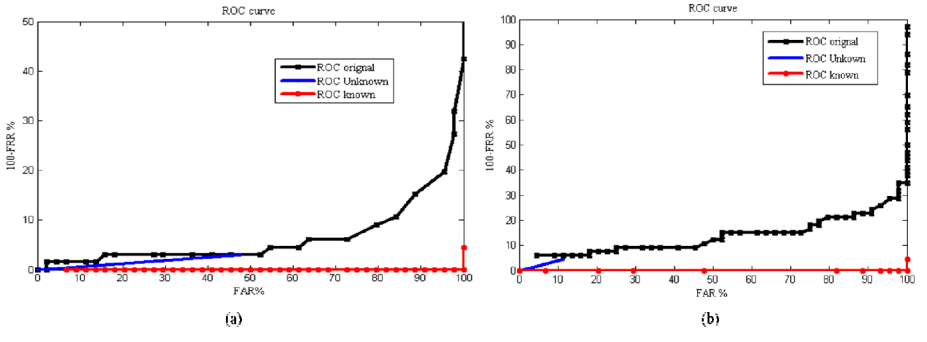

Fig. 1. ROCorig, $ROC_{Unknown}$, ROC_{known} curve of the first system (a) and the second system (b)

As comparison of the two systems, the second system is more efficient than the first; this performance can be explained by the use of the *SVDA* method which gives better results than *LDA* [14].

For intrusion attacks we also evaluated the measures of the criteria, $CIRD_{KP}$, CR_E and $CIRD_{UP}$.

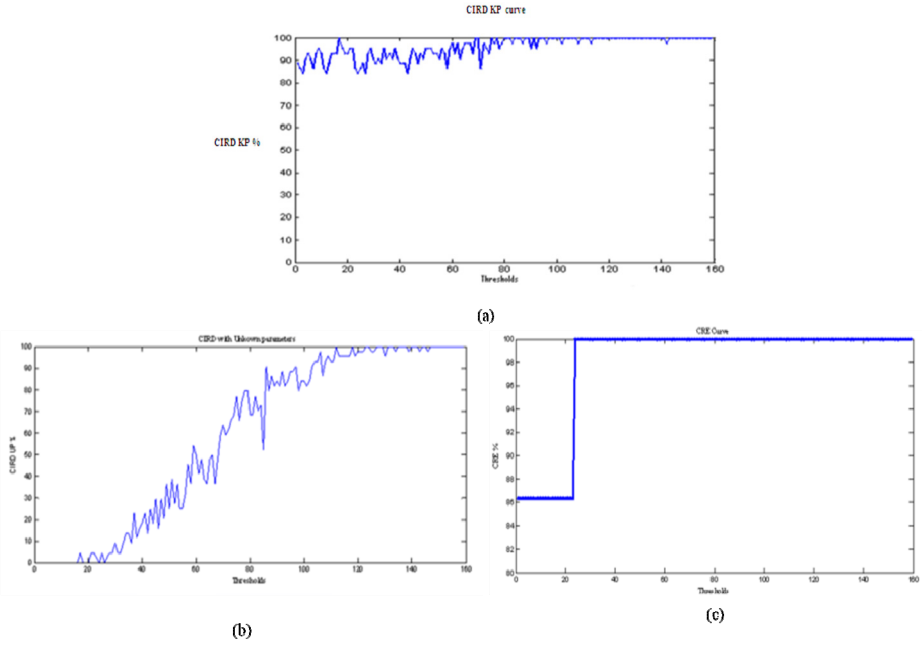

Fig. 2. *CIRDKP, CR_E, $CIRD_{UP}$* curves of *Fuzzy Commitment*

Figure 2 (a) shows the representation of $CIRD_{KP}$ for different thresholds. This figure shows the possibility of success of the attacker to access a '*different*' system that uses the same biometric traits of the user. We note that the probability of success of the attacker is changed if the threshold is less than or equal to 80, due to the intra-class variation between the user and the attacker. This variation prevents the attacker to gain 100% access to the system. As it is shown in the curve, the minimum probability that an attacker can access to the system is equal to 86%. So even with the intra-class variation, the probability that an attacker succeeds to access the system remains high. For a threshold above 80, the value of $CIRD_{KP}$ increases up to 100% which means more vulnerability of the system. The probability of success of such attack is higher if the attacker knows the helper data stored in the database of the first system and the encryption parameters on both systems. The attacker tries to generate a helper data $H_U^{'}(X_U, K_U)$ from the data of the first system $H_U^{S1}(X_U, K_U)$ and the two code words c_U^{S1} and c_U^{S2} of the two systems as given by the following equation.

$$H_U^{'}(X_U, K_U)=(H_U^{S1}(X_U, K_U) + c_U^{S1}) - c_U^{S2} = X_U - c_U^{S2} \quad (11)$$

We can conclude that the method of *Fuzzy Commitment* is vulnerable to intrusion attacks. If the attacker knows the encryption parameters and the model stored in the system (represented by *CIRS*) then the probability that he may have access to the system is of 100%.

In the case where the attacker wants to access to another system that uses the same biometric features and has the helper data of the first system and the encryption parameters of the first and second systems (represented by $CIRD_{KP}$), protection with *Fuzzy Commitment* is not guaranteed against this type of attacks. Only the intra-class variation can decrease the access probability of the attacker, but from a certain threshold the attacker can access with a probability of 100%.

The Figure 2 (b) shows the *CIRD* with *Unknown Parameters*. We note that the attacker cannot access to the system if the threshold is below 17; the rate of intrusion increases with variation according to thresholds and equal to 100% when the threshold is greater than 140.

Figure 2 (c) shows the representation of '*Cross Rate in Encrypted domain*' CR_E according to thresholds. For threshold values less than or equal to 38, the cross rate is equal to 86.36%. For other values of the threshold (above 38) the success rate of this attack is increased to 100%. In this type of attacks, the rate of vulnerability is due to the knowledge of two helper data by the attacker, which makes easy the connection in encrypted domains by just matching the different helper data. The vulnerability of *Fuzzy Commitment* according to the proposed scenario can be explained by the ease of obtaining the original model from the elements known by the attacker namely the helper data and the encryption parameters.

In '*Combination Attack*' *CA* as shown in Figure 3 (a), the attacker and the user use the same model to authenticate. The acceptance rate of the attacker may be 0% for certain thresholds such as the range of thresholds [0, 20]. The rate of access to the system by the attacker is increased with variation because he uses the same record as the user. The maximum value of the vulnerability of the system is reached in the 119 threshold for a rate of attack equal 25%.

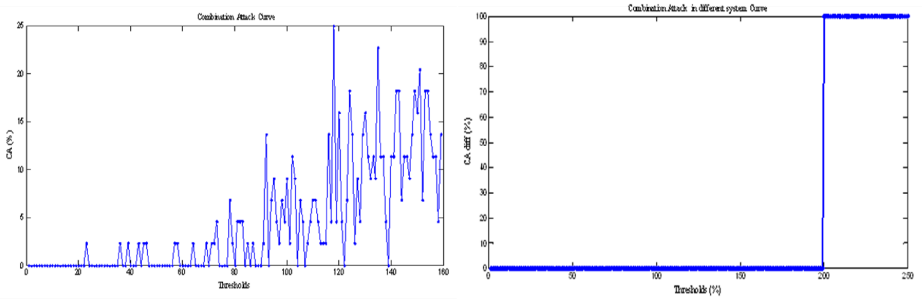

Fig. 3. *CA*, CA_{diff} curves of *Fuzzy Commitment*

In the case of '*Combination Attack in Different system*' illustrated by Figure 3(b), the attacker has a helper data generated by these biometric data and the encryption parameters of the user, then he makes a combination with the auxiliary data of the user and tries to attack a second system that uses the same biometric trait of the user. We notice that the attacker does not have access to the system for thresholds below 199, after

this threshold the value of vulnerability is increased to 100% because the attacker uses the key of the user. *Fuzzy Commitment* is more vulnerable to this attack, where several helper data generated from the same biometric trait can be adapted by the attacker to extract the original biometric model, and thus the ability of the revocation is affected.

4.3 Security Analysis Results of Fuzzy Vault Technique

After applying the proposed criteria on the method of "*Fuzzy commitment*", we analyzed the security of the second method i.e. "*Fuzzy Vault*" using same criteria.

Figure 4 shows the ROC curves before encryption ROC_{orig}, after encryption $ROC_{Unknown}$ curve and ROC_{Known} where the attacker knows the encryption parameters. We notice a less performance than the original system ROC_{orig} and degradation of performances if the attacker knows the encryption parameters. In case where the attacker does not have the encryption parameters, the possibility to be accepted is varied. If the encryption parameters are known to the attacker, the possibility of acceptance is 100% (ROC_{known}) while the acceptance in case of unknown parameters $ROC_{Unknown}$ is less than 100%. This vulnerability is due to the knowledge of the polynomial p by the attacker where the possibility of having an illegitimate access to the system of 100%.

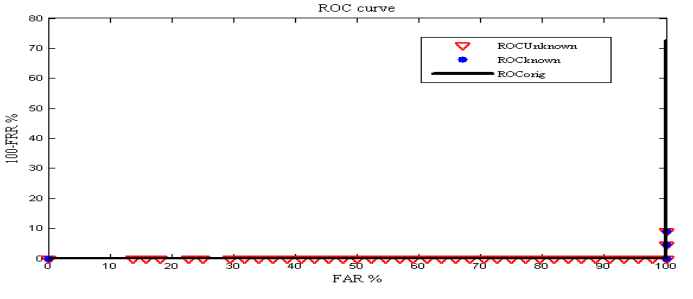

Fig. 4. ROCorig, $ROC_{Unknown}$, ROC_{known} curves of *Fuzzy Vault*

Figure 5 (a) shows the '*Cryptosystem Intrusion Rate in a Different system with Known Parametrs' CIRD*$_{KP}$. In this scenario, the system is vulnerable after the threshold 3070 because the attacker knows the polynomial *p1* and *p2* of two biometric systems and also knows the Vault *V1* stored in the first system. He has all the elements allowing to find the model X_U used to estimate the Vault *V2* of the second system and hence has an illegitimate access to the system using the Equations 12 and 13.

$$X'_U = \text{Racine}\ (V_U^{S1} - FP) = \text{Racine}\ (\text{Projection}\ (p1, X_U)) \quad (12)$$

$$V'_U{}^{S2} = \text{Projection}\ (p_2, X'_U) + FP' \quad (13)$$

The attacker is rejected by the system up to the threshold 3070 due to the intra-class variation and the false points as well.

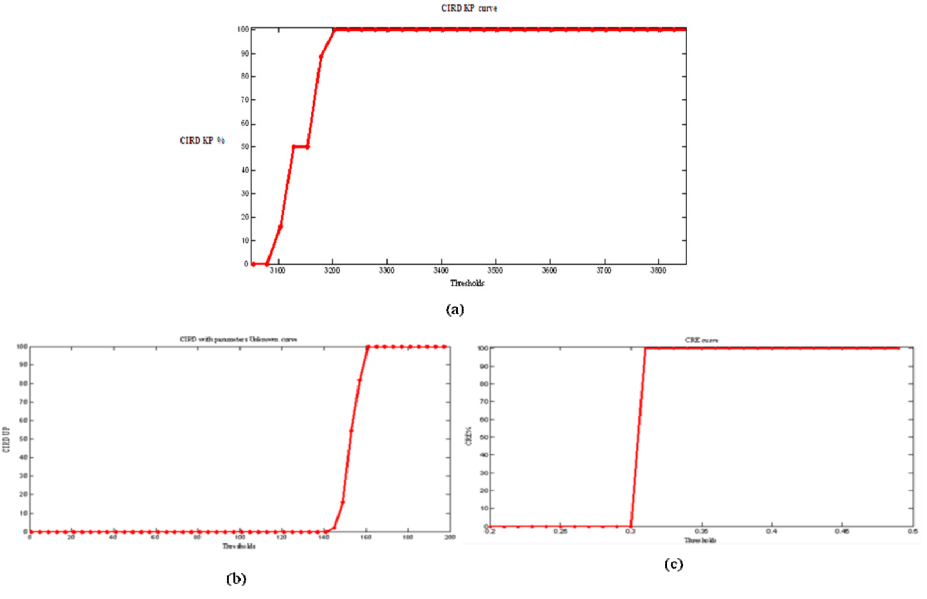

Fig. 5. *CIRDKP, $CIRD_{UP}$, CR_E* curves of *Fuzzy Vault*

Figure 5 (b) shows the '*Cryptosystem Intrusion Rate in a 'Different' system with Unknown parameters' $CIRD_{UP}$*. We note an increase in vulnerability of the system after the threshold 140. This vulnerability is due to the knowledge of two Vaults of the two systems (the first system and the second system) and the encryption parameters of the first system, the attacker tries to find the original model using known elements according to Equations 14.

$$X'_U = \text{Racine}\,(V_U^{S1} - FP'_A) = \text{Racine}\,(\text{Projection}\,(p1, X_U^{S1})) = \text{Racine}\,(V_U^{S2} - FP'_A) \qquad (14)$$

Figure 5 (c) shows the '*Cross Rate in Encrypted domain' CR_E* according to the thresholds. For threshold values less than or equal to 0.3, the attacker cannot link the two Vaults (the cross rate is 0%). This result can be explained by the false point that can make a difference between the two Vaults. For other threshold values (greater than 0.3) the success rate of this attack is increased to 100% because the attacker knows the two polynomials and also the two Vaults. Then to make the correspondence in encrypted domain, the attacker can simply match the two Vaults following thresholds higher than 0.3.

We note that the method of *Fuzzy Vault* is vulnerable to attack from a certain threshold depending on the proposed scenarios; this vulnerability is due to the possibility of obtaining the original model from the information known to the attacker i.e. encryption parameters and stored Vault in the database.

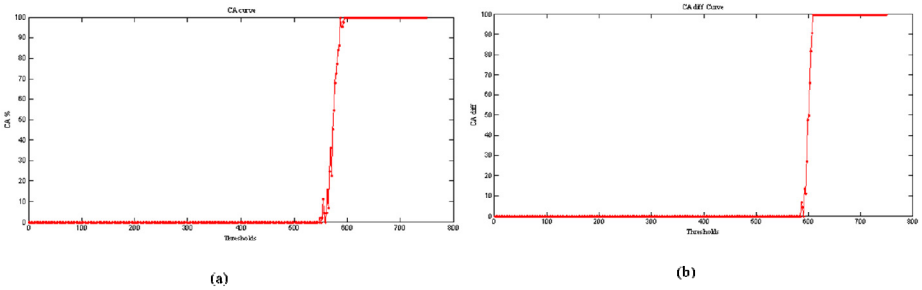

Fig. 6. *CA 'combination Attack' and* CA_{diff} *'combination Attack in different system'* curve of the *Fuzzy Vault*

In *CA* attack (Figure 6 (a)), the attacker adds his Vault V_A generated with his key K_A to the Vault of the user V_U^{S1} stored in the first system S_1 (Equation 15) which can disrupt the system after certain thresholds. We notice that the attacker can access to the system after the threshold 550 and then the value of this attack increases according to the threshold up to 100 after the threshold 600.

$$V_A^{S1} = V_A(K_A) + V_U^{S1}(K_U^{S1}) \tag{15}$$

In CA_{diff} attack (Figure 6 (b)), the attacker adds the Vault of the user V_U^{S1} to his Vault V_A generated with the key of the user K_U^{S1} to attack a second system (Equation 16). The attacker can access the system after the threshold 585. The vulnerability of the attack increases up to 100% if the threshold exceeds 600.

$$V_A^{S2} = V_A(K_U^{S1}) + V_U^{S1}(K_U^{S1}) \tag{16}$$

In combination attack, the attacker has difficulty of access to the same system as illustrated by CA curve. This difficulty can be higher in case of attack in a second system that uses the same biometric features of the user knowing the key to the first system as shown in CA_{diff}.

5 Conclusion

Biometric cryptosystems are developed to protect the biometric models; however no study is conducted in this domain for a formal security analysis. In this paper, we have proposed different measures to assess the security strength of key binding biometric cryptosystems. We applied these criteria for the protection of a biometric facial recognition system. The emphasis here was on the security analysis, which was tested on *Fuzzy Commitment* and *Fuzzy Vault* techniques showing the interest of the proposed measures. Our analysis shows that both methods are vulnerable to 'intrusion' and 'binding' attacks especially if the attacker knows the encryption parameters in intrusion attacks and the helper data along with the encryption parameters in the cross attacks. Our experiments expressed that the method of *Fuzzy Commitment* is more vulnerable to proposed scenarios than *Fuzzy Vault*. This vulnerability can be explained by the ease of obtaining the original model from the auxiliary data and the encryption parameters. The proposed criteria allow evaluating the robustness of the biometric

cryptosystems (as shown for both techniques *Fuzzy Commitment* and *Fuzzy Vault*) and also make the difference between security and usability.

The experimental field in the future will be extended to include different parameters for the protection of biometric systems. As a future work, we plan to offer other attack scenarios.

References

1. Ratha, N.K., Connell, J.H., Bolle, R.M.: An Analysis of Minutiae Matching Strength. In: Bigun, J., Smeraldi, F. (eds.) AVBPA 2001. LNCS, vol. 2091, pp. 223–228. Springer, Heidelberg (2001)
2. Nagar, A.: Secure Biometric Recognition. In: PRIP Seminar (2008)
3. Nagar, A., Nandakumar, K., Jain, A.K.: A hybrid biometric cryptosystem for securing fingerprint minutiae models. Elsevier Pattern Recognition Letters (2010)
4. Nagar, A., Nandakumar, K., Jain, A.K.: Biometric Model Transformation: A Security analysis. SPIE (2010)
5. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric Model Security. Eurasip Journal (2008)
6. Uludag, U., Pankanti, S., Prabhakar, S., Jain A.: Biometric cryptosystems: Issues and challenges, pp. 948–960. IEEE (2004)
7. Hao, F., Anderson, R., Daugman, J.: Combining crypto with biometrics effectively. IEEE Trans. Comput., 1081–1088 (2006)
8. Li, Q., Sutcu, Y., Memon, N.: Secure Sketch for Biometric Templates. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 99–113. Springer, Heidelberg (2006)
9. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, pp. 523–540. Springer (2004)
10. Juels, A., Wattenberg, M.: A Fuzzy Commitment Scheme. In: Sixth ACM Conference on Computer and Communications Security, Singapore, pp. 28–36 (1999)
11. Juels, A., Sudan, M.: A Fuzzy Vault Scheme. In: IEEE International Symposium on Information Theory, Lausanne, Switzerland (2002)
12. Adair, K.L., Parthasaradhi, S.T.V., Kennedy., J.: Real World Evaluation: Avoiding Pitfalls of Fingerprint System Deployments. BiometricsIndia Expo. (2008)
13. Gu, S., Tan, Y., He, X.: Laplacian Smoothing Transform for Face Recognition, pp. 2415–2428. Springer (2010)
14. Khan, A., Farooq, H.: Principal Component Analysis-Linear Discriminant Analysis Feature Extractor for Pattern Recognition. International Journal of Computer Science Issues (IJCSI) 8(6) (2011)
15. Moujahdi, C., Ghouzali, S., Mikram, M., Abdul, W., Rziza, M.: Inter-communication classification for Multi-view Face Recognition. In: The 4th International Conference on Multimedia Computing and Systems (ICMCS), Tangier, Morocco (2012)
16. Gu, S., Tan, Y., He, X.: Discriminant Analysis via Support Vectors. Neurocomputing (2010)
17. Bellhumer, P.N., Hespanha, J., Kriegman, D.: Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Trans. Patt. Anal. and Mach. Intel. Special Issue on Face Recognition, 711–720 (1997)
18. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North Holland (1977)
19. Schneider, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edn. Wiley, New York (1996)
20. Fawcet, T.: ROC Graphs: Notes and Practical Considerations for Researchers. HP Laboratories, 1143–1501 (2004)