Cracking Biometric Authentication Cryptosystems

Maryam Lafkih[1,2]
[1]SmartiLab, National School of Engineering Sciences, Rabat, Morocco
[2]LRIT (Associated Unit with the CNRST), Faculty of Sciences, Mohammed V University, Rabat, Morocco

Keywords: Biometric Cryptosystems, Security Evaluation, Framework Conception, Attacks.

Abstract: Biometric systems are becoming an alternative solution to replace traditional authentication systems. However, security and privacy concerns against these systems arise from the direct storage and the misuse of biometric information. In order to overcome these problems, biometric cryptosystems are proposed as template protection solution improving the confidentiality and the security. Biometric cryptosystems present a secret key mechanism where a secret key is used to overlap biometric data. Several approaches using biometric cryptosystems have been proposed, however a few works have been published giving detailed analysis of these systems and their security. In this paper we give a rigorous discussion on biometric cryptosystems taking into account their security evaluation. Besides, a conception framework of different attacks on biometric cryptosystems is proposed. On the other hand, several measures that can be exploited to decrease the probability of such type of attacks are also presented.

1 INTRODUCTION

The use of biometric systems is becoming a necessity in the world, these systems are proposed to hamper the problems of traditional authentication systems. Biometrics ensures the user's identification and reduces the theft and menaces. However, biometric system can be attacked using different threats such as correlation of stored templates and spoofing attacks. In order to overcome these weaknesses, the cryptography domain is investigated to protect different information and data. Then, Biometric cryptosystems are proposed as biometric data protection technologies. As basic biometric systems, biometric cryptosystems are based on both steps to ensure the authentication process. In the first step, a secret key is used to generate the intermediated data referred to as helper data. This data must not reveal significant information about the user's information. The second step is the enrollment process where the secret keys must be derived using the helper data and the user's request. Based on how the helper data are derived, biometric cryptosystems are categorized on two kinds: the key binding and the key generation biometric cryptosystems (A. K. Jain et al,1999).

1) Key Binding Systems: this type aim to binding a random secret key with biometric data to generate the helper data in the enrollment step. During authentication processes, the Key is obtained from the helper data and the biometric request (C. Soutar et al, 1998). *Fuzzy Vault* (K. Nandakumar et al, 2007) and *Fuzzy Commitment* (A. Juels and M. Wattenberg, 1999) are examples of these systems. This mode is considered as more tolerant to biometric variations due to the use of error correcting code in order to generate the secret key (Figure 1).

2) Key Generation: In this mode, helper data are generated only from biometric data. Biometric template can be recovered from the helper data and the given biometric request (Yongjin Wang et al, 2007). *Fuzzy extractors* and *secure sketches* are considered famous formalisms of these systems (C. Soutar, 1998) (Figure 2).

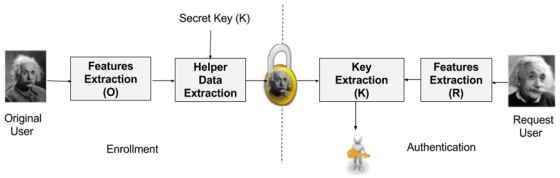

Figure 1: Key Binding process.

Although the proposed modes are considered to secure the biometric information, biometric cryptosystems still suffer from several security and privacy concerns; where several attacks can be performed on different system level. In this paper, we explored different proposed approaches of biometric cryptosystems in both binding and generation mode.

Lafkih, M.
Cracking Biometric Authentication Cryptosystems.
DOI: 10.5220/0009169405140522
In *Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2020) - Volume 4: VISAPP*, pages 514-522
ISBN: 978-989-758-402-2; ISSN: 2184-4321

Hybrid approaches which make the fusion of different basic concepts have been also presented. The comparison of proposed approaches is presented accompanying to the rigorous analysis of the weakness and powerful points. The evaluation of the security and privacy is also discussed where a conception framework of different attacks is proposed to summarize different attacks possible in biometric cryptosystems. In this paper, we present a general Attack conception framework, this framework regroup different type of attack that can affect any biometric cryptosystems. Classification of existing security evaluation is firstly proposed and the overall possible attacks are then discussed in order to present detailed security evaluation. New types of attacks are also proposed in this framework. The goal of this framework is to let researchers to easily evaluate their systems in a quantitative manner, to enhance the presented database of common threats. Since researchers may overestimate the efficiency of their developed systems.

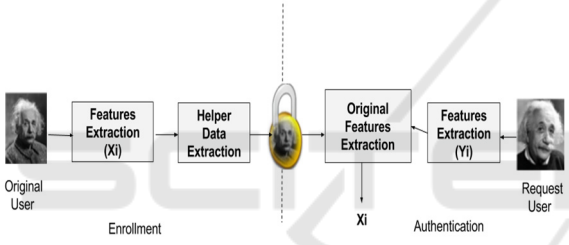

Figure 2: Key generation process.

The rest of this paper is organized as follows: Section 2 provides security evaluation of biometric systems without protection. Different existing security evaluation of biometric cryptosystems is discussed in Section3. In Section 4, the proposed conception framework is proposed to detail different points of threads in biometric cryptosystems. Discussion of possible solution is also presented in Section 5. Finally, Section 6 concludes the paper and a number of future works.

2 BIOMETIC CRYPTOSYSTEMS

Security has become increasingly a concern in biometric systems, it ensure confidentiality by providing a robust authentication process against any type of threats (Ross, A., Jain, A., 2003). For this purpose biometric cryptosystems are proposed as cryptography based technology to minimize the vulnerabilities exploited illegitimately to gain access to a system (Ratha, N. et 2001). 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 (Ross, A., Jain, A. 2003). 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* (Li, Q et al, 2006). In Key binding cryptosystem, biometric template is linked with a secret key in a single entity to build a helper data. This data reveals 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. Fuzzy Commitment method, proposed by Juels and Wattenberg (Juels, A., Wattenberg, M., 1999) 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. During the authentication, the secret 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).

To address the weakness of the Fuzzy Commitment, another main approach is proposed by Juels and Sudan named Fuzzy Vault (Juels, A., Sudan, M, 2006). 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 (Scheirer, W. J., Boult, T. E., 2007), 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 fX_1; X_2;..; Xrg, a random key K is generated of length l, and converted into polynomial P of degree d. Using this polynomial we obtain the set f(Xi; P(X_i))gri=1 that is secured by hiding a set of random chaff points (aj ; bj)j=1 q where b_j 6= P(a_j) and aj 6= Xi. 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 n. Fuzzy Vault approach was presented as solution for protecting biometric template and preserving privacy, however the security of several existing Fuzzy Vault schemes cannot 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. Ratha et al. [7] have identified eight locations of possible attacks in a generic biometric system. In the case of biometric cryptosystems, other kinds of attack can be appeared. Even if different studies discuss the biometric cryptosystems security, this assessment does not follow a formal framework, hence to this end, we aim to propose a conception framework in order to generalize the possible attacks on biometric cryptosystems. This framework is independent to the used modalities and the used protection approach.

3 BIOMETRIC CRYPTOSYSTEMS EVALUATION

Biometric crypto-systems evaluation is considered as a major issue for several reasons. It offers researchers and developers a tool to better test and evaluates these systems taking into account the user's behavior. Furthermore, Evaluation and security analysis allows understanding the needs and deploying this technology with efficiency manner. On the other hand, the biometric cryptosystems analysis allows the identification of industrial applications base on various criteria as the performance, usage, security and deployment cost. Despite the obvious advantages of biometric cryptosystems, they are still vulnerable to several kinds of attacks which may deeply affect their utility and functionality. In order to improve the security of biometric cryptosystems, the evaluation of their security presents a necessity. Therefore, it is important that biometric cryptosystems be designed to withstand the presented threats when employed in security-critical applications and to achieve an end to end security. Towards this goal, the aim of this work is to present a general framework towards the security threats of biometric authentication cryptosystems. The goal of this framework is to regroup all the possible threats on biometric cryptosystems. These threats are classified on already discussed threats and other new threats which are not yet studied. On the other hand, this framework let researchers to easily evaluate their systems in a formal manner, and to enhance the presented evaluation of common threats and vulnerabilities.

3.1 Classification of Existing Evaluation

Security evaluation of biometric cryptosystems has been discussed in several studies. In order to classify the possible threats we first categorize existing evaluation literature work on four categories: (1) Classical evaluation, (2) Evaluation based on Information theory, (3) Secret key evaluation, (4) Evaluation using attacks.

3.1.1 Evaluation based on Information Theory

Xuebing (Xuebing Zhou, 2011) propose a framework in order to analyze the security of protection approaches using mutual information and entropy. Zhou et al. are studied the security of fuzzy commitment using 3D

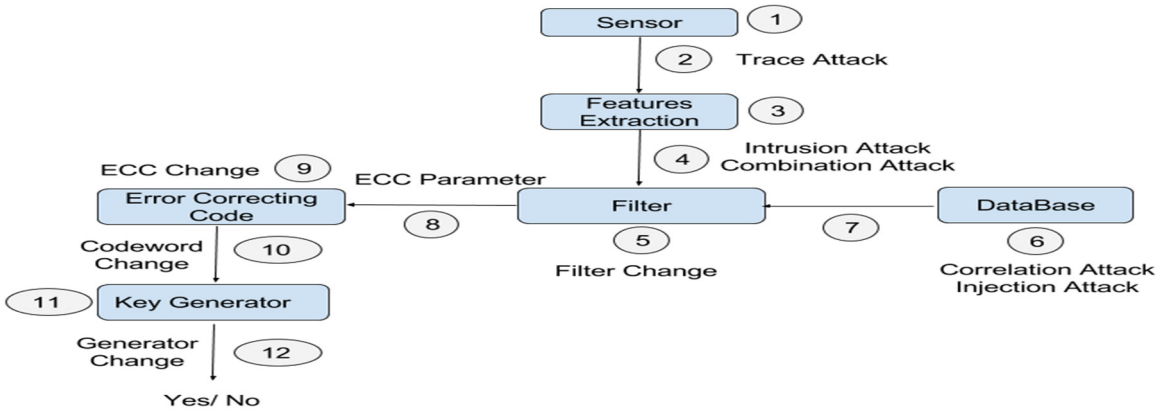

Figure 3: Biometric Cryptosystems attacks Framework.

face recognition system based on the mutual information. Authors are studied the security and the privacy using entropy in order to evaluate the independence and biometric features distribution. The distribution of the iris codes and Markov proprieties are then generated. Besides, the security of fuzzy commitment is measured by Nagar (Abhishek Nagar,2012) using the entropy taking into account the biometric features distribution and the probability to steal the auxiliary data. Wang et al. (Ye Wang, 2011) are proposed a comparative study using both approach secure helper data and fuzzy commitment. This analysis is based on the information theory and False Acceptance and False Rejection Rates (FAR, FRR). The Quatratic Reny Entropy is used by Hidano et al.(Seira Hidano, 2012) to estimate the quantity of information in fingerprints features. Meenakshi and Padmavathi (VS Meenakshi, 2009) have proposed a new Fuzzy Vault approach and analyze the security using minimal entropy. Al-Assam and Jassim (Hisham Al-Assam, 2012)] are combined the Kullback-Leibler divergence and the entropy in order to create a new entropy formula.

3.1.2 Secret Key Evaluation

Biometric cryptosystems link a secret key to biometric features. This key must have a sufficient size and entropy. On the other hand, biometric cryptosystems performance can be presented using the FAR and FRR, these measures are linked to the key entropy. For these reasons, a new relation between the secret key and FAR / FRR is performed by Andry et al. (Andy Adler,2003). Hence, an ideal biometric cryptosystem must have FAR<2k, which is not possible in practice. Kelkboom et al. (Emile JC Kelkboom, 2010) have also proposed a new measure based on the relation between the key and FAR/FRR to measure the security of fuzzy commitment. The security of this scheme is also discussed by Ignatenko et Willems (Tanya Ignatenko, 2012), based on linked information and the key's maximum size.

3.1.3 Evaluation using Attacks

In (Christian Rathgeb, 2012), Rathgeb and Uhl are applied statistic attack on iris Fuzzy Commitment; this attack is based on the execution of error correcting code in decoding mode in order to generate the near codeword (A Stoianov,2009). This allows correcting several errors which decrease the FRR and Increase the FAR. The brute force attack is related to the hardness to recover the polynomial from the vault, and the probability that t vault points are in the genuine features is $\binom{k}{t}\binom{n}{t}^{-1}$. This attack is discussed also in (Preda Mihailescu, 2007). Tams (Benjamin Tams, 2013) have studied the impact of false acceptation attack which is easier than brute force attack because it depends directly to the average rate necessary to execute attacker's request. In Correlation attacks, the attacker has two vaults of the same user stored in different systems and tries to link the both data. The aim of this attack is to derive the biometric trait of the real user. These attacks are particularly investigated on the fuzzy vault context in (Soweon Yoon, 2012). In (Emile JC Kelkboom, 2010), Kelkboom et al have tested a correlation attack using fingerprint. This attack consists to define the real biometric from biometric models stored in different systems using exhaustive research. Chang et al. (T Charles Clancy, 2003) have identified the location of chaff points; this was proved by the observation of non-randomness of fuzzy vaults (i.e, free zone in the vault). Scheirer et al. (Walter J Scheirer, 2009) have proposed theoretical analysis of Fuzzy Vault and biometric encryption Scheme against several attacks without any criterion and any

implementation to represent these attacks (T Charles Clancy, 2003). Authors are proposed injection attack where the attacker can inject his biometric data in the database; On the other hand, correlation attack is also discussed. Poon and Miri (Hoi Ting Poona, 2009) are proposed the collision attack against fuzzy vault, where the attacker has different encoded values using a secret key. This attack can be applied to distinguish the genuine points in the vault.

3.2 Proposed Conception Framework

In order to compare different biometric cryptosystems in term of the usability, performance, security, the security analysis presents a necessity. To evaluate the security of biometric cryptosystems with rigorous and detailed manner, we propose a generalized conception to schematize different possible threats on biometric cryptosystems. Ratha et al. (Ratha, N, 2001) have identified eight points or levels of attack in biometric authentication systems, however, biometric cryptosystem are vulnerable to the several threats. These threats (ex. filtrate attacks, error correcting attacks) are not possible in biometric systems without protection mechanism. To this effect, we propose a generalized scheme which regroups different threats that biometric cryptosystems may consider. This scheme (Figure 3) presents overall proposed attack studied and discussed on literature and also other that no yet proposed.

3.2.1 Sensor Attack

Biometric data are captured using the sensor which scans the biometric trait to convert it into digital form. After converting it to digital form, the data is transmitted to feature extraction module. The sensor module is vulnerable to the “Attack at the sensor”. In this attack (Figure 4), an attacker presents a fake biometric trait such as an artificial finger or facial image to the sensor in order to bypass recognition systems. An attacker can also physically damage the recognition system and flood the system with bogus access requests. Sensors are unable to distinguish between fake and real characteristics of an individual and can be fooled easily by using synthetic fingerprints or facial image of a person.

The most common attack is the one against the sensor. When the samples acquisition process is fully automated (e.g. no watching guard exists to monitor the acquisition process) an impostor can easily bypass the system by simply presenting a copy of biometric data of a legitimate user in front of the sensor. The attempt of breaking the biometric system using such method is named spoofing attack. To date, there is no commercial biometric technology that is robust against such attacks. The copy may come in various formats, depending on the biometric modality. In the case of facial biometric, the impostor may present a still image, video sequence playback, or even a 3D silica or rubber mask of the genuine user. A demonstration carried out 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 (Ton Van der Putte , 2000).

Figure 4: Examples of Sensor Attacks.

Figure 5: Examples of Alteration Attacks.

In the case of fingerprints, authors did the falsification 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.(Tsutomu Matsumoto, 2002) have tested fingerprint falsified with the help of real users in 11 biometric systems, their results show’s 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 (Figure 5).

3.2.2 Trace Attack

Despite active research in recent years in the evaluation of biometric-based applications, very few studies have focused on the effect of alteration on the security and robustness of these systems. Alteration of fingerprints has been used to hide the identity of the impostor and gain unauthorized access to the biometric system. This alteration is classified into three categories: obliteration, distortion, and imitation. In the case of facial authentication, the alteration is applied on the face via plastic surgery or prosthetic make-up. With advances in technology, a hacker was able to clone a politician's fingerprint using pictures taken at different angles with a standard photo camera. In this paper, we present other types of alterations that can be applied on different biometric authentication systems, especially biometric mobile applications. This attack can be applied using different modalities, making it dangerous not only in the case of mobile applications based on fingerprint or facial authentication but also in iris- and voice-based Mobile Information Systems (Figure 6).

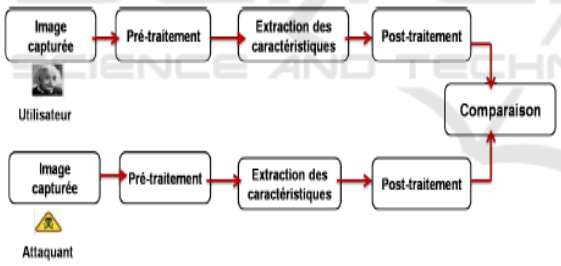

Figure 6: Illustration of Trace Attack.

3.2.3 Features Extraction Attack

During the features extraction attack, the attacker can modify the extracted features; the attacker replaces other characteristics by synthetic data (By pass matcher Attack) on the channel. He could steal biometric characteristics of the real user and submits 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 Martinez who proposed a hill-climbing attack (Martinez-Diaz 2006) 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 (Adler, A, 2003) 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 matcher. The procedure is completed if there is no improvement in score.

3.2.4 Intrusion Attack

In this attack we suppose that the attacker has the secret key $K^{S1}{}_U$ and the user's helper data U enrolled in the first systems S1, $H^{S1}{}_U$ (U; $K^{S1}{}_U$)), then, the attacker uses this information in order to estimate user's data in the second system S2 (when the same user's is enrolled), the estimated data is then presented to the system S2 as request in order to gain illegitimate access (Figure 7).

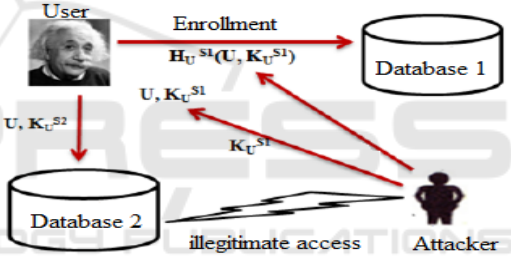

Figure 7: Example of intrusion attack.

3.2.5 Correlation Attack

In this type of threats (Figure 8), the attacker try to link several helper data His U ($X^{Si}{}_U$;$K^{Si}{}_U$) when 1<i<n of the same user enrolled in different systems in order to derive the original model Xu or the secret key $K^{Si}{}_U$

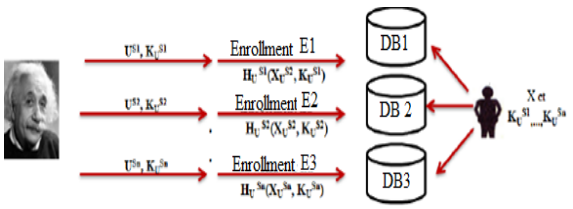

Figure 8: Example of Correlation attack.

3.2.6 Injection Attack

This attack aims to inject attackers biometric data in the database (where the helper data $H(U;K_U)$ of the

real user U is stored in order to gain access to the system (Figure 9).

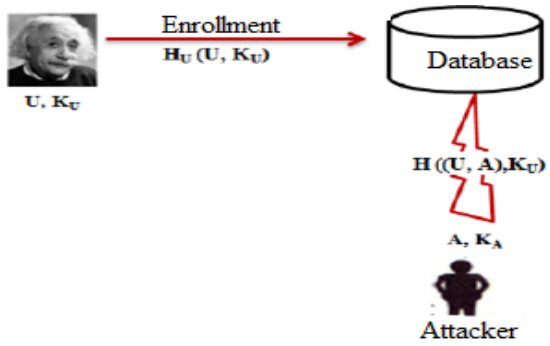

Figure 9: Illustration of injection attack.

3.2.7 Combination Attack

The attacker has a part of user's biometric features U and try to create a complete request in order to gain access to the system using the combination of some data with the user's stolen part (U, A) (Figure 10).

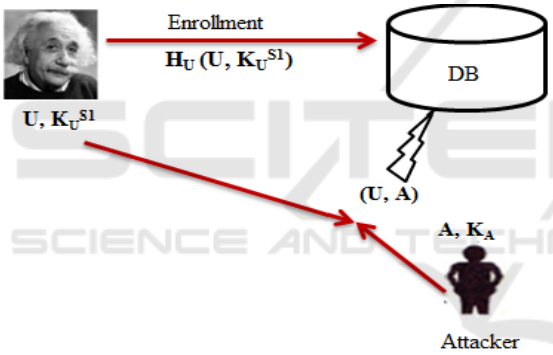

Figure 10: Illustration of combination attack.

3.2.8 Filter Change Attack

In this attack (Figure 11), the attacker based on the following observation, where the attacker uses the helper data value to estimate the extracted features which will be injected as user's request. For example, in Biometric cryptosystems based fuzzy vault scheme, the attacker can detect the small free area in the generated chaff point. Given the sketch PX of the original X where |X| = s, the goal of an attacker is to find X. The attacker can query a blackbox. On input of a set Q of s points, the blackbox will return YES if Q = X. The effectiveness of an attacker is measured by the number of queries he sent. The blackbox is the decryption of the file using the key Q. The output of YES corresponds to the situation where the file is successfully decrypted.

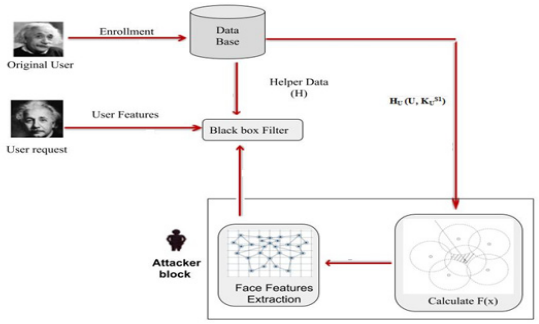

Figure 11: Filter change attack.

3.2.9 Error Correcting Parameter Attack

Instead of changing the error correcting module, the attacker can change the error correcting parameters in order to have high error correction capacity. For example, we suppose that the system use RS(n, k) where the coder uses the k symbol and added n control symbol, resulting n-k , the RS can correct then t symbol where 2t = nk.

3.2.10 Error Correcting Attack

Error correcting codes aim to cope with biometric feature's variations in biometric data. For these reasons, Linear codes such as BCH, Reed Solom, are used in the literature. However, these linear codes are inflexible. Using these kinds of block codes requires binary biometric vector having the same size of the employed codeword, where some bits have to be isolated, or a bits-padding has to be performed. On the other hand, even if biometric cryptosystems are provable secure in information theoretic sense, they are indeed vulnerable to several dreadful security and privacy attacks in practice. For example, the attacker can change the error correcting module using error correcting code with high error correction capacity.

3.2.11 Code Word Generation Attack

Attack based on error correction code histograms was introduced in (Florence Jessie,1977). This attack aims to run error correction in decoding mode which returns always the nearest codeword. The attacker is supposed in knowledge of applied error correction. The decoder can correct more errors decreasing the false rejection rate and increasing the false accept rate is increased. Figure 14 explain the attack's operation mode. The binary biometric features are chosen by the attacker and successive decommitment is applied for each chunk in decoding mode. Based on counting the number of possible codewords, the histogram is

stored and analyzed during the verification process resulting the most likely codeword.

3.2.12 Key Generation Attack

In this attack the attacker can inject a generated series as secret key so that he can gain access to the systems. The key generation module can be also changed by the attacker using another one that makes the illegitimate access easier.

4 CONCLUSIONS

Biometric cryptosystems are proposed as secure technologies for protecting biometric template. However, these systems stay vulnerable to several attacks. Despite active research in recent years in the evaluation of biometric cryptosystems, very few studies have focused on the security and robustness of these systems. Most of proposed biometric cryptosystems evaluation studies are based on information theory such as entropy, mutual information etc, these measures are difficult to be estimated when the distribution of biometric features is unknown (do the intra-class and inter-class variability). On other hand, many studies consider the false acceptance rate FAR to evaluate the security when this criterion is considered as performance measure and can't be sufficient to measure the security. Consequently, the proposed studies to analyze the security of biometric cryptosystems are very limited. In order to present a generalized study to evaluate the security of biometric cryptosystems, we proposed in this work a generalized conception framework. This framework takes in into account all the modules threats.

REFERENCES

A. K. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identification in Networked Society. Norwell, MA: Kluwer, 1999.

C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. V. K. Vijaya Kumar, "Biometric encryption using image processing," in Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, 1998, pp. 178–188.

K. Nandakumar, A. Nagar, and A. K Jain. Hardening fingerprint fuzzy vault using password. In Advances in biometrics, pages 927-937.Springer, 2007.

Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security, pages 28-36. ACM, 1999.

Yongjin Wang and KN Plataniotis. Fuzzy vault for face based cryptographic key generation. In Biometrics Symposium, pages 1-6. IEEE, 2007.

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

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.

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

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

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

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

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

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

Xuebing Zhou, Arjan Kuijper, Raymond Veldhuis, and Christoph Busch. Quantifying privacy and security of biometric fuzzy commitment. In International Joint Conference on Biometrics (IJCB), pages 1-8. IEEE, 2011.

Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Multibiometric cryptosystems based on feature-level fusion. IEEE Transactions on Information Forensics and Security, 7(1) :255-268, 2012.

Ye Wang, Shantanu Rane, Stark C Draper, and Prakash Ishwar. An information-theoretic analysis of revocability and reusability in secure biometrics. In Information Theory and Applications Workshop (ITA), pages 1-10. IEEE, 2011. (Cité en pages 45 et 50.)

Seira Hidano, Tetsushi Ohki, and Kenta Takahashi. Evaluation of security for biometric guessing attacks in biometric cryptosystem using fuzzy commitment scheme. In BIOSIG-Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), pages 1-6. IEEE, 2012.

VS Meenakshi and G Padmavathi. Security analysis of password hardened multimodal biometric fuzzy vault. World Acad. Sci. Eng. Tech, 56 :312-320,2009.

Hisham Al-Assam and Sabah Jassim. Security evaluation of biometric keys.computers & security, 31(2) :151-163, 2012.

Andy Adler. Sample images can be independently restored from face recognition templates. In CCECE Canadian Conference on Electrical and Computer Engineering, volume 2, pages 1163-1166. IEEE, 2003

Emile JC Kelkboom, Jeroen Breebaart, Ileana Buhan, and Raymond NJ Veldhuis. Analytical template protection performance and maximum key size given a gaussian-modeled biometric source. In SPIE Defense, Security, and Sensing, pages 76670D-76670D. International Society for Optics and Photonics, 2010.

Tanya Ignatenko and Frans MJ Willems. Information leakage in fuzzy commitment schemes. IEEE Transactions on Information Forensics and Security, 5(2) :337-348, 2010. (Cité en page 46.)

Christian Rathgeb and Andreas Uhl. Statistical attack against fuzzy commitment scheme. IET biometrics, 1(2) :94104, 2012. (Cité en pages 46 et 52.)

A Stoianov, T Kevenaar, and M Van der Veen. Security issues of biometric encryption. In Toronto International Conferenceon Science and Technology for Humanity (TIC-STH), pages 3439. IEEE, 2009.

Preda Mihailescu. The fuzzy vault for fingerprints is vulnerable to brute force attack. arXiv preprint arXiv :0708.2974, 2007.

Benjamin Tams. Attacks and countermeasures in fingerprint based biometric cryptosystems. arXiv preprint arXiv :1304.7386, 2013

Soweon Yoon, Jianjiang Feng, and Anil K Jain. Altered fingerprints : Analysis and detection. IEEE Transactions on Pattern Analysis and MachineIntelligence, 34(3) :451- 464, 2012.

T Charles Clancy, Negar Kiyavash, and Dennis J Lin. Secure smartcard based fingerprint authentication. In Proceedings of the ACM SIGMM workshop on Biometrics methods and applications, pages 45-52. ACM, 2003

Walter J Scheirer and Terrance E Boult. Cracking fuzzy vaults and biometric encryption. In Biometrics Symposium, pages 1-6. IEEE, 2007

Hoi Ting Poona and Ali Miria. A collusion attack on the fuzzy vault scheme. The ISC Int'l Journal of Information Security. Bd, 1(1), 2009.

Ton Van der Putte and Jeroen Keuning. Biometrical fingerprint recognition : don't get your fingers burned. In Smart Card Research and Advanced Applications, pages 289-303. Springer, 2000 .

Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial gummy fingers on fingerprint systems. In Electronic Imaging, pages 275-289. International Society for Optics and Photonics, 2002.

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

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

Florence Jessie MacWilliams and Neil James Alexander Sloane. The theory of error correcting codes, volume 16. Elsevier,1977.