# Protecting Biometric-based Authentication Systems against Indirect Attacks

Hossein Malekinezhad, Hossein Ebrahimpour-Komleh
*Islamic Azad University Naragh Branch, University of Kashan*

## Abstract

*Biometric systems have many advantages but there are some vulnerability points that reduce security and user's privacy of biometric authentication systems. One of the important vulnerabilities in biometric systems is the escape of biometric template information. The biometric template protection techniques that are presented until now, have failed to provide all requirements of practical biometric authentication systems. In this Paper, we analyze vulnerabilities of biometric systems and review the biometric template protection approaches. Finally we present a method for biometric template protection based on fractal coding. The experiment results indicate the increasing in robustness of biometric system against attacks to biometric template database. Fingerprint templates protecting is a difficult problem due to many variations such as rotation, partial prints, etc. In spite of mentioned problems, proposed method has acceptable performance in fingerprint template protection.*

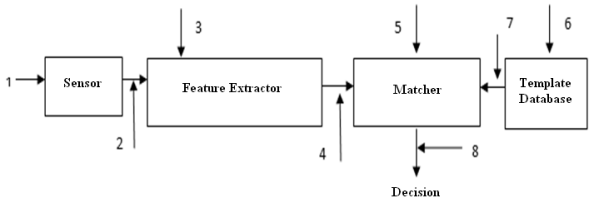
## 1. Introduction

In spite of the advantages of biometrics-based authentication systems compared to traditional authentication schemes, there are still unresolved problems associated with the earlier. These problems generally appear from the security characteristics of the biometrics-based systems. There is no an exact definition for biometric systems security. The term security refers to authentication accuracy and also may refers to the total reliability of the systems. This is true that any increase in authentication accuracy can increase the security of the system but there are other issues must be considered for a practical biometric authentication system [1].

Due to nature of the data they need to operation, the number and complexity of the applied components and the overall architectural design, biometric systems are more complicated than others authentication systems and have more critical points are be able to compromised. Fig.1 Shows the Biometric systems vulnerability points. We can divide potential attacks in biometric based authentication systems into two main groups, direct attacks, point 1, and indirect attacks other points in fig.1.

Fig.1: Locations of possible attacks in a biometric system

In direct attacks, the attacker doesn't need to




know anything about internal system operations and this type of attacks just happen at sensor level by generating an artificial biometric sample. Direct attack happens in the analog domain, thus, digital protection techniques like digital signature and watermarking couldn't be used.

There is three way for indirect attack to biometric systems. In first, the attacker uses of a Trojan horse program in feature extractor or matcher components (points 3 and 5 in fig.1). In second way, the attacker uses of communication channel vulnerabilities to manipulate information (points 2, 4, 7 and 8 in fig.1). In last way, the attacker compromises biometric system database by adding, changing or deleting biometric templates (point 6 in fig.1).

The attack to biometric template database is very dangerous because could be lead to many security and privacy problems. For example an intruder is able to replace the template of a legal user or the stolen template could be replayed to the matcher to gain unauthorized access to system. In this paper we have focused on the biometric template protection and a method for protecting biometric system against this attack is presented. The rest of this paper is organized as follows. Section 2 reviews the techniques for biometric template protection. Fractal coding basics describe in section 3. Our approach is detailed in section 4. Experimental results are discussed in section 5 and finally section 6 concludes this paper.

## 2. Biometric Template Protection Schemes

In a perfect template protection scheme there are three important properties [2]. The first one is that secure template must be Non-invertible. This means illegal users couldn't generate original template from secure stored template in system database. The second important property is renewability or Cancelability. This means the biometric template protection scheme must be able to generates multiple secure templates from the same original biometric data and cancels previous template of that biometric data if it is in danger. The last important property is authentication accuracy. An effective biometric template protection scheme must not decrease the matching performance of the biometric system. There is a tradeoff between matching performance and the security degree of biometric template protection schemes. We can divide biometric template protection methods have been proposed in literatures into two main groups: Biometric cryptosystems and Cancelable biometrics or Template transformation.

### 2.1 Biometric cryptosystems

The basic of biometric cryptosystems is binding a digital key to a biometric template or generating a key from a biometric template [3]. In enrollment phase of a biometric cryptosystem the public information, called helper data, is derived from the biometric template and stored in system database. This is computationally very complicated to reconstruct the original template from the helper data. In Authentication phase of a biometric cryptosystem if the input biometric template is sufficient close to original biometric template, the original template recovering by decoding the helper data. We can divide biometric cryptosystems into main groups: key binding and key generation approaches.

Key-binding: In enrollment phase a digital secret key binds to a biometric template and combinations of them stores in the system database as helper data [4]. In recognition phase a key retrieval algorithm applied to input template and helper data to extract the secret key. Fig 2, Shows the mechanism of this method. Whenever an adversary behaviour take places on the system database the helper data removes and a new helper data using a new secret key and biometric template generates.

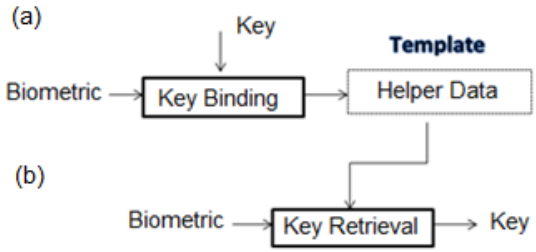



Fig.2: Basic structure of biometric key-binding. a) enrollment, b) authentication.

Examples of key-binding methods are fuzzy commitment [5] and fuzzy vault [6] schemes.

Key-generation: In enrollment phase helper data extracts from biometric template and the secret key generates from the helper data and biometric template [4]. In recognition phase the stored helper data and input biometric template used to generate the secret key. Fig 3, Shows the mechanism of this method. Examples of key-generation methods are private template approach [7] and quantization schemes [8].

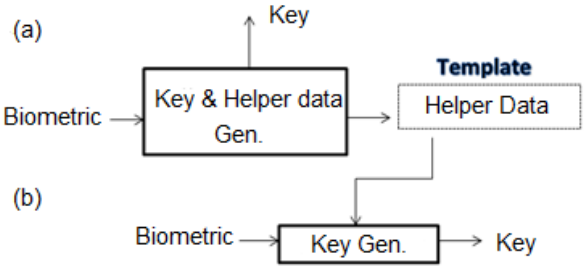



Fig.3: Basic structure of biometric key generation. a) enrollment, b) authentication.

There are some other methods that we couldn't take them to account as biometric cryptosystems but they use of secret key and biometric template for enhancing the security of biometric authentication systems. These types of approaches called key release schemes [4].

### 2.2 Template transformation

The basic of Template transformation is applying a transform function on biometric data in a way that reconstructing original biometric data from transformed biometric is computationally so hard [3]. The transformation could be done on raw biometric such as face image and also on biometric features such as face features. In enrollment phase the biometric template transforms to transformed template using user specific parameters for transformation. The transformed template stores in system database along with user specific parameters. In recognition phase the transformation with same user specific parameters occurs on input biometric template and resulting transformed template compares with stored transformed template. A perfect transformation shouldn't be reduced the biometric characteristics and also should be robust again intra-class variations. For enhancing the security of this method should be used of different transformations for different

applications. Based on the type of transform function applying in this method there are two main groups of template transformation [3]: Non-invertible transformation and Biometric salting.

Non-invertible transformation: In this method usually a one-way function applying on biometric data. To renew a biometric template the parameters of function must be changed. In cases the parameters of transformation are compromised the attacker is not able to reconstruct the original biometric template [9]. Because of intra-class variations the transformation needs to align biometric template to perform an effective comparison and this causes to reduce the authentication performance [10].

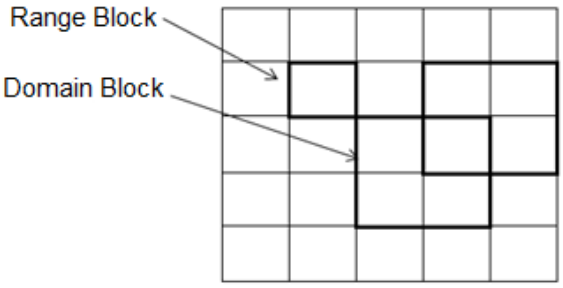
Biometric salting: The transformation function used in this method is usually an invertible function [11]. Therefore this is very important that the parameters of transformation are kept secret. Otherwise the attacker is able to reconstruct the original biometric template from the transformed template. The authentication performance of this method in comparison with non-invertible transformation method is higher but has the lower accuracy.

There are some methods that use of combination of two basic above method that we called them hybrid approaches. Examples of hybrid methods are presented in [12, 13]. The mentioned template protection methods have their pros and cons in relation to degree of security, performance, storage requirements and ability to apply on various types of biometric data. One of the main limitations of mentioned methods is the issue of alignment that reduces the recognition performance. In next sections we introduce a method for template protection based on fractal coding that is a type of template transformation methods along with some changes and has many advantages in relation to alignment and applicability to different types of biometric data.

## 3. Basics of Fractal Image Coding

Fractals are self-similar objects that are similar under various geometrical scales and could be described by a set of transformations [14]. This definition could be used for objects that aren't inherently fractal. Each object has some parts that there is some degree of self-similarity within them. This idea is true about images and fractal image coding exploits non-linear transformations that approximate a given image. Therefore the fractal code is a set of non-linear transformations that approximating a given image. Fractal codes are very smaller than the original image and many algorithms have been proposed to use these codes for image compression. Because of self-similarity in transformations, fractal image coding could be applied for recognition. In fractal image coding a given image divides to non-overlapping blocks that called rang blocks and also partitioned to larger blocks that called domain blocks. Domain blocks could be overlapped. Fig.4 shows an example of partitioning an image to range and domain blocks.

Fig.4: Examples of image partitioning to range and domain blocks




The encoder searches for the best domain block that matches with each range block. An example of matching process illustrated in fig 5.

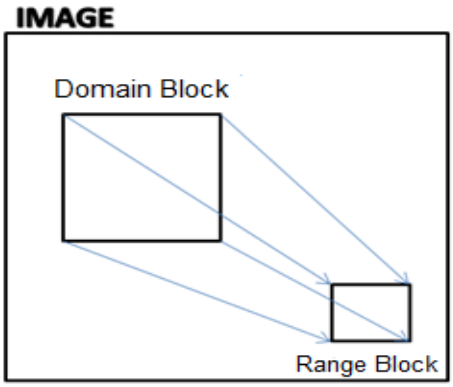



Fig.5: Example of mapping domain blocks to range blocks

In the implementation of fractal image coding we consider the following assumptions: The square blocks of size 4 by 4 pixels as range blocks. The square overlapping blocks of size 8 by 8 pixels as domain blocks. In order to mapping domain blocks to range blocks more accurately, the geometric transformations such as rotation and reflection are applied.

## 4. Recognition Using Fractal Image Coding

In proposed method a database of fractal codes of user's biometric image has been created. The fractal codes of known users decode on query image and the distance between query image before and after one iteration decoding calculates using Euclidean distance measure for each code. The identity of fractal code that minimizes this distance is taken as the recognition result. The reason is

when the fractal code of an initial image X decodes on another image such as Y, the image Y converges to initial image X after several iterations. When image Y is close to image X the number of iterations is fewer and distance between images Y before and after the decoding becomes shorter. When a fractal code applied on different initial images iteratively, they converge toward the original image that fractal code belongs to it. The initial image that is closer to the original image has fewer steps and shorter distances. Fig.6 shows the paths of three different initial images toward the original image. The image x03 is closer to original image and at result d3 is shorter than d1, d2 [15].

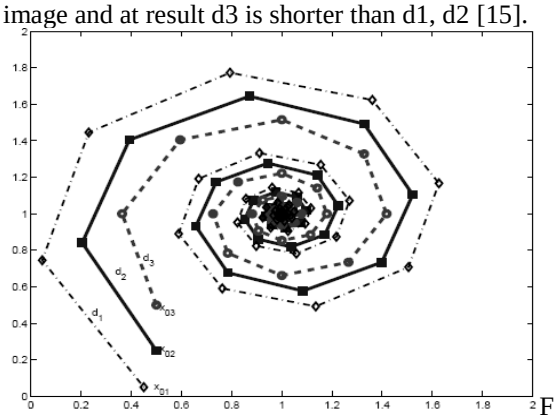



Fig.6: The paths for three different initial images towards original image when the same fractal code is applied iteratively [15].

## 5. Experimental Results

For fingerprint recognition a set of 50 individuals and 5 fingerprint images per individual from various fingerprint databases such as FVC2000, FVC2002 and FVC2004 selected. We used one image for enrollment and four images as test images per person. The original images converted to 128×128 pixel grid and binarized images. Obtained results for fingerprint recognition are illustrated in fig.7 and fig.8.

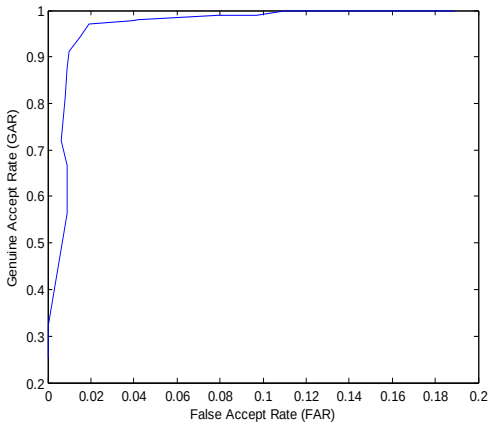



Fig.7: ROC curve for fingerprint recognition.

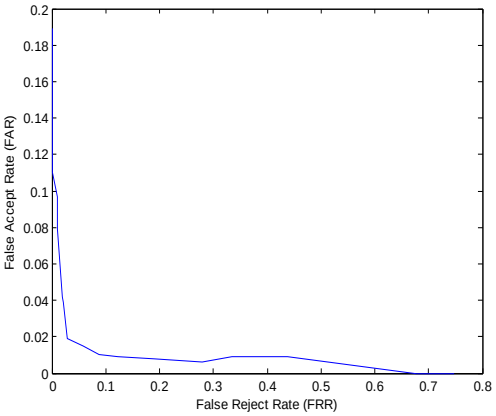



Fig.8: False accept rate against false reject rate

Fig.8 shows that the equal error rate of proposed method is equal to 1.9% and the recognition accuracy of proposed method is 98.1%. In comparison with other practical fingerprint recognition methods the matching performance of proposed method is not perfect but our method is invariant to translations, rotations and illumination differences without additional processing. Furthermore, the proposed method provides template security and Cancelability.

For face recognition a set of 50 persons and 5 face images for each person from BANCA database selected. One image for enrollment and 4 images for recognition test. The face images converted to 128×128 pixels grid and binarized images. The recognition accuracy of proposed method is 98.92% that is acceptable.

Face recognition using fractal image coding has been proposed and applied by others but the difference between our proposed method and previous works is in matching performance [15, 16]. Table 1 illustrates the performance of proposed method in comparison with previous methods with best performance.

Table 1: Comparison between best previous methods and proposed method

| Method | FAR/(FRR=0) | FAR=FRR | FRR(FAR=0) | Recognition Accuracy |
|---|---|---|---|---|
| Ebrahimpour et al. | 53.33% | 16.4% | 51.85% | 95% |
| Tan et al. | 94% | 13.6% | 81.3% | 98.25% |
| Proposed Method | 13.71% | 2.7% | 94.05% | 98.92% |

## 6. Conclusions

One of the important vulnerabilities in biometric systems is the escape of biometric template information. The biometric template protection techniques that are presented until now, have failed to provide all requirements of practical biometric authentication systems. In this paper we reviewed the vulnerabilities of biometric authentication systems and biometric template protection schemes briefly. A method based on fractal image coding for biometric authentication proposed that provides both system database security and Cancelability characteristics. The main advantage of our method is robustness again rotation, translation and different illuminations of input biometric templates without extra processing. The experiment results demonstrate the performance of proposed method.

## 10. References

[1] J. Galbally, J. Fierrez, J. Ortega-Garcia, "Vulnerabilities in Biometric Systems:Attacks and Recent Advances in Liveness Detection", Biometrics Recognition Group-ATVS, Escuela Politecnica Superior Universidad Autonomade Madrid, 2007.

[2] A.K. Jain, A. Ross, U. Uludag, "Biometric template security: challenges and solutions", In Proceedings of the European Signal Processing Conference (EUSIPCO 2005), Antalya, Turkey, 2005.

[3] A.K. Jain, K. Nandakumar, A. Nagar, "Biometric template security", EURASIP Journal on Advances in Signal Process, 2008, 1-17.

[4] U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain, "Biometric cryptosystems: issues and challenges", Proc IEEE, 2004, 92(6):948-960.

[5] A. Juels, M. Wattenberg, "A Fuzzy Commitment Scheme", In: Proc. Sixth ACM Conference on Computer and Communications Security, Singapore, 1999, pp. 28–36.

[6] A. Juels, M. Sudan, "A Fuzzy Vault Scheme", In: Proc. IEEE International Symposium on Information Theory, Lausanne, Switzerland, 2002, p. 408.

[7] G. Davida, Y. Frankel, B. Matt, "On enabling secure applications through offline biometric identification", Proc of IEEE, Symp on Security and Privacy, 1998, p.148-157.

[8] H. Feng, CC. Wah, "Private key generation from on-line handwritten signatures", Inf Manag Comput Secur, 2002, 10(18):159-164.

[9] N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, 2001, (40):614-634.

[10] J. Zuo, N.K. Ratha, J.H. Connel, "Cancelable iris biometric", Proc of the 19th Int Conf on Pattern Recognition, 2008, (ICPR'08) p.1-4.

[11] M. Savvides, B. Kumar, P. Khosla, "Cancelable biometric filters for face recognition", ICPR '04: Proc of the Pattern Recognition, 17th Int Conf on (ICPR'04), 2004, (3):922-925.

[12] K. Nandakumar, A. Nagar, A.K. Jain, "Hardening Fingerprint Fuzzy Vault Using Password", In: Proc. Second Intl. Conf. on Biometrics, Seoul, South Korea, 2007, pp. 927–937.

[13] W. Sheirer, T. Boult, "Bio-cryptographic protocols with bipartite biotokens", In: Proc. Biometric Symposium, 2008.

[14] Fisher, Y., Fractal Image Compression: Theory and Application, Springer-Verlag Inc, 1995.

[15] H. Ebrahimpour-komleh, V. Chandran, S. Sridharan, "An Application of Fractal Image-set Coding in Facial Recognition", Springer Verlag Lecture Notes in computer science, Vol 3072, Biometric Authentication, 2004, pp.178-186.

[16] T. Tan, H. Yan, "Face recognition using the weighted fractal neighbour distance", IEEE Trans. Systems, Man, and Cybernetics, 2005, vol. 35, pp.576-582.