A Novel Technique for Enhancing Security in Biometric Based Authentication Systems

Atiya Zahed and Mohammad Reza Sakhi

Abstract—Traditional personal authentication systems that are based on knowledge (e.g., password) or physical tokens (e.g., ID card) are not able to meet strict security performance requirements of a number of modern applications. Biometric-based authentication systems that use physiological and/or behavioral traits (e.g., fingerprint, face and signature) are good alternatives to traditional methods. These systems are more reliable (biometric data cannot be lost, forgotten or guessed) and more user-friendly (there is nothing to remember or carry). In spite of these advantages of biometric systems over traditional systems, there are many unresolved issues associated with the former. In this article, we analyze structure of biometric-based authentication systems and vulnerability of these systems and develop a method for increasing the security of image-based (e.g., fingerprint and face) biometric templates. We use a method based on fractal image coding for face and fingerprint recognition. We create a database from fractal codes of biometric images. For identification the input image is decoded with each fractal code in the database. The fractal code that minimizes the Euclidian difference between the input image and the result image after one iteration of decoding is taken as the best. We used this method for fingerprint and face recognition. Similar methods for face recognition have been proposed by others, but what distinguishes our work from the rest is that we improve the recognition rate needles to execution proposed by others, but what distinguishes our work from the previous work is that we improve the recognition rate needles to execution.

Index Terms—Authentication, Biometric Template, Fractal Image Coding, Security

I. INTRODUCTION

Data security in computer systems usually refers to the ability of system for confidentiality and integrity of information. Present an exact definition for biometric system security, because of differences between biometric system and traditional systems, is complicated. Biometric systems have certain traverses, among a) the loss of confidentiality (e.g. everybody could get our fingerprints), and b) a biometric trait cannot be replaced (if we forget a password we can easily generate a new one, but we can not generate a new fingerprint). Furthermore, biometric systems are vulnerable to external attacks which could decrease their level of security. The security analysis of traditional password-based authentication schemes can be based on explicit elements, such as the minimum length of passwords (e.g., minimum of 8 characters). Similarly, the security of token-based systems can be analyzed based on the expectancy of illegal use of the token (e.g., the probability that a valid ID card is lost and later found by an attacker) and the feasibility of illegally replicating/generating a token (e.g., how easy it is to manufacture an ID card that includes a signature)[1],[7].

Biometric systems are inherently much more complicated than these traditional authentication schemes, due to (a) nature of the data they need to operation (e.g., biometric data of individuals are not same in each acquisition, compared to a ID card), (b) the number and complexity of the associated modules (e.g., complex image enhancement operations may be necessary for poor quality fingerprints) and (c) the overall architectural design (e.g., the need to securely access stored biometric data). As a result, there are many critical points in a biometric system that can be compromised, which are inherently absent in traditional authentication schemes [2], [9].

II. REVIEW OF VULNERABILITIES IN BIOMETRIC SYSTEMS

Even though biometric systems offer several advantages over traditional token (e.g., key) or knowledge (e.g., password) based authentication methods, they are still vulnerable to attacks. These attacks analyzed and grouped into eight classes. Figure1 shows the locations of these attacks in a biometric system.

A type 1 attack encompasses presenting a fake biometric (e.g., facemask) to the sensor. The second type of attack is called a replay attack, because a snatched biometric data is submitted to the feature extractor, bypassing the sensor.

In the third type of attack, the feature extractor module is replaced with a Trojan horse program that functions according to its designer’s specifications. In the fourth type of attack, original feature values are replaced with values (synthetic or real) selected by the attacker. In the fifth type of attack, the matcher is replaced with a Trojan horse program. The attacks on the template database (e.g., addition, modification, or removal of templates) form the sixth type of attack. In the seventh type of attack, the templates are slanted
(stolen, replaced, or altered) in the transmission medium between the template database and matcher. Lastly, the matcher result (accept or reject) can be trampled by the attacker [2].

Note that the relative threats of these attacks depend on (a) biometric modality (e.g., it is harder to physically replicate a retina scan than it is to forge a signature), (b) type of sensor (2D vs. 3D face sensors), (c) type of matcher operating on the same biometric (face matchers based on texture vs. geometry), and (d) the security settings of the biometric system.

The main problems of biometric systems are the loss of confidentiality (e.g., face images being captured by hidden cameras), and non situation ability (e.g., once the biometric data is compromised, there is no way to return to a secure situation, dissimilar to replacing a password).

The problems that may appear from the above-mentioned attacks on biometric systems are raising concerns as more and more biometric systems are being deployed. This, combined with the increase in using these systems may cause to remarkable financial, privacy, and security related violations [8].

III. SECURITY ASPECTS OF BIOMETRIC SYSTEMS

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. In this article, the term security is used to characterize the total reliability of the system, rather than just the facile notion of increased authentication accuracy brought about by the use of biometrics for verification/identification. While it is true that any increase in such authentication accuracy increases the security of the system, there are many other issues that need to be taken into account before arriving at a truly secure biometric system.

One security-related issue is the robustness of the biometric systems against attacks invented specifically to defeat their operation. Vulnerability points which are presented in Figure 1 can broadly be divided into two main groups: Direct attacks and indirect attacks [3].

Direct attacks: To generate artificial biometric samples (for instance, fingerprints) in order to deceitful access to a system was defined as the first vulnerability point in a biometric security system. These attacks at the sensor level are referred to as direct attacks. It is benefit noting that in this type of attacks no specific knowledge about the system operation is needed (matching algorithm used, feature extraction, etc.). Furthermore, the attack is carried out in the analog domain and there is no the digital limitations of the system, so the digital protection mechanisms (digital signature, watermarking...) cannot be used. This group included point 1 in fig 1[3].

Indirect attacks. This group includes all the remaining seven points of attack identified in figure 1. Attacks 3 and 5 might be carried out using a Trojan Horse program that bypasses the feature extractor, and the matcher respectively. In attack 6 the system database is manipulated (a template is changed, added or deleted) in order to access to the application. The remaining points of attack (2, 4, 7 and 8) are thought to exploit possible weak points in the communication channels of the system, extracting, adding or changing in formation from them. In dissent to direct attacks, in this case the trespasser needs to have some information about the internal working of the identification system and, in most cases physical access to some of the application components (feature extractor, matcher, database...) is required [3].

A specific problem inside this general scope of system robustness against attacks is guaranteeing the security of biometric templates. One of the most damaging attacks on a biometric system is against the biometric templates stored in the system database. Attacks on the template can lead to the following three vulnerabilities: (a) A template can be replaced by an intruder’s template to gain unauthorized access, (b) A physical spoof can be created from the template to gain unauthorized access to the system and (c) The stolen template can be replayed to the matcher to gain unauthorized access. For protecting of biometric template, a set of salient features that extracted from biometric data of an individual save in system database instead of saving biometric template. These extracted features have compact nature and can not be used to elicit complete information about original biometric data. The template protection schemes proposed in the literature can be broadly classified into two categories namely, feature transformation approach and biometric cryptosystem [4].

The issue of perfect integration of biometric components into existing authentication systems is also important. Due to the rather independent development of traditional and biometrics-based authentication systems many of the current applications are designed especially around traditional systems. Trying to incorporate biometric components into such applications brings along problems that need to be resolved. For example, using biometric data in traditional encryption/decryption architectures for copyright protection of multimedia data is an unresolved problem.

Considering that both the traditional cryptographic systems and biometrics-based authentication systems, direct at the common goal of reliable access control, there have been attempts to combine these apparently separate domains. Essentially, these approaches can be grouped into two groups: (a) the biometric element acts as a wrapper around the cryptographic component, and (b) the biometric element is merged with the cryptographic domain at a much deeper level, where biometric matching essentially takes place within the cryptography domain.

These biometric cryptographic systems provided their components are combined intelligently, having the capacity to merge the proven security of cryptographic systems with the user-friendly property of biometric systems [5].

These problems are represented in Fig 2, which also represents the domains of biometrics and security areas.
IV. PROPOSED METHOD

A. Fractal Coding

Using fractal codes as features for object or shape recognition is a new application of fractal image encoding. The goal of the fractal image encoding algorithms is to be able to create a series of mathematical processes which would produce an accurate reproduction of an image. Fractal codes are much more compact than the original image and many algorithms have been proposed to use these codes for image compression. Recently some other applications of fractal codes have been reported. In some of these applications like face recognition, fractal codes are used directly as features and in others, like content-based retrieval in fractal coded image databases, these codes are used after extracting features. Initial experiments conducted on face images demonstrate that fractal codes make robust features possessing good shape information. The first fully automated algorithm for fractal image compression, proposed by Jacquin in 1989. Until Jaquin’s encoder became available, attempts had been made to design fractal encoders which were supposed to create transformation with the structure of iterated function systems. Jaquin’s method was based on partitioned iterated function systems (PIFS), a more general type of transformation which exploits the fact that a part of an image can be approximated by a transformed and down-sampled version of another part of the same image, this property is called piecewise self-similarity. A PIFS consists of a complete metric space X, a collection of sub-domains, \( D_i \subseteq X, i = 1, \ldots, n \) and a collection of contractive mappings, \( w_i : D_i \rightarrow X, i = 1, \ldots, n \). The encoder works as follows:

- Range Blocks: An image to be encoded is partitioned into non-overlapping range blocks \( R_i \).
- Domain Blocks: An image is also partitioned into larger blocks \( D_i \) called domain blocks which can be overlapped.

Transformation: The task of a fractal encoder is to find a domain block \( D_i \) of the same image for every range block \( R_i \) such that a transform \( w_i : D_i \rightarrow X, i = 1, \ldots, n \)

\[
d(p,q) = \sqrt{\sum_{k=0}^{255} \sum_{l=0}^{255} (p(k,l) - q(k,l))^2}
\]  

B. Algorithm

Step1 (preprocessing): using Histogram Equalization and Fourier Transform to do image enhancement and then the biometric image is converted to binary format.

Step2: create a database of fractal codes of biometric images

Step3: The input image is decoded with each fractal code in the database.

Step4: identity of the fractal code that minimizes the difference between the input image and the resultant image after one iteration of decoding is taken as the best match.

C. Experimental Results

For fingerprint recognition we selected a set of 34 individuals and 3 fingerprint images per individual from various fingerprint databases like FVC2000, FVC2002 and FVC2004. We used first image for training set and other images as test images. Images were 128×128 pixel grid. Both identification and verification with our method have desirable results.

The fingerprint recognition accuracy in this method is 90%. This accuracy in comparison with other methods for fingerprint recognition is not proper but our method needs no heavy preprocessing like others and works on whole of fingerprint image instead of work on local features of fingerprint (minutiae points). Results of fingerprint verification by use of this method described in Fig. 3 and Fig. 4.

For face recognition we selected a set of 50 individuals and 5 face images per individual with different expressions from BANCA face database. We used first image for training set and other images as test images. Images were 128×128 pixel grid. Both identification and verification with our method have desirable results.

Face recognition accuracy in this method is about 98.98%. This accuracy in comparison with other methods for face recognition is desirable whereas our method works on whole of face image and needs no heavy preprocessing operations like face detection and eye location. Results of face verification by use of this method described in Fig. 5 and Fig. 6.
V. SUMMARY AND CONCLUSIONS

In order to improve the performance of biometric systems it is of great importance to study its vulnerabilities to external attacks. In this paper we reviewed vulnerabilities of general biometric systems and presented a method for fingerprint and face recognition based on fractal coding that improves the biometric system security. Similar methods for face recognition have been proposed by others, but what distinguishes our work from the rest is that we improve the recognition rate needles to execution same complicated preprocessing. Other advantages of this method are: increasing security because use of fractal codes instead of original images, and acceptable result in face recognition in spite of different face expression. Similar methods for fingerprint recognition have not been suggested by others. Our work and its incentive results confirm the possibility of using fractal coding for fingerprint recognition.

REFERENCES


Atiya Zahed, Birth Place: Kashan/Iran, Birth Date: 1978, Education Record: M.S Degree, Major: computer science, Field: software, Institution: Islamic Azad University Branch of Najafabad, City/Country: Najafabad/Iran, Year of degree obtaining: 2008
She experience as an instructor for 3 year, including Algorithms , Data Structures & Theory of Languages and Automata in Islamic Azad University Branch of Kashan. She has investigated on the issue of “Digital Watermarking”.

Mohammad Reza Sakhi, Birth Place: Kashan/Iran, Birth Date: 1970, Education Record: B.S Degree & Student f M.S, Major: computer science, Field: Information Technology, Institution: Shiraz University, City/Country: Shiraz/Iran, Year of degree obtaining: 2011
He is completing his thesis titled “Fast and Effective Clustering of XML Document Using Genetic Algorithm”.