International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 5, September – October 2013 ISSN 2278-6856

A Study on Attacks and Security Against Fingerprint Template Database

Mrs.U.Latha[1], Dr.K.Rameshkumar[2]

[1]Department of Information Technology, DACE,
Padappai, Chennai, India,
Corresponding Author

[2]Department of Information Technology, HITS,
Padur, Chennai, India,

Abstract: ***Biometric based authentication, the science of using physical or behavioral characteristics for identity verification is becoming a security mainstay in much areas.This paper examines the major forms of known attacks against biometric systems and Biometric template database attacks. A literature study of the attack points in each of the biometric system and the various methods to combat the attacks at these points is conducted and analyzed in this paper. In spite of numerous advantages of biometrics-based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. In this paper, we analyze these attacks in the realm of a fingerprint biometric system. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system. Protecting the template is a challenging task due to variability in the acquired biometric traits. We present an overview of various biometric template protection schemes and discuss their advantages in terms of security, revocability, and impact on matching accuracy***.

Keywords: Biometrics, Attacks, Hill climbing, Modification, Watermarking, Cryptography.

1. INTRODUCTION

Biometric systems offer several advantages over traditional authentication methods. Biometric information cannot be acquired by direct covert observation. It is impossible to share and difficult to reproduce. It enhances user convenience by alleviating the need to memorize long and random passwords [1]. It protects against repudiation by the user. In spite their numerous advantages, biometric systems are vulnerable to attacks, which can decrease their security.Ratha et al. [2] analyzed these attacks, and grouped them into eight classes. In following sections we discuss about the (i) structure of Biometric system (ii) Biometric system performance (iii) attacks on biometric system (iv) possible attacks on template storage and (v) Securing the template database.

2. STRUCTURE OF BIOMETRIC SYSTEM

Every biometric system consists of four basic modules:

2.1 Enrollment Unit

The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation.

2.2 Feature Extraction Unit

This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

2.3 Matching Unit

This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one to many matching).

2.4 Decision Maker

This module accepts or rejects the user based on a security threshold and matching score.

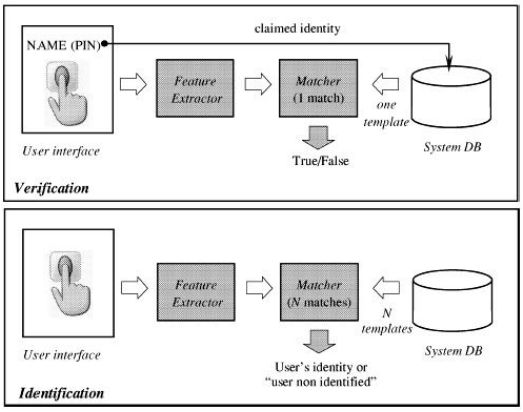

Figure 1: Biometric System

3. BIOMETRIC SYSTEM PERFORMANCE

The performance evaluation of a biometric system depends on two types of errors – matching errors and acquisition errors [3]. The matching errors consist of the following:

3.1 False Acceptance Rate (FAR)

Mistaking biometric measurements from two different persons to be from the same person. The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

3.2. False Rejection Rate (FRR)

Mistaking biometric measurements from the same person to be from two different persons. The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

However, FAR only provides half the information. When selecting a biometric solution, we need to find out what the False Rejection Rate (FRR) is at the said FAR. So when a biometric solution provider claims to have a very low FAR, it is very important to find out what is the FRR at this 'low' FAR. Then depending upon the application one needs to evaluate whether the FAR & FRR ratio is acceptable for the application. In a practical scenario a low FAR & a high FRR would ensure that any unauthorized person will not be allowed access. It would also mean that the authorized people will have to put their finger on the device several times before they are allowed access. Therefore, it is good to have a very low FAR, but please remember that if this low FAR is coming at the cost of high FAR then the solution needs to be re-evaluated.

The acquisition errors consist of the following:

3.3. Failure to Capture Rate (FTC)

Proportion of attempts for which a biometric system is unable to capture a sample of sufficient quality. Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

3.4. Failure to Enroll Rate (FTE)

Proportion of the user population for which the biometric system is unable to generate reference templates of sufficient quality. The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs. This includes those who, for physical or behavioral reasons, are unable to present the required biometric feature [4]. All of the above are used to calculate the accuracy and performance of a biometric system.

4. ATTACKS ON BIOMETRIC SYSTEM

Biometric system modules have nine different points of attack. These points of attack are discussed in detail below

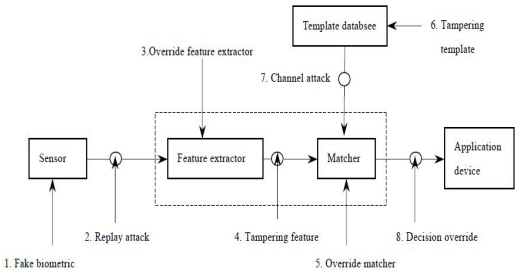

Figure: 2 Attack points on Biometric System

4.1 Type 1

This point of attack is known as "Attack at the scanner". In this attack, the attacker can physically destroy the recognition scanner and cause a denial of service. The attacker can also create a fake biometric trait such as an artificial finger to bypass fingerprint recognition systems, or inject an image between the sensing element and the rest of the scanner electronics to bypass facial recognition systems.

4.2 Type 2

This point of attack is known as "Attack on the channel between the scanner and the feature extractor" or "Replay attack". When the scanner module in a biometric system acquires a biometric trait, the scanner module sends it to the feature extractor module for processing.

4.3 Type 3

This point of attack is known as "Attack on the feature extractor module". In this attack, the attacker can replace the feature extractor module with a Trojan horse.

4.4 Type 4

This point of attack is known as "Attack on the channel between the feature extractor and matcher". The difference is that the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher at a later time.

4.5 Type 5

This point of attack is known as "Attack on the matcher". The difference is that the attacker replaces the matcher with a Trojan horse. The attacker can send commands to the Trojan horse to produce high matching scores and send a "yes" to the application to bypass the biometric authentication mechanism.

4.6 Type 6

This point of attack is known as "Attack on the system database". In this attack, the attacker compromises the security of the database where all the templates are stored. Compromising the database can be done by exploiting vulnerability in the database software or cracking an account on the database. In either way, the attacker can

add new templates, modify existing templates or delete templates.

4.7 Type 7

This point of attack is known as "Attack on the channel between the system database and matcher". In this attack, the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data.

4.8 Type 8

This point of attack is known as "Attack on the channel between the matcher and the application". In this attack, the attacker intercepts the communication channel between the matcher and the application to replay previously submitted data or alter the data.

4.9 Type 9

We claim that a 9th point of attack exists in biometric systems. We call this attack "Attack on the application". Bugs are a consequence of the nature of the programming task that no one can deny. It is a fact that any software has at least one bug in it. Since biometric authentication systems are not 100% accurate, most of these systems use traditional authentication schemes as a backup.

5. GENERIC SECURITY THREATS

Any system (including biometric systems) is susceptible to various types of threats. These threats are discussed below:

i. Denial of Service: An adversary overwhelms computer and network resources to the point that legitimate users can no longer access the resources.

ii. Circumvention: An adversary gains access to data or computer resources that he may not be authorized to access.

iii. Repudiation: A legitimate user accesses the resources offered by an application and then claim that an intruder had circumvented the system.

iv. **Covert acquisition:** An adversary compromises and abuses the means of identification without the knowledge of a legitimate user.

v. Collusion: In any system, there are different user privileges. Users with super-user privileges have access to all of the system's resources. Collusion occurs when a user with super-user privileges abuses his privileges and modifies the system's parameters to permit incursions by an intruder.

vi. Coercion: A legitimate user is forced to give an intruder access to the system. For example, an ATM user could be forced to give away her ATM card and PIN at gunpoint.

6. POSSIBLE ATTACKS ON TEMPLATE DATABASE

Attacks against Secure Template Protection Technologies

• **Basic Brute Force**- Attacker tries every possible bit combination till they guess the correct original feature data or key.

• **Correlation Attack**- From a cryptanalysis point of view, a good stream cipher should be resistant against a known-plaintext attack. In a known-plaintext attack the cryptanalyst is given a plaintext and the corresponding cipher text, and the task is to determine a key K. For a synchronous stream cipher, this is equivalent to the problem of finding the key K that produces a given key stream z1, z2,..., zN.

• **Known Key Attack**- Evaluate whether or not the fixed permutation with a randomly chosen key is ideal.

• **Substitution Attack**- "How difficult will it be to break into a folder containing biometric signatures and replace them with an attacker's biometric signature so that the attacker can get in with his/her own signature easily?"

• **Decidability Attack**- Exploit available information to link across databases.

• **Doppelganger Attack**- If the FAR is 1 in *X*, then an attacker can try more than *X* different prints.

• **Hill climbing Attack**-Security attacks based on generating artificial data, injecting it in the system and after analyzing the output and modifies the data.

7. PROTECTING THE TEMPLATE DATABASE

Several methods have been suggested in the literature to protect biometric templates from revealing important information. In order to prevent the Hill-Climbing Attack from successfully converging, Soutar [5] has suggested the use of coarsely quantized match scores by the matcher. However, Adler [6] demonstrated that it is still possible to estimate the unknown enrolled image although the number of iterations required to converge is significantly higher now.

Yeung and Pankanti [7] describe an invisible fragile watermarking technique to detect regions in a fingerprint image that have been tampered by an attacker. In the proposed scheme, a chaotic mixing procedure is employed to transform a visually perceptible watermark to a random-looking textured image in order to make it resilient against attacks. This "mixed" image is then embedded in a fingerprint image. The authors show that the presence of the watermark does not affect the feature extraction process. The use of a watermark also imparts copyright capability by identifying the origin of the raw fingerprint image. Jain and Uludag [8] suggest the use of steganography principles to hide biometric data (e.g., fingerprint minutiae) in host images (e.g., faces). This is particularly useful in distributed systems where the raw biometric data may have to be transmitted over a non-secure communication channel. Embedding biometric data in an innocuous host image prevents an eavesdropper from accessing sensitive template information. The authors also discuss a novel application

wherein the facial features of a user (i.e., eigen-coefficients) are embedded in a host fingerprint image (of the user). In this scenario, the watermarked fingerprint image of a person may be stored in a smart card issued to that person. At an access control site, the fingerprint of the person possessing the card will first be compared with the fingerprint present in the smart card. The eigen-coefficients hidden in the fingerprint image can then be used to reconstruct the user's face thereby serving as a second source of authentication.

Ferri et al. [9] propose an algorithm to embed dynamic signature features into face images present on ID cards. These features are transformed into a binary stream after compression (used in order to decrease the amount of payload data). A computer-generated hologram converts this stream into the data that is finally embedded in the blue channel of a face image. During verification, the signature features hidden in the face image are recovered and compared against the signature obtained on-line. Ferri et al. [9] report that any modification of the face image can be detected, thereby disallowing the use of fake ID cards. Since the biometric trait of a person cannot be easily replaced (unlike passwords and PINs), a compromised template would mean the loss of a user's identity. Ratha et al.[10] propose the use of distortion functions to generate biometric data that can be *canceled* if necessary. They use a non-invertible transformation function that distorts the input biometric signal (e.g., face image) prior to feature extraction or, alternately, modifies the extracted feature set (e.g., minutiae points) itself. When a stored template is compromised, then the current transformation function is replaced with a new function thereby "canceling" the current (compromised) template and generating a new one. This also permits the use of the same biometric trait in several different applications by merely adopting an application-specific transformation function. However, it is not clear how matching can be accomplished in the transformed domain. In the realm of template transformation, the so-called *biometric cryptosystems* are gaining popularity (for a survey on existing techniques, see [11]). These systems combine biometrics and cryptography at a level that allows biometric matching to effectively take place in the cryptographic domain, hence exploiting the associated higher security. For example, Uludag et al. [12] convert fingerprint templates (minutiae data) into point lists in 2D space, which implicitly hide a given secret (e.g., a 128-bit key). The list does not reveal the template data, since it is augmented with chaff points to increase security. The template data is identified only when matching minutiae data from an input fingerprint is available.

8. SUMMARY AND CONCLUSIONS

We have discussed various types of attacks that can be launched against a biometric system. We have specifically highlighted techniques that can be used to elicit the contents of a biometric template thereby compromising the information. We discuss the importance of adopting watermarking and steganography principles to enhance the integrity of biometric templates. Cancelable biometrics may be used to "reset" the biometric template of a user in the event that the user's template is compromised. Also, biometric cryptosystems can contribute to template security by supporting biometric matching in secure cryptographic domains.

References

[1] Jain A. K., Uludag U., Attacks on biometric systems: a case study in fingerprints, Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI, San Jose, CA, pp.622–633, 2004.

[2] Jain A. K., Ross A., Uludag U., Biometric template security: challenges and solutions, in Proceedings of the European Signal Processing Conference (EUSIPCO '05), Antalya, Turkey, and September 2005.

[3] Ailisto, Heikki, Mikko Lindholm, Satu-Marja Mäkelä, Elena Vildjiounaite, "*Unobtrusive user identification with light biometrics*", Proceedings of the third Nordic conference on Human-computer interaction, October 2004.

[4] Arndt, Craig M., "*Biometric template revocation*", Proceedings of SPIE -- Volume 5404, August 2004.

[5] C. Soutar, "Biometric system security," White Paper, Bioscrypt, http://www.bioscrypt.com.

[6] A. Adler, "Images can be regenerated from quantized biometric match score data," in *Proc. Canadian Conf.Electrical Computer Eng.*, pp. 469–472, (Niagara Falls, Canada), May 2004.

[7] M. Yeung and S. Pankanti, "Verification watermarks on fingerprint recognition and retrieval," in *Proc. SPIE,Security and Watermarking of Multimedia Contents,*vol. 3657, pp. 66–78, (San Jose, USA), January 1999.

[8] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intelligence*, vol. 25,no. 11, pp. 1493–1498, 2003.

[9] L. C. Ferri, A. Mayerhofer, M. Frank, C. Vielhauer, and R. Steinmetz, "Biometric authentication for ID cards with hologram watermarks," in *Proc. SPIE, Security and Watermarking of Multimedia Contents IV*,vol. 4675, pp. 629–640, (Bellingham, WA), January2002.

[10] N. Ratha, J. Connell, and R. bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614– 634, 2001.

[11] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[12] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," *To appear in Proc. Audio- and*

Video based Biometric Person Authentication (AVBPA), (Rye Brook, NY), July 2005.

Author:

U.Latha (Umapathy Latha) received the M.Tech (IT) degree from Sathyabama University, Chennai, India in 2008. Currently she is an **Assistant professor in the Department of Information Technology at Dhaanish Ahmed College of Engineering, Chennai, India**. Currently her research work is on Biometrics and the Biometric databases. She participated in many national and International events in Chennai.

Dr.K.Rameshkumar received the PhD (CSE) degree from Alagappa University, India, in 2011. He is currently an **Associate Professor in the Department of Information Technology at Hindustan University, Chennai, India**. His research interests are in knowledge discovery from real time databases and Cloud data management. Current he is concentration on Big Data research. He participated many international and national level events around the country. Dr. K.Rameshkumar is working as editor in various International and national level journals.