IJITKM Volume 8 • Number 1 June-Dec 2014 pp. 85-95 (ISSN 0973-4414)

Biometric Systems Security and Challenges

Shiwani Goyal
Asst. Professor, Department of Computer Science, DAV, College, Yamuna Nagar

Abstract: A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. These days, biometric technologies are typically used to analyze human characteristics for security purposes. In spite of numerous advantages of biometric based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. This paper is confined to the analysis of these attacks in regard of fingerprint biometric systems, and presents several measures to prevent them at the end.
Keywords Biometrics, fingerprint, minutiae, security, template, attack.

1. Introduction

Biometrics-based personal authentication systems that use physiological (e.g., fingerprint, face) or behavioral (e.g., speech, handwriting) traits are becoming increasingly popular, compared to traditional systems that are based on tokens (e.g., key) or knowledge (e.g., password)[1].Traditional authentication systems cannot discriminate between an impostor who fraudulently obtains the access privileges (e.g., key, password) of a genuine user and the genuine user herself. Furthermore, biometric authentication systems can be more convenient for the users since there is no password to be forgotten or key to be lost and a single biometric trait (e.g., fingerprint) can be used to access several accounts without the burden of remembering passwords. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. The characteristics are measurable and unique. These characteristics should not be duplicable, but it is unfortunately often possible to create a copy that is accepted by the biometric system as a true sample.

Fingerprint Deformations

Deformations are basically the factors affecting the performace of a biometric trait during its enrollment or authenticating process. Though fingerprint biometric systems are known for their accuracy and wide acceptability, there are numerous factors that affect its performance. One must consider the following factors while choosing fingerprint as biometric trait[2]:

•**Live scan quality**—Live scan quality directly affects the number of biometric features that can be extracted from the fingerprint. Remember that the number of features is directly related to overall biometric system performance. The scan device must reliably deliver high-quality fingerprint scans each and every time the scanner is used and under all use scenarios.

•**Enrollment scan quality**—Poor enrollment scan quality permanently degrades accuracy for that user and drags down overall system performance. Thus, a higher standard of fingerprint scan and biometric template quality should be applied to the enrollment process.

•**Scan device usability**—The location and orientation of the scanning device should be such that the user can quickly and accurately place their finger in a manner that reliably leads to a high-quality live scan with one touch.

•**User skin condition**—Many types of scanners are sensitive to user skin conditions and placement pressure since they rely on a measurement approach that only differentiates areas in contact with the scanner (fingerprint ridges) from areas not in contact (valleys). As a result, dry or damp skin can degrade the quality of the live scan, as can surface contaminants or variability in pressure applied to the sensor by the user.

•**User fingerprint expression**—Some individuals have poor fingerprint expression or very fine fingerprint features. In addition, as a person becomes older, the collagen level in the skin is reduced enough to cause complications in fingerprint scan reliability.

•**Closed vs. open biometric systems**—An open system is one where a variety of fingerprint scan devices, biometric template generators, and automatic biometric template matchers are used. Open or interoperable systems offer convenience in the design and implementation of the system. However, open systems have lower performance because of least common denominator effects.

•**Liveness detection**—A scanner with liveness detection is one that prevents the use of copies of the fingerprint to be used. This includes means to prevent the activation of a latent print, the use of a 2-dimensinal paper copy, or the use of a sophisticated 3-dimensional copy. A scanner lacking this capability will accept copies, and this would result in a system breach similar to a stolen user ID or password pair.

In spite their numerous advantages, biometric systems are vulnerable to attacks, which can decrease their security. Ratha et al.[3] analyzed these attacks, and grouped them into eight classes. Figure 1 shows these attacks along with components of a typical biometric system that can be compromised. Type 1 attack involves presenting a fake biometric to the sensor. Submitting a previously intercepted biometric data constitutes the second type of attack (replay). In the third type of attack, the feature extractor module is comprised to produce feature values selected by the attacker. Genuine feature values are replaced with the one selected by attacker in the fourth type of attack. Matcher can be modified to output an artificially high matching score in fifth type of attack. The attack on template database (e.g. adding a new template, modifying an existing template, removing templates etc.) constitutes the sixth type of attack. The transmission medium between the template database and matcher is attacked in seventh type of attack resulting in the alteration of the transmitted templates. Finally, the matcher result (accept or reject) can be overridden by the attacker.

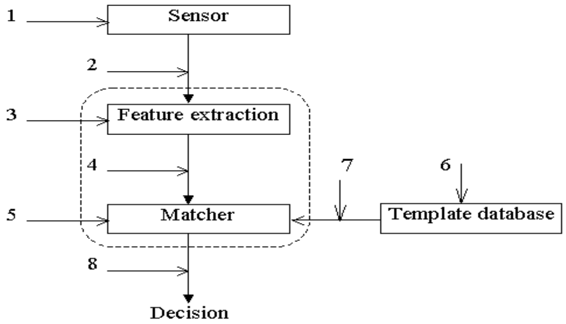

Figure 1 Eight different points in biometric authentication systems.

In *Denial of Service (DoS),* an attacker corrupts the authentication system so that legitimate users cannot use it. For a biometric authentication system, an online authentication server that processes access requests (via retrieving templates from a database and performing matching with the transferred biometric data) can be bombarded with many bogus access requests, to a point where the server's computational resources cannot handle valid requests any more. In *circumvention,* an attacker gains access to the system protected by the authentication application. This threat can be cast as a privacy attack, where the attacker accesses the data that she was not authorized (e.g., accessing the medical records of another user) or, as a subversive attack, where the attacker manipulates the system (e.g., changing those records, submitting bogus insurance claims, etc.). In *repudiation,* the attacker denies accessing the system. For example, a corrupt bank clerk who modifies some financial records illegally may claim that her biometric data was "stolen", or she can argue that the False Accept Rate (FAR) phenomenon associated with any biometric may have been the cause of the problem.

In *contamination (covert acquisition),* an attacker can surreptitiously obtain biometric data of legitimate users (e.g., lifting a latent fingerprint and constructing a three-dimensional mold) and use it to access the system. Further, the biometric data associated with a specific application can be used in another unintended application (e.g., using a fingerprint for accessing medical records instead of the intended use of office door access control). This becomes especially important for biometric systems since we have a limited number of useful biometric traits, compared to practically unlimited number of traditional access identities (e.g., keys and passwords). Cross-application usage of biometric data becomes more probable with the growing number of applications using biometrics (e.g., opening car or office doors, accessing bank accounts, accessing medical records, locking computer screens, gaining travel authorization, etc.). In *collusion*, a legitimate user with wide access privileges (e.g., system administrator) is the attacker who illegally modifies the system. In *coercion*, attackers force the legitimate users to access the system (e.g., using a fingerprint to access ATM accounts at a gunpoint)[4] .

2. Existing Work

In this section, we summarize several studies that show the vulnerability of biometric systems and provide solutions to some of the attacks presented in Section 1.

Fake biometric submission to the sensor (type 1 attack) are quite successful as these attacks do not need anything more than a fake biometric; hence the feasibility of it compared to the other attacks can be high. For example, neither a knowledge of the matcher or template specifications nor template database access privileges are necessary. Also, since it operates in the analog domain, outside the digital limits of the biometric system, the digital protection mechanisms such as encryption, digital signature, hashing etc. are not applicable.

Putte and Keuning[5] tested several fingerprint sensors to check whether they accept an artificially created (dummy) finger instead of a real finger. The authors describe methods to create dummy fingers with and without the cooperation of the real owner of the biometric. When the owner cooperates obviously, the quality of the produced dummy fingers can be higher than those produced without cooperation. In the former case, after creating the plaster cast of the finger, liquid silicon rubber is filled inside the cast to create a wafer-thin dummy that can be attached to a finger, without being noticed at all. This operation is said to take only a few hours. In the latter case, more time (nearly eight hours) and more skill are needed:first, a fine powder is used to enhance the latent fingerprints left on a glass or scanner surface. Then, a photo of the print is taken which is used to transfer the print to a PCB (Printed Circuit Board). UV light exposure and acid etching leaves the profile of the print on the board, which is used for producing the silicon cement dummy. Five out of six sensors (that included both optical and solid state sensors) tested by the authors accepted a dummy finger created by the above methods as a real finger in the first attempt; the remaining sensor accepted the dummy finger in the second attempt.

To overcome such fake biometric attacks, Derakhshani et al.[6] proposed two software-based methods (not based on sensors that measure temperature, conductivity, etc.) for fingerprint liveness detection. They used a commercially available capacitive sensor and the sole input to the liveness detection module is a 5-second video of the fingerprints. In their static method, the periodicity of sweat pores along the ridges is used for liveness detection. In the dynamic method, sweat diffusion pattern over time along the ridges is measured.

We can see that fake biometric attacks can be quite successful in fooling the existing systems, and no perfect (either hardware or software) solution is currently available. As noted previously, this attack aims at a point in the biometric system that is very close to the end user (in the sense that a physical replica is used) and this may hinder the utilization of some protection mechanisms. One other problem associated with this attack is that the means to detect an attack are limited.

The remaining attacks are feasible only if some knowledge about the biometric authentication system and/or some access privileges are available to the attacker. This fact may decrease their applicability compared to type 1 attacks. On the other hand, it may also increase their applicability since no physical production (that is still more costly and time consuming compared to digital production) such as plastic molding, is necessary. Further, in the digital domain, the attacks can be executed in relatively less time.

For eliminating type 2 attacks, where a previously intercepted biometric is replayed there is a challenge/response based system. A pseudo-random challenge is presented to the sensor by a secure transaction server. At that time, the sensor acquires the current biometric signal and computes the response corresponding to the challenge (for example, pixel values at locations indicated in the challenge). The acquired signal and the corresponding response are sent to the transaction server where the response is checked against the received signal for consistency. An inconsistency reveals the possibility of the *resubmission* attack.

Data hiding and watermarking techniques have also been proposed as means of increasing the security of fingerprint images, by detecting modifications by hiding one biometric into another and by hiding messages (authentication stamps such as personal ID information) in the compressed domain.

How the attack system works

Our attack system inputs synthetic minutiae sets to the matcher with the aim of gaining access to the system in place of a genuine user. Note that the user’s template information is unknown to the attack system. Using the scores returned by the matcher and the characteristics of these minutiae sets, the attack system tries to generate a minutia set that results in a sufficiently high matching score to achieve positive identification. The block diagram of the proposed system is given in figure 2[7].

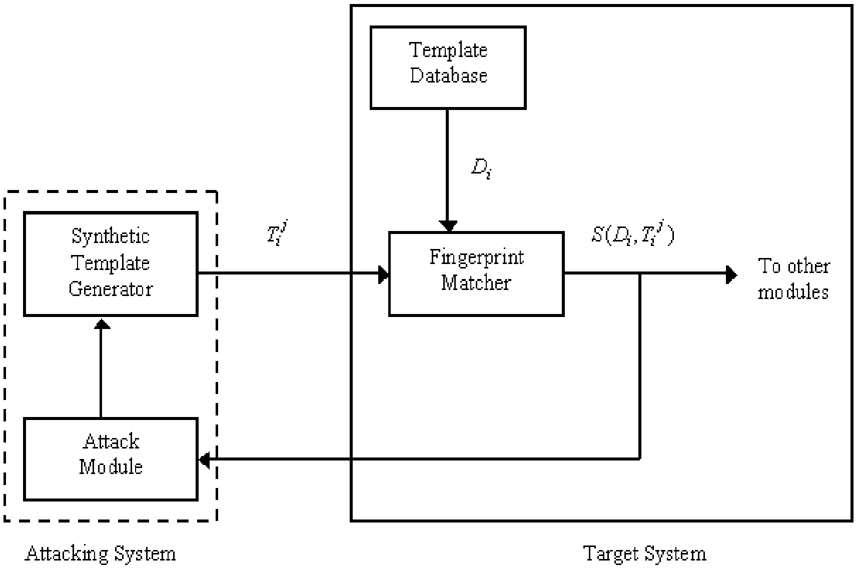

Figure 2 Overview of attack system.

Notations used in this paper are as follows[8]:

D_i : The database template corresponding to user i =1, 2, 3, ..., N , where N is the total number of users registered in the system. It is assumed that the attacking system knows the format of this template, but it cannot access the template itself.

n_i : The total number of minutiae in Di . Note that the attacking system does not know this value.

$T_i^{\ j}$: The synthetic template generated by the attacking system for user i . This template has the same format as database templates where each row represents column index, row index and orientation associated with a minutia; upper left hand subscript denotes the minutiae index, so the total number of minutiae in Tij is nij.

$$T_i^j = \begin{bmatrix} {}^1c_i^j & {}^1r_i^j & {}^1\theta_i^j \\ {}^2c_i^j & {}^2r_i^j & {}^2\theta_i^j \\ \vdots & \vdots & \vdots \\ {}^{n_{ij}}c_i^j & {}^{n_{ij}}r_i^j & {}^{n_{ij}}\theta_i^j \end{bmatrix},$$

S(D_i, T_i^j) : The matching score between Di and Tij.

$S_{\text{threshold}}$: The decision threshold used by the matcher. Note that the attacking system does not know this value.

For attacking a specific user's (i) account, the attacking system follows the following five steps:

- Step 1 (Initial guessing): Generate a fixed number of synthetic templates. In the current implementation, 100 random minutia templates are created.
- Step 2 (Try initial guesses): Attack user i account with the templates generated in Step 1; accumulate the corresponding matching scores.
- Step 3 (Pick the best initial guess): Declare the best guess (T_i^{best}) to be the template resulting in the highest matching score. Declare the best score (S^{best}(D_i)) to be the highest matching score.
- Step 4 (Try modification set): Modify (T_i^{best}) by (i) perturbing an existing minutia, (ii) adding a new minutia, (iii) replacing an existing minutia, and (iv) deleting an existing minutia. If for any one of these

attempts, the matching score is larger than ($S^{best}(D_i)$), declare the modified template as ($S^{best}(D_i)$) accordingly. Else, do not change the parameters of (T_i^{best}).

- Step 5 (Obtaining result): If the current best score is accepted by the matcher namely, (S^{best} (D_i)> $S_{threshold}$) stop the attack; else, go to Step 4.

3. Solutions to Fingerprint Biometric Systems

This section is intended to ensure that common mistakes are avoided and that the deployed system achieves the objectives of convenience, security, and compliance. The successful implementation of a fingerprint biometrics solution involves a continuing process with four fundamental best practices, shown in Figure 3.

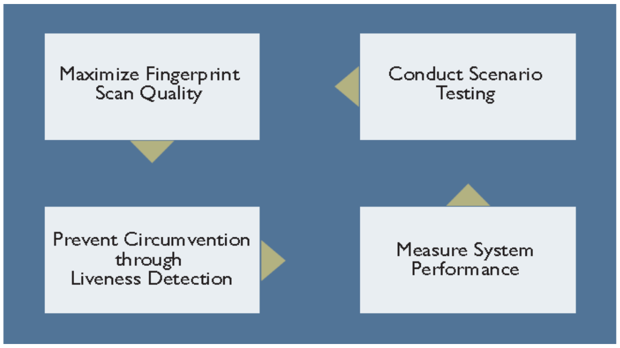
Maximize Fingerprint Scan Quality
Conduct Scenario Testing
Prevent Circumvention through Liveness Detection
Measure System Performance

Figure 3 Solution approaches for Implementing Fingerprint Biometrics in practical[9].

Maximize Fingerprint Scan Quality

Fingerprint scan quality is by far the most important aspect of a fingerprint biometric system design. There is no other single controllable design element that is as important or so poorly understood. There are four interrelated aspects involved:

• **Scanner resolution**—Measurement systems have a resolution limit within which finer or smaller features may not be accurately resolved. Most scanners describe pixel resolution in dots per inch (dpi).

• **Scanner measurement area**—If the scanner measurement area is smaller than the full area of the fingerprint, the amount of biometric data available will be reduced. In addition, when the measurement area is smaller than a complete fingerprint, the placement of the finger effects which subset of features is scanned. While the live scan itself may be high quality, a mismatch is possible between the fingerprint enrolled and the live scan fingerprint.

• **Scanner measurement technology**— Most scanners use one of two measurement methods: semiconductor capacitive or optical total internal reflectance (TIR). These measurement approaches are contact-based and are based on differentiating the areas in contact with the scanner (fingerprint ridges) from areas not in contact (valleys). Other scanners use direct imaging and are immune to contact-related effects. Multispectral scanners are also available which collect subsurface fingerprint detail.

• **Human and environmental factors**—These are a very broad set of issues related to how the user and the user's skin interact with the measurement system under all expected conditions. A high-quality fingerprint scan is a scan that, when passed through an automated biometric feature extractor, yields a large number of true biometric features.

Prevent Circumvention through Liveness Detection

A copy of an authorized person's fingerprint may be used to attempt to bypass a biometrics system. This is analogous to the theft of a password in a conventional identity management system. There are three categories of fingerprint copies and each has a related level of effort and expertise required to make the copy and use it.

Activated latent print—Each time a person touches a scanner, finger oils are left behind along with those of previous users. Normally this composite of users' fingerprints is not useful. However, a clean latent print can be left if the scanner surface is cleaned immediately before use. If the scanner can be triggered to scan this latent print, it is possible to gain fraudulent access.

• **Two-dimensional copies**—A paper copy of a fingerprint can be created from a latent fingerprint lifted from an object such as a glass or a faucet handle. Additionally, in an identity management system that stores fingerprint scans, copies of these prints can be illegitimately accessed and used to print 2-dimensional copies.

• **Three-dimensional copies**—Like 2-dimensinal copies, 3-dimensional copies can be created from latent prints. However, the fingerprint ridge and valley detail are additionally simulated to make a 3-Dimensional copy. Contact-based scanners in particular are susceptible to this form of copying.

Liveness detection or copy protection provides the assurance that a copy of an authorized person's fingerprint cannot be used in the system. Liveness detection can help prevent many of the copy attempts described. Here are some best practices for liveness detection:

- Use scanners with, at minimum, built-in latent and 2-dimensional copy protection.
- Protect electronic copies of fingerprints or simply do not save copies of live or enrollment scans.
- If the potential for fraud is high, use scanners with built-in 3-dimensional copy protection.
- Use a two-factor approach, such as a combination of fingerprint and user ID or fingerprint/credential.
- In addition to built-in protections, consider the use of system-level pattern detection and copy prevention technologies similar to those in use today for password fraud prevention.

Measurement of System Performance

In a fingerprint biometric system, it is important to continuously measure and understand system performance and adjust this performance to meet overall system requirements. To facilitate this, the ability to measure system performance attributes should be part of the overall system design.

Following are the best practices for performance monitoring and tuning:

- Implement a monitoring system that can capture performance information from the system continuously.
- Implement a change management process for all elements of the identity management system and require that each change is proven with scenario testing (see next section) or by monitoring results.
- Measure the single-touch failure rate—the total number of times the single touch of an enrolled user fails to produce a match score greater than the match threshold. This rate includes situations where the scanner does not return a scan (FTA), times out, or rejects an enrolled user (FRR).
- Measure the failure to enroll rate (FTE)—the number of users that cannot use the system reliably and therefore must use an alternate form of authentication.

Conduct Scenario Testing

Scenario testing is a live test of the entire system with a representative set of users conducted under conditions that represent the system deployment environment. This testing is used to characterize the performance of the overall system A sample set of users is enrolled in the system using the enrollment rules that have been selected and verified in the system under representative conditions. This is the first time all the components of the system are used together and system-level performance can be determined[10].

4. Conclusion

Biometric is a unique identity management approach that offers the combination of user convenience, cost effective provisioning and a non- repudiated compliance audit trail for the system operator. After analyzing the feasibility of attacks against fingerprint-based biometric systems, we have shown that the system was able to synthesize templates that guarantee positive identification in a relatively small number of attempts .Even though we proposed several measures to counter such attacks, each has its own limitations, especially for multimodal biometric systems. We need to work on modified attack systems with the aim of decreasing the number of attempts even further.

5. References

1. A.K. Jain, R. Bolle, and S. Pankanti, (Eds.), *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, 2008

2. Frost and Sullivan,(Eds.), A Best practices Guide to Fingerprint Biometric :ensuring a successful biometric implementation.,2012.

3. N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", *Proc. AVBPA 2010, ThirdInternational Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223-228, 2010

4.. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.

5. T. Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned", *Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App.*, pp. 289-303, 2000

6. R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners", *Pattern Recognition*, vol. 36, pp. 383-396, 2008

7. Umut Uludag*, Anil K. Jain*,(Eds.), Attacks on Biometric Systems: A Case Study in Fingerprints http://www.comp.hkbu.edu.hk

8. Biometric- Wikipedia the free encyclopedia http://en.wikipedia.org/wiki/Biometrics

9. Frost and Sullivan,(Eds.), A Best practices Guide to Fingerprint Biometric :ensuring a successful biometric implementation.,2012.
10. John Chirillo, and Scott Blaul(Eds.), Implementing Biometric Security, Wiley Red Books.