Vulnerabilities of Biometric System

Puja Sahay Prasad

Abstract— Biometric security systems are nowadays being introduced in many applications, such as access control, sensitive data protection, on-line tracking systems, etc., due to their advantages over traditional security approaches. Nevertheless, they are also susceptible to external vulnerabilities of biometric systems so that their weaknesses can be found and useful countermeasures against foreseeable attacks can be developed. These attacks are attacks that can decrease their security level. Therefore, it is of the utmost importance to analyse the intended to either avoid the security afforded by the system or to deter the normal functioning of the system. In this paper I describe the various threats that can be catched by a biometric system. I specifically focus on attacks designed to elicit information about the original biometric data of an individual from the stored template Furthermore, I discuss the solution related to the threat.

Index Terms— circumvention, collusion, denial of service, hill climbing attack, masquerade attacks, replay, synthetic template generator.

1 Introduction

Biometrics refers to the automatic identification or identity verification of living persons using their enduring physical or behavioral characteristics. Many body parts, personal characteristics and imaging methods have been suggested and used for biometric systems: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odors. This means that biometrics is the automated approach to authenticate the identity of a person using individual's unique physiological or behavioral characteristics. Since it is based on a unique trait which is part of you, you do not have to worry about forgetting it, losing it or leaving it at some place. Since it is unique to you, it is more difficult for others to copy, duplicate or steal it. Thus in general, biometrics offers a more secure and friendly way of identity authentication [1, 2].Authentication is the act of establishing or confirming something (or someone) as authentic, that is, the claims made by or about the thing are true. In modern approach, Biometric characteristics can be divided in two main classes:

A. Physiological are related to the shape of the body and thus it varies from person to person finger prints, face recognition, hand geometry and iris recognition are some examples of this type of biometric.

B. Behavioural are related to the behaviour of a person. Some examples in this case are signature, key stroke dynamics and voice. Sometimes voice is also considered to be a physiological biometric as it varies from person to person.

1.1 Modes of Operation

A typical biometric system operates in two main modes: Enrolment and Authentication. In the enrolment mode, the system captures the biometric samples from the user and stores the features extracted from the sample in the system database as a biometric template, xE, along with the identity of the user, I. Depending on whether the biometric system is being used for identification or verification, the authentication stage is implemented differently. In a verification system, the user provides his identity, I, along with the biometric sample to the system. The features, xA extracted from the query biometric sample is matched only with the template, xE stored against the claimed identity and the system declares a match if the match score is greater than the system threshold and declares a non-match, otherwise.

In an identification system, the user provides only the biometric sample to the system without claiming any identity during authentication. The query thus acquired by the system is matched with all the templates stored in the system database. If one of the templates in the database matches the query, a match is declared; otherwise the system declares a non-match.

While a biometric system can enhance user convenience and provide security, it is also vulnerable to various types of threats as discussed below [2, 3].

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/he 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.).

Privacy attack: Attacker accesses the data that she/he was not authorized (e.g., accessing the medical records of another user).

Subversive attack: Attacker manipulates the system (e.g., submitting bogus insurance claims).

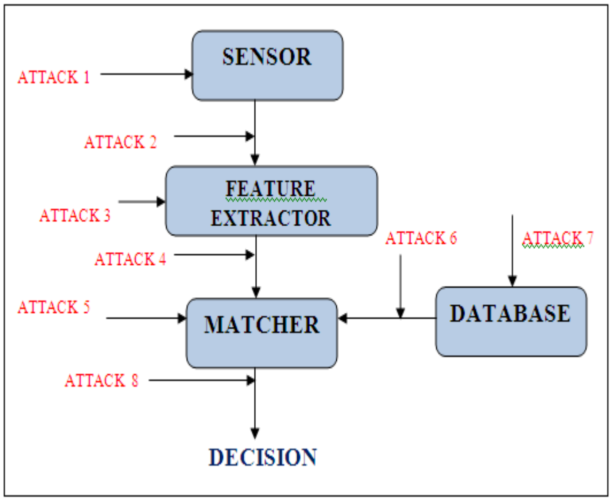
Repudiation: In repudiation, the attacker denies accessing the system. For example, a corrupt bank clerk who modifies some financial records illegally may claim hat her biometric data was "stolen", or she can argue that the False Accept Rate (FAR) phenomenon associated with any biometric may have been the cause of the problem.

Contamination (covert acquisition): 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

- *Puja Sahay Prasad is currently lecturer at Rajiv Gandhi College of Engineering & Research, Nagpur, India, and pursuing Ph.D. in Computer Science &Engineering from Banasthali Vidyapith, India, PH-91-9028005541. E-mail:puja.s.prasad@gmail.com*

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.). coercion, attackers force the legitimate users to access the system (e.g., using a fingerprint to access ATM accounts at a gunpoint) [5].
Collusion: A user with wide super user privileges (e.g., system administrator) illegally modifies the system.
Coercion: An attacker forces a legitimate user to access the system (e.g., using a fingerprint to access ATM at a gunpoint).
Denial of Service (DoS): An attacker corrupts the biometric system so that legitimate users cannot use it
A server that processes access requests can be bombarded with many bogus access requests, to the point where the server's computational resources can not handle valid requests any more. The above threats that lead to such security lapses typically belong to one of the following four categories: intrinsic failures, administrative privileges, non-secure infrastructure and access to biometric data.

2. ATTACKS AGAINST BIOMETRIC SYSTEMS



ATTACK 1 A fake biometric trait such as an artificial
Finger may be presented at the sensor. In this case no
A detailed system knowledge or access privilege is
necessary.
ATTACK2 Bypass Sensor-illegally intercepted data may be resubmitted to the system.
ATTACK3 The feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets.
ATTACK4 Legitimate feature sets may be replaced with synthetic feature sets.
ATTACK5 The matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security.
ATTACK 6 The templates stored in the database may be modified or removed, or new templates may be introduced in the database.
ATTACK7 The data in the communication channel between various modules of the system may be altered and the last
ATTACK 8 the final decision output by the biometric system may be overridden.

3. COMPROMISING BIOMETRIC INFORMATION

The failure modes of a biometric system can be categorized into two classes:
Intrinsic failure: Intrinsic failures occur due to inherent limitations in the sensing, feature extraction, or matching technologies as well as the limited discriminability of the specific biometric trait.
Adversary attack: In adversary attacks, a resourceful hacker (or possibly an organized group) attempts to circumvent the biometric system for personal gains. There are list of attacks that compromises biometric information.

3.1 Hill-climbing attacks

A hill-climbing attack may be performed by an application that sends random templates to the system, which are perturbed iteratively. The application reads the output match score and continues with the perturbed template only when the matching score increases until the decision threshold is exceeded. Adler demonstrated that a face image can be regenerated from a face template using a "Hill Climbing Attack" (attack level 2 in Figure 1). He employed an iterative scheme to reconstruct a face image using a face verification system that releases match scores. The algorithm first selects an estimate of the target face from a local database comprising of a few frontal images by observing the match score corresponding to each image. An Eigen-face (computed from the local database) scaled by 6 different constants is added to this initial estimate resulting in a set of 6 modified face images which are then presented to the verification system. The image resulting in an improved match score is retained and this process is repeated in an iterative fashion. Within a few thousand iterations, an image that can successfully masquerade as the target face image is generated. The important feature of this algorithm is that it does not require any knowledge of either the matching technique or the structure of the template used by the authentication system. Furthermore, template encryption does not prevent this algorithm from successfully determining the original face image. The algorithm was able to "break" three commercial face recognition systems.

3.2 Synthetic Biometric Submission

In synthetic fingerprint submission no detailed system knowledge or access privileges is necessary. Digital protection mechanisms (e.g., encryption) are also not applicable. Ulu dag and Jain [4] devised a synthetic template generator (STG) that also uses the "Hill Climbing Attack" (attack level 4 in Figure 1) to determine the contents of a target fingerprint template (Di) for the i^{th} user. The minutiae template is assumed to be a sequence of (r;c;q) values representing the location and orientation of component fingerprint minutiae. The STG begins by generating a fixed number of synthetic templates each comprising of randomly generated minutiae points. These templates are compared against the target template in the database (via the matcher) and the synthetic template resulting in the best match score is retained. The retained template is then modified iteratively via the following four operations: (i) the r, c and q values of an existing minutia are perturbed, (ii) an existing minutia is replaced with a new minutia, (iii) a new minutia is added to the template, and (iv) an existing minutia is deleted. The modified template (T_{ij}) is compared against the target template and the match score (S (D_i; T_{ij})) computed. This process, viz., modifying the current synthetic template and comparing it against the target template, is repeated until the match score exceeds a pre-determined threshold. The authors used this scheme to break into 160 fingerprint accounts; their algorithm required only 271 iterations, on an average, to exceed the matching threshold for each one of those 160.

3.3 Masquerade Attacks

Hill [7] describes a masquerade attack wherein the fingerprint structure is determined using the minutiae template alone (attack level 7 in Figure 1). It is assumed that each minutia point is characterized using its 2D location, orientation and the curvature of the ridge associated with it. Based on minutiae points, the author predicts the shape of the fingerprint (i.e., its class) using a neural network classifier consisting of 23 input neurons, 13 hidden neurons and 4 output neurons (corresponding to 4 fingerprint classes).

3.4 Denial of Service (DoS)

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.

4. Solutions to Biometric Attacks

A number of specific hardware and software solutions have been proposed to protect biometric templates. The hardware solutions mainly involve designing a "closed" recognition system, where the template never leaves a physically secure module and thus cannot be inverted or linked. An example of such a solution is a commercial product called privaris Plus ID [2]. In this product, the complete biometric system including the biometric sensor is encased in a keyfob-sized device. During enrolment, the device generates a template from the biometric sample captured from the user and stores it inside the device. And during authentication, if the query captured from the user matches with the stored template, the device transmits a key to, say, an access control system (e.g., a garage door) that can open or close based on the key it receives. A common name for similar devices is "system on card". Another similar system, called "match on card" hosts a template database and the matcher inside a small physically secure module where, during authentication, the biometric captured by an external entity is sent to the system for matching. One of the main limitations of the hardware based solutions is that they are expensive and inconvenient mainly because a user has to carry them and are prone to being lost. Similarly there are few lists that reflects the solution-

4.1 Fingerprint Liveness Detection

There are various Software-based systems that detect the liveness of the fingerprint.

Static in which we mark periodicity of sweat pores along the ridges.

Dynamic in which sweat diffusion pattern along the ridges over time to time mark

For liveness detection there is liveness detection module which is 5 sec video of the finger

4.2 Eliminate Replay

A challenge-response based system guarantees that image is really coming from the fingerprint sensor (i.e., the attacker has not bypassed the sensor):

Server generates a pseudo-random challenge after transaction gets initiated by the client. Secure server sends the challenge to intelligent sensor .The sensor acqituires the fingerprint image and computes the response to the challenge .The challenge can be the checksum of a segment of the image, a set of samples from the image, etc. The response and the sensed image are sent to the server. The validity of response/image pair is checked.

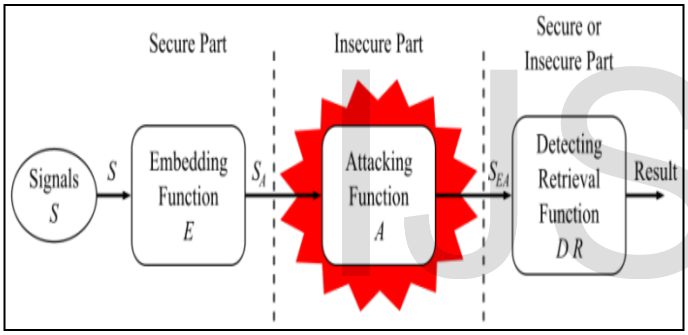
4.3 Eliminate Hill-Climbing

In a hill climbing attack the attacker essentially implements an iterative optimization algorithm to recover the original template where the fitness function is determined by the matching score between the transformed version of the current estimate of the original biometric and the stored template. It does not reveal the actual matching scores; only reveal a coarsely quantized version. This may render the hill-climbing based attack infeasible or impossible.

4.4 Watermarking Techniques

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system [7] is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.



Jain and Uludag [4] worked with hiding fingerprint minutiae in images. For this purpose, they considered two application scenarios: A set of fingerprint minutiae is transferred as the watermark of an arbitrary image and a face image is watermarked with fingerprint minutiae. In the first scenario, the fingerprint minutiae are transferred via a non-secure channel hidden in an arbitrary image. Before being embedded into the host image, the fingerprint minutiae are encrypted, which further increases the security of the data. The produced image is sent through the insecure communication channel. In the end, the image is received and the fingerprint minutiae are extracted, decrypted and ready for any further processing. In the second scenario, a face scan is watermarked with fingerprint minutiae data and the result is encoded in a smart card. For the authentication of a user, the image is retrieved from the smart card, the fingerprint minutiae are extracted from it and they are compared to the minutiae obtained from the user online. The user is authenticated based on the two fingerprint minutiae data sets and the face image. Jain et al. [4] have presented a fingerprint image watermarking method that facial information into host fingerprint images. The considered application scenario in this case is as follows: The fingerprint image of a person is watermarked with face information of the same person and stored on a smart card. At an access control site, the fingerprint of the user is sensed and compared with the one stored on the smart card. After the fingerprint matching has successfully been completed, the facial information can be extracted from the fingerprint image on the smart card and can be used for further authentication purposes.

5. Conclusions

Biometrics offers a valuable approach to extending current security technologies that make it far harder for fraud to take place by preventing ready impersonation of the authorized user. However, in order to make use of biometrics we need to register users, a procedure that may be costly, and onerous for users, and we have to have a socially/culturally acceptable means of checking the biometric at the point of authentication. These problems may also give rise to the need for safeguards over the use of the biometric. In using biometrics we must be aware of the fact that they are not measuring perfectly, and that many operational factors may cause them to fail. In such cases administrative procedures to resolve operational failures may need to be put in place to prevent adverse customer reaction, bad publicity and failures in public acceptability. Whilst these failures may not represent a significant proportion of transactions they will have a 'publicity' effect that is far more damaging that all the success gained by the service. Insufficient information from extensive pilot studies exists at the moment to indicate either how best to manage the situation or tune the service to give acceptable financial or anti-fraud results.

REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP*, vol. 8, no. 2, pp. 1–17, 2008.
[2]. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: a tool for information security. *IEEE Trans. on Information Forensics and Security* 1, 125–143 (2006)
[3] *Smart Cart Alliance Identity Council* (2007): Identity and Smart Card Technology and Application Glossary,
[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer-Verlag, 2003.
[5] U. Uludag and A. K. Jain, "Attacks on biometric systems:a case study in fingerprints," in *Proc. SPIE, Security,Seganography and Watermarking of Multimedia Contents VI*, vol. 5306, pp. 622–633, (San Jose, CA),January 2004.
[6] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis", *http://www.smartcardalliance.org*, as visited on 25/10/2008.