An Analysis on Biometric Template Protection Schemes

Miss. Ashwini N. Ingle[1] Dr. G. R. Bamnote[2]
[1]ME student [2]Head of Department
[1,2]Department of Computer Science & Engineering
[1,2]Prof. Ram Meghe Institute of Technology Research, Badnera, India

Abstract— A biometric authentication system operates by getting raw biometric data from a user e.g., fingerprint and iris images. This paper summarizes the various aspects of biometric system security. It broadly classify the various factors that cause biometric system failure and identify the effects of such failures. In this system, biometric templates are stored in central database. Preserving the privacy of this digital biometric template has become very important. The main focus of this paper is on Biometric template security. It also provides a high-level classification of the attacks on biometric templates and a detail overview of different template protection approaches that have been proposed in the literature.

Key words: Authentication, Biometric Templates, Steganography, Watermarking

I. INTRODUCTION

Establishing the identity of an individual is very importance in several civilian and government applications such as ATMs, access to nuclear facilities, airport security, issuance of passports or driver licenses, etc. BIOMETRICS-BASED identification technique is a reliable and convenient way for person authentication. It uses physiological or behavioral characteristics of individuals and is becoming increasingly popular compared to traditional token-based or knowledge-based techniques such as identification cards (ID), passwords, etc.

Traditionally, token-based security such as ID cards and knowledge-based security such as Pins/Passwords has been used to verify the identity of an individual. These techniques suffer from several limitations. Passwords and PINs can be illegally acquired by secret observation. Once an intruder acquires the user ID and the password, he has total access to the user's resources. In addition, there is no way to verify that the system or service is used by the actual user, that is, there is no protection against repudiation by the user ID owner. Conditions are similar when a transaction involving a credit card number is conducted on the web. Even though the data are transmited using secure encryption methods, present systems are incapable of assuring that the transaction was initiated by the rightful owner of the credit card.

In the modern distributed systems environment, the authentication policy operates on a simple combination of username and password has become Biometric recognition is the science of establishing the identity of a person using his/her physical and behavioral traits. Commonly used biometric traits include fingerprint, face, iris, hand geometry, voice and palm print. Biometric traits have a number of desirable properties. They are reliable because of their uniqueness. They are also convenient and universal, and therefore very useful for biometric authentication system. a generic biometric authentication system havefive major components system, namely, sensor, feature extractor, template database, matcher, and decision module (see Figure 1&2). Sensor is the interface between the user and the authentication system that scan the biometric features of the user. Feature extraction module used the scanned biometric data to extract the prominent information (feature set) that is useful in distinguishing between different users. During enrollment, scan information of user is stored in a database as a template. Since the template database could be geographically distributed and contain thousands of records, maintaining its security is very important. The matcher module match the biometric feature sets from template and query, respectively, as inputs, and outputs a match score indicating the similarity between the two sets. Finally, the decision module takes the identity decision and initiates a response to the query.

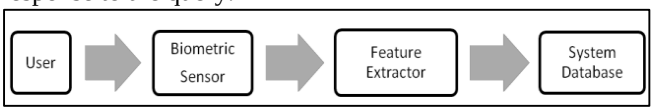

Fig. 1: Enrollment

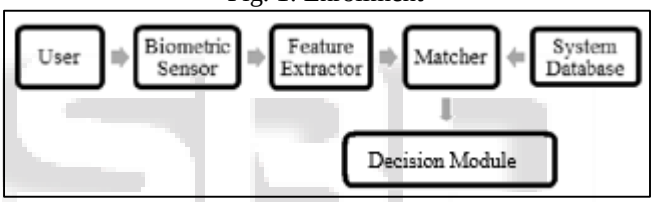

Fig. 2: Authentication

Now a day, biometric systems are becoming affordable and are easily embedded in a variety of consumer devices (e.g., mobile phones, laptops, etc.). Thus, this technology has become vulnerable to the harmful designs of terrorists and criminals. This paper summarizes the various aspects of biometric system security. In section 2, it broadly categorizes the various factors that cause biometric system failure and identify the effects of such failures. This paper is not necessarily complete in terms of all the security threats that have been identified, but it provides a high-level classification of the possible security threats. Template security is one of the most crucial issues in designing a secure biometric system and section 3 of paper focuses on major attacks on this system. A detailed overview of different template protection approaches that have been proposed in the literature is presented in section 4, whereas, section 5presents a discussion on this approaches based on advantages and disadvantages

II. FACTORS & THREATS IN BIOMETRIC SYSTEM

A. Factors for Biometric System Failures:

A biometric system can be broadly categorized into two classes: Internal and External factors.

1) Internal Factors:

Intrinsic failures occur due to inbuilt limitations in the sensing, feature extraction, or matching technologies as well as the limited discrimination of the specific biometric feature.

2) External Factors:
Extrinsic factors may occurs due to resourceful hackers can covertly acquire the biometric characteristics of a genuine user, improper administration in biometric system, insecure hardware, software, and the communication channels between the various modules,.

B. Threats in Biometric System:

A biometric System is susceptible to various types of threats as discussed below [3,4].

1) Circumvention:
An intruder may gain access to the system protected by biometrics and peruse sensitive data such as medical records pertaining to a legitimately enrolled user. He can violate the privacy of the enrolled user and can also modify sensitive data.

2) Repudiation:
A legitimate user may access the facilities offered by an application and then claim that an intruder had circumvented the tem.

3) Covert acquisition:
An intruder may surreptitiously obtain the raw biometric data of a user to access the system.

4) Conspiracy:
An individual with wide super-user privileges (such as an administrator) may deliberately modify system parameters to permit incursions by an intruder.

5) Coercion:
An impostor may force a legitimate user (e.g., at gunpoint) to grant him access to the system.

6) Denial of Service (DoS):
An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service.

III. MAJOR ATTACKS ON BIOMETRIC TEMPLATE

A template represents a set of prominent features that summarizes the biometric data of a person. Due to its compact nature, it is commonly assumed that the template cannot be used to extract complete information about the original biometric signal. Furthermore, since the templates are typically stored in an encrypted form, it is substantially difficult to decrypt and determine the contents of the stored template (without the knowledge of correct decrypting keys). Thus, traditionally, template-generating algorithms have been viewed as one-way algorithms. However, in the recent literature there have been techniques presented that contradict these assumptions.

Adler [6] demonstrated that a face image can be regenerated from a face template using a "Hill Climbing Attack". 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 in a set estimate resulting of 6 modified face images. These modified images are then presented to the verification system. The image that has improved match score is retained and this process is repeated in an iterative fashion. 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.

Uludag and Jain [4] developed a synthetic template generator (STG) that also uses the "Hill Climbing Attack" to determine the contents of a target fingerprint template (Di) for the ith user (see Fig.3). 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 (Tij) is compared against the target template and the match score (S(Di;Tij)) 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 accounts.

Hill [7] describes a masquerade attack wherein the fingerprint structure is determined using the minutiae template alone. 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. However, the classification performance is rather low (an error rate of 28:9% on a small set of 242 fingerprints). The author then uses a generic orientation map and the minutiae information to generate line drawings that are a digital artifact of the original fingerprint. The proposed technique is observed to work on a database of 25 fingerprints from arch class.

Ross et al. [8] propose another technique to obtain the fingerprint structure from the minutiae template. Each minutia is assumed to be represented by its 2D spatial

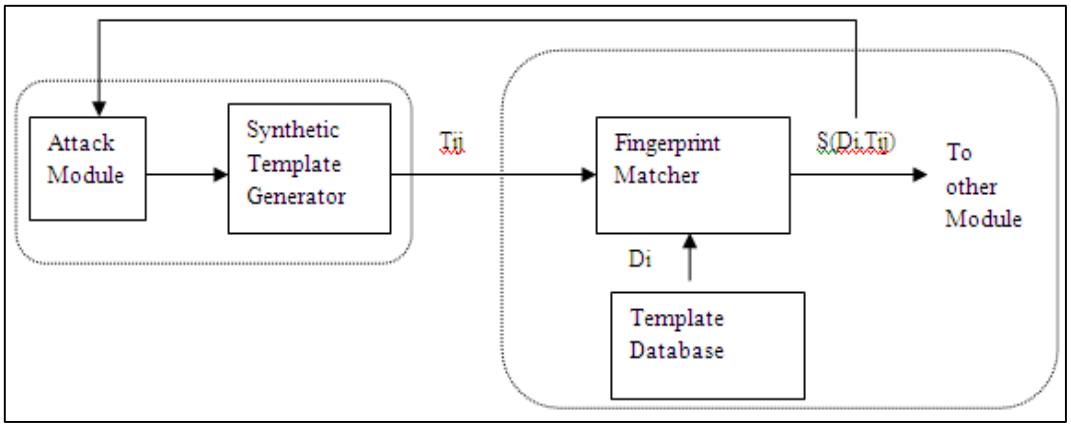

Fig. 3: Algorithm to synthesize minutiae templates

Location and its local orientation. The authors identify minutia triplets which are used to estimate the underlying orientation map. The estimated orientation map is observed to be remarkably consistent with the flow of ridges in the original (unseen) parent fingerprint. Furthermore, they use a set of 11 features derived from the minutiae points to predict the class of the fingerprint. A 5 Nearest Neighbor classifier is used to classify the minutiae set of a fingerprint into one of four classes, viz., arch (A), tented arch (T), right loop (R), left loop (L) and whorl (W). Alternately, the T and A classes may be combined into one single class resulting in four classes.

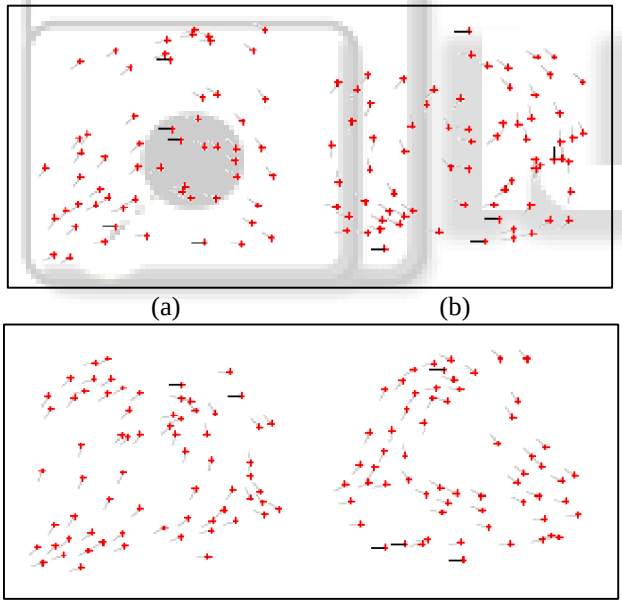

Fig. 4: Minutiae distributions of 4 fingerprint classes: (a) A, (b) W, (c) L, and (d) R.

Besides these types of attacks, an intruder may alter the contents of a template in order to deter a legitimate user from being successfully verified.

IV. BIOMETRIC TEMPLATE PROTECTION APPROACHES

Several methods have been suggested in the literature to protect biometric templates from revealing important information. In order to prevent the action of Hill-Climbing Attack, Soutar [10] has suggested the use of coarsely quantized match scores by the matcher. However, Adler 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 [12] describe an invisible fragile watermarking technique to detect regions in a fingerprint image that have been altered by an attacker. In the proposed scheme, a disorganized mixing procedure is employed to transform a visually noticeable 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 presence of the watermark does not affect the feature extraction process. The copyright capability can also be revealed with the use of watermarks by identifying the origin of the raw fingerprint image.

Jain and Uludag [13] 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. Implanting biometric data in a safe host image prevents an eavesdropper from accessing sensitive template information. A novel application wherein the facial features of a user (i.e., eigen-coefficients) are embedded in a host fingerprint image (of the user) is also discussed. In this scenario, the watermarked fingerprint image of a person may be stored in a smart card issued to that individual. 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. [14] propose an algorithm to embed dynamic signature features into face images present on ID cards. These features are altered into a binary stream after compression. 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 characteristics hidden in the face image are recovered and compared against the signature obtained on-line. Ferri et al. report that any modification in the face image can be detected. Therefore, the use of fake ID cards can be detected and disallowed.

Ratha et al.[15] 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 revises 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 creating a new one. This also allows 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 biometric cryptosystems are gaining popularity (for a survey on existing techniques, see [16]). These systems combine biometrics and cryptography at a level that allows biometric matching to effectively take place in the cryptographic domain, hence increasing the security. For example, Uludag et al. [17] 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. When matching minutiae data from an input fingerprint is available then the template data is identified. The system is observed to operate at a Genuine Accept Rate (GAR) of 76% with no false accepts on a database comprising of 229 users.

Arun Ross and Asem Othman [1], explores the possibility of using visual cryptography for imparting privacy to biometric data. They applied visual cryptography by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image. During the enrollment process, the private biometric data is sent to a trusted third-party entity. Once the trusted entity receives it, the biometric data is divided into two images and the original data is discarded. These images are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server. During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the private image.

Although several techniques have been proposed to enhance the security of a user's template, government regulations will also have to be established in order to address the issue of template privacy. For example, issues related to the sharing of biometric templates across agencies (e.g., medical companies and law-enforcement agencies) and the inferring of personal information about an enrolled user from biometric data (e.g., "Is this person having cancer?") have to be countered by establishing an appropriate legal framework.

V. Summary & Conclusion

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 privileged 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. Visual Cryptography may be applied to avoid any complicated decryption and decoding computations that are used in watermarking [12], [15], steganography [13], or cryptosystem [16] approaches.

References

[1] Arun Ross and Asem Othman, "Visual Cryptography for Biometric Privacy", IEEE Transaction on Information Forensic and Security, vol. 6, no. 1, March 2011.
[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006.
[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer-Verlag, 2003.
[4] U. Uludag and A. K. Jain, "Attacks on biometric systems:a case study in fingerprints," in Proc. SPIE, Security, Seganography and Watermarking of Multimedia.
[5] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in Proc. Audio and Video-based Biometric Person Authentication (AVBPA), pp. 223–228, (Halmstad, Sweden), June 2001.
[6] A. Adler, "Can images be regenerated from biometric templates?," in Biometrics Consortium Conference, (Arlington, VA), September 2003.
[7] C. J. Hill, "Risk of masquerade arising from the storage of biometrics," B.S. Thesis, Australian National University, November 2001, http://chris.fornax.net/biometrics.html.
[8] A. Ross, J. Shah, and A. K. Jain, "Towards reconstructing fingerprints from minutiae points," in Proc. SPIE, Biometric Technology for Human Identification II, vol. 5779, pp. 68–80, (Orlando, FL), March 2005.
[9] R. Cappelli, R. Erol, D. Maio, and D. Maltoni, "Synthetic fingerprint-image generation," in Proc. Int'l. Conf. Pattern Recognition (ICPR), vol. 3, pp. 475–478, (Barcelona, Spain), September 2000.
[10] C. Soutar, "Biometric system security," White Paper, Bioscrypt, http://www.bioscrypt.com.
[11] 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.
[12] 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.
[13] A. K. Jain and U. Uludag, "Hiding biometric data," IEEE Trans. Pattern Anal. Mach. Intelligence, vol. 25, no. 11, pp. 1493–1498, 2003.
[14] 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), January 2002.
[15] 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.
[16] 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.
[17] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," To appear in Proc. Audio- and Videobased Biometric Person Authentication (AVBPA), (Rye Brook, NY), July 2005.
[18] J. Dong and T. Tan, "Effects of watermarking on iris recognition performance," in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008 (ICARCV 2008), 2008, pp. 1156–1161.
[19] N. Agrawal and M. Savvides, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching," in Proc. Computer Vision and Pattern Recognition Workshop, 2009, vol. 0, pp. 85–92.
[20] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Advances Signal Process., pp. 1–17, 2008.
[21] Naor .M and Shamir .A, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
[22] Maltoni.D, Maio.D, Jain .A, and Prabhakar .S, Handbook of Fingerprint Recognition. Secaucus, NJ: Springer-Verlag New York, Inc., 2003.

