ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 9, March 2014

Biometric Security

Pravin Sonsare
Shri Ramdeobaba College of Engineering and Management, Nagpur

***Abstract*— A biometric system is vulnerable to a variety of attacks aimed at undermining the integrity of the authentication process. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system. With the wide spread utilization of biometric identification systems, establishing the authenticity of biometric data itself has emerged as an important research issue. The fact that biometric data is not replaceable and is not secret, combined with the existence of several types of attacks that are possible in a biometric system, make the issue of security/integrity of biometric data extremely critical. In this paper we discuss methods to hide biometric data.**

***Index Terms*— Biometrics, steganography, watermarking, encryption, SVM.DWT.**

I. INTRODUCTION

Biometrics is the science of establishing or determining an identity based on the physiological or behavioral traits of an individual. These traits include fingerprints, facial features, iris, hand geometry, voice, signature, etc. In conjunction with traditional authentication schemes, biometrics is a potent tool for establishing identity [1].

Traditional token-based or knowledge-based personal identification techniques are unable to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person. Biometrics technology is based on using physiological or behavioral characteristics in personal identification, and can easily differentiate between an authorized person and a fraudulent impostor. While the biometrics techniques offer a reliable method for personal identification, the problem of security and integrity of the biometrics data poses new issues. For example, if a person's biometric data (e.g., his/her fingerprint image or fingerprint features) is stolen, it is not possible to replace it as compared to replacing a stolen credit card, ID or password [2].

Encryption, steganography and watermarking are possible techniques to increase security of the biometric data. Encryption attempts to make the biometric information meaningless to attackers. Once the data is decrypted, the encryption does not provide any security. Both Steganography and watermarking pertain to the area of data hiding, which aims at private information protection by hiding critical information in unsuspected carrier signal. Steganography is introduced to embed secret biometric data into host signal without suspicion during transmission (hence protect the biometric data), while watermarking helps to detect the tempered biometric data for integrity authentication [3].

In this paper, we discuss biometric module, various attacks, and various techniques for security of biometric data. Section I briefly introduces biometrics, watermarking, steganography and encryption. Section II presents biometric module and various attacks. Various techniques regarding biometric security reported in Section III and concluding remarks is given in the Section IV.

II. BIOMETRIC MODULE AND ATTACKS

A typical biometric system comprises of several modules. The sensor module acquires the raw biometric data of an individual in the form of an image, video, audio or some other signal. The feature extraction module operates on the biometric signal and extracts a salient set of features to represent the signal; during user enrolment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a template. The matching module compares the feature set extracted during authentication with the enrolled template(s) and generates match scores. The decision module processes these match scores in order to either determine or verify the identity of an individual. Thus, a biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into one of several identities (viz., identification) or into one of two classes - genuine and impostor users (viz., verification) [1].While a biometric system can enhance user convenience and bolster security, it is also susceptible to various types of threats as discussed below [4, 5].

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. Besides violating the privacy of the enrolled user, the impostor 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 system. A bank clerk, for example, may modify the financial records of a customer and then deny responsibility by claiming that an intruder could have possibly stolen her biometric data.

3. *Covert acquisition*: An intruder may surreptitiously obtain the raw biometric data of a user to access the system. For example, the latent fingerprints of a user may be lifted from an object by an intruder and later used to construct a digital or physical artifact of that user's finger.

4. *Collusion*: 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.

Denial of Service (DoS): An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service. For example, a server that processes access requests can be flooded with a large number of bogus requests, thereby overloading its computational resources and preventing valid requests from being processed.

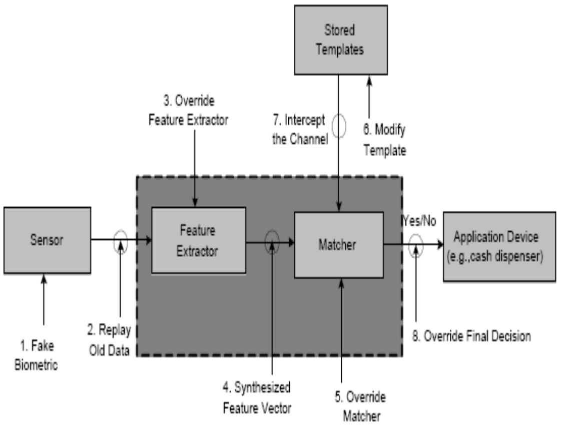

Fig1: Biometric module

In the first type of attack, a fake biometric (such as a fake finger) is presented at the sensor. Resubmission of digitally stored biometric data constitutes the second type of attack. In the third type of attack, the feature detector could be forced to produce feature values chosen by the attacker, instead of the actual values generated from the data obtained from the sensor. In the fourth type of attack, the features extracted using the data obtained from the sensor are replaced with a synthetic feature set. In the fifth type of attack, the matcher component could be attacked to produce high or low matching scores, regardless of the input feature set. Attack on the templates stored in databases is the sixth type of attack. In the seventh type of attack, the channel between the database and matcher could be compromised to alter transferred template information. The final type of attack includes altering the matching result itself. All of these attacks have the possibility to decrease the credibility of a biometric system [6][7].

III. TECHNIQUES REGARDING BIOMETRIC SECURITY

A. Watermarking Techniques

Digital watermarking, or simply watermarking, which is defined as embedding information such as origin, destination, access level, etc. of multimedia data (e.g., image, video, audio, etc.) in the host data, has been a very active research area in recent years [8]. General image watermarking methods can be divided into two groups according to the domain of application of watermarking. In spatial domain methods (e.g., [9]), the pixel values in the image channel(s) are changed. In spectral-transform domain methods, a watermark signal is added to the host image in a transform domain such as the full-frame DCT domain [10]. The extent to which the artifacts of a watermarked image can be tolerated by a recognition system depends upon the combination of (i) characteristics of the noise introduced by the watermarking algorithm and (ii) the design of the recognition system. In order to appreciate what kinds of artifacts could be tolerated by a fingerprint-based identification system, one need to study the details of the design of that particular system [11]. A digital watermark can be a string of binary bits or can be a logo, seal or trademark that is used to display ownership.

The watermarking technique consists of (1) the watermark insertion, and the (2) watermark extraction. The extracted watermark is then used for verification of image content to detect unauthorized alteration or tampering. In the watermark insertion process, a watermark image, W(i,j), is embedded into the source image, I(i ,j),to produce a watermarked image I’(i,j. Each pixel in the source image is processed in turn. The processing applies a watermark extraction function WX(*) to the selected pixel I(i,j), and tests the extracted binary watermark value b(i,j) to determine whether it is equal to the desired watermark value W(i,j). If the embedded and extracted watermarks are equal, the processing proceeds to the next pixel. If they are not equal, the value of the selected pixel is modified until the value of the extracted watermark is equal to the desired value [11].

It is advantageous to develop embedding schemes such that the image patterns embedded are not only visually invisible, but also more robust against attacks and recognition failures. Preferably, it should be difficult, if not impossible, for an interloper to decide whether an image has been watermarked or not, what and where the information is embedded, such that he or she cannot re-apply the watermark after an alteration to fool the verification process. In the case of monochrome 8-bit images, only one table of 256 entries is necessary for decoding the watermark and this reduces the difficulty of attack. In this regard, we apply some forms of chaotic mixing on the watermarked images to transform a visually pleasant into unrecognizable forms (structured noise), but still retain the advantage of using visual patterns which can be recovered after inverse transformation. By mixing the watermark to a random-textured pattern, watermarking of monochrome images can be made more resilient against attacks. This is especially valuable in watermarking fingerprint images most of which are captured in monochrome gray scales.

Rein-Lein Hsu[2] proposed data hiding method, novel watermarking method for fingerprint images, in which we embed facial information into fingerprints, is described. The watermark data, which consists of the eigen-face coefficients of a user’s face, can be used in authenticating the host fingerprint image. The data is hidden in such a way that the fingerprint features that are used in matching are not significantly changed during encoding/decoding. As a consequence, the verification accuracy based on decoded watermarked fingerprint images is very similar to that with original fingerprint images. The robustness of the method against several possible attacks on watermarked images helps in authentication of attacked images.

We discuss wavelet-based watermarking method for fingerprint images and this method can be used in steganography-based application to embed minutiae data in fingerprint images. The use of a biometric data (fingerprint image) to hide another one (fingerprint minutiae) increases the level of security because the unauthorized person who obtains the fingerprint image watermarked is likely to treat the fingerprint image instead the hidden minutiae data. The method used to embed the watermark is an extension of the method proposed by Kundur and Hatzinakos [13] who proposed to embed the watermark in the coefficients of the discrete wavelet transform (DWT) using quantization-based watermarking proposed by Chen and Wornell [14]. We propose to embed the watermark three times in the details coefficients of the highest level discrete wavelet transform of the host image (i.e. fingerprint image). This redundancy of embedding increases the correct extraction rate of the hidden data (i.e. minutiae data). This method doesn't require the original image to extract the embedded minutiae. The introduced method is highly robust to compression and additive noise and quite resilient to moderate linear mean filtering. Future work will be concentrate on making the method more robust to attacks [12].

Mayank Vasta [15] proposed biometric watermarking algorithm for improving the recognition accuracy and protecting the biometric images from tampering. Multi-resolution Discrete Wavelet Transform is used for embedding the face image in fingerprint image. An intelligent learning algorithm based on Support Vector Machine (SVM) is introduced to enhance the quality of the extracted face image. The performance of the watermarking algorithm is experimentally validated using existing fingerprint and face recognition algorithm. he result show that the extracted fingerprint and face images are of high quality. The use of SVM enhance the performance of face recognition by at least 10% even when watermarked image is subjected to certain geometric and frequency attacks such as scaling, cropping, compression and filtering. SVM-based algorithm use to select the best quality pixels from two extracted face images to generate a high quality image.

B. Steganography Technique

Steganography involves hiding critical information in unsuspected carrier data. As a result, steganography-based techniques is suitable for transferring critical biometric information from a client to a server, hence reducing the chances of being intercepted by a pirate and illegal modification of the biometric data. Wang Na [3] proposed, iris feature or iris code will be used as secret information, and the proposed secure framework based on steganography is shown in Fig.2.Biometric image is captured from the sensor and image processing algorithms are performed to extract the features. These data are unique for different person and converted into a binary stream to generate the iris code. The hiding and extracting module separately implement the two steps, hiding and extracting iris information. In the matching phase, the matcher module evaluates the scores by matching the data acquired with the database. There are many algorithms to extract iris feature in the literature [16, 17]. Without loss of generality, we assume that good iris codes are obtainable with modified 2D Gabor filter, and we focus on the established of the steganography-based framework

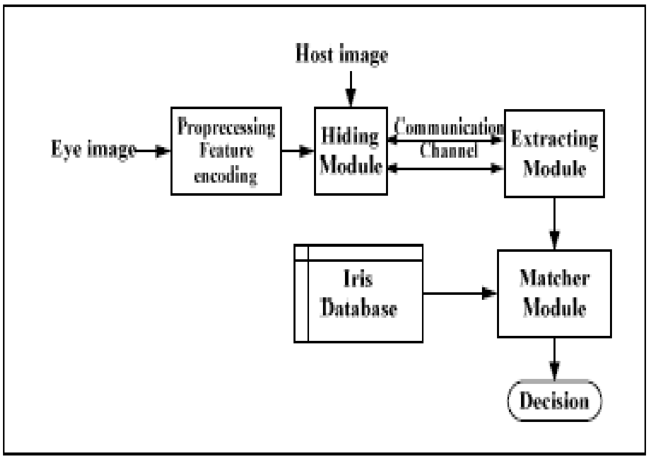

Fig 2. Iris-based recognizing system combining steganography

IV.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. Also, biometric cryptosystems can contribute to template security by supporting biometric matching in secure cryptographic domains. Smart cards are gaining popularity as the medium for storing biometric templates. As the amount of available memory increases (e.g., state-of-the-art smart cards have 64-KByte EEPROM), there is a propensity to store more information in the template. This increases the risks associated with template misuse. As a result, the issue of template security and integrity continues to pose several challenges, and it is necessary that further research be conducted in this direction.

Table1.Comparision table of data hiding technique

Technique	Description
1.Digital Watermarking	Embedding information of multimedia data (e.g., image, video, audio, etc.) in the host data
2.Fragile Watermarking	The watermark insertion and extraction

3.Chaotic Watermarking	By mixing the watermark to a random-textured pattern
4.Amplitude Modulation base Watermarking	Include image adaptivity ,minutiae analysis, watermark strength controller along with basic method
5.Wavelet-based Watermarking method	Embed the watermark in the coefficients of the discrete wavelet transform (DWT) using quantization-based watermarking
6.DWT and SVM Watermarking	Enhance the quality of extracted face image
7.Steganography	Hiding critical information in unsuspected carrier data

REFERENCES

[1] A. K. Jain, A. Ross, and U. Uludag, "Biometric template security: challenges and solutions," Proc. of the European Signal Processing Conference (EUSIPCO '05), Sep.2005.

[2] A.K.Jain, U.Uludag, and R.K.Hsu, “Hiding a face in a fingerprint image,” Proc. of Intl Conf. on Pattern Recognition, vol.3, pp. 756-759, Aug. 2002.

[3] Wang Na, Zhang Chiya, Li Xia, Wang Yunjin,”Enhancing Iris-feature Security with steganography”, 2010.

[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, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622–633, (San Jose, CA), January 2004.

[6] A.K.Jain and U.Uludag, “Hiding biometric data,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, Nov.2003.

[7] N.K. Ratha, J.H. Connell, and R.M. Bolle, “An Analysis of Minutiae Matching Strength,” Proc. Third Int’l. Conf. Audio-and Video-Based Biometric Person Authentication, pp. 223-228, June 2001.

[8] F. Hartung and M. Kutter, “Multimedia Watermarking Techniques,” Proc. IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[9] M. Kutter, F. Jordan, and F. Bossen, “Digital Signature of Color Images Using Amplitude Modulation,” Proc. SPIE, vol. 3022, pp. 518-526, 1997.

[10] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, “A DCT Domain System for Robust Image Watermarking,” Signal Processing, vol. 66, no. 3, pp. 357-372, May 1998.

[11] S.Pankanti and M.M.Yeung, “Verification Watermarks on Fingerprint Recognition and Retrieval”, Proc.SPIE, vol.3657, pp.66-78, 1999.

[12] K.Zebbiche, L.Ghouti, F.Kheli and A.Bouridane, “Protecting fingerprint data using watermarking,” Proc. of the 1st AHS conference, pp.451–456, June.2006.

[13] D. Kundur and D. Hatzinakos, “Digital Watermarking Using Multiresolution Wavelet Decomposition”, International conference on acoustic Speech and Signal Processing (ICASSP), Seattle, May. 1998, pp. 2969-2972.

[14] B. Chen and G.W. Wornell, “Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding”, Proc. IEEE Transactions on Information theory, vol. 47, No. 4, May. 2001.

[15] M.Vatsa, R.Singh, and A.Noore, “Improving biometric recognition accuracy and robustness using dwt and svm watermarking,” IEICE Electronics Express, vol.2, pp. 362-367, Dec. 2005.

[16] J. Daugman. “High Confidence Visual Recognition of Persons by a Test of Statistical Independence”, IEEE Tans. Pattern Analysis and Machine Intelligence, vol.15, pp.1148-1161, 1993.

[17] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, and S.McBride, “A machine-vision system for Iris recognition, “Machine Vision and Applications,pp.1-8,1.

AUTHOR BIOGRAPHY

Pravin Sonsare: Author has M.E. in computer science & Engineering and working as assistant professor.