International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-5, June 2014

Study of Fragile Watermarking to Protect the Fingerprint Database Template

Jitendra Kumar Gothwal, Ram Singh

Abstract*— Biometric based authentication, described as the science of recognizing an individual based on physical or behavioral characteristics for identity verification is becoming a security mainstay in much areas. Biometric systems have now been deployed in various commercial, civilian, and forensic applications as a means of establishing identity. Protection of biometric data & templates is gaining interest and crucial issue for the security of biometric systems. Digital watermarking techniques are used to protect the biometric data from either accidental or intentional attacks. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system. Thus a protective scheme is needed which will preserve fidelity and prevent alterations. One possible solution to gratify this problem is by using fragile image watermarking techniques which is one of the sub disciplines of watermarking techniques in information hiding domain. This paper proposed one of the information hiding techniques which is called fragile watermarking techniques that will embed a secondary data into the fingerprint images to cater the vulnerability of the images. In this way, the authenticity of the fingerprint images can be established.

***Keywords*— Biometrics, Fingerprint, Information hiding, Fragile watermarking, Authenticity.**

I. INTRODUCTION

Biometric authentication systems make use of unique physiological or behavioral characteristics of the user. As of today biometrics is the most secure ways to establish authentication. Biometric systems offer several advantages over traditional authentication methods and are superior because the biometric methods check for the physical presence of the specific user, whereas the knowledge/possession based methods are only capable of verifying the presence of the secret or token respectively. The biometric methods can therefore establish a direct relation between the presence of the biometric trait and the person itself. It is thus not possible to hand over a biometric trait to someone else as it is with passwords or tokens. It is therefore very difficult to lose, forget, or steal someone's biometric signature. For most application fields this is a highly valued quality. However, there are certain applications where this close relation between the person and its biometric signature is undesirable.

Manuscript published on 30 June 2014.
***** Correspondence Author (s)
Jitendra Kumar Gothwal, Research Scholar, Department of Computer Science & Engineering, Sunrise University, Alwar, (Rajasthan), India.
Dr. Ram Singh, Supervisor, Department of Computer Science & Engineering, Sunrise University, Alwar, (Rajasthan), India.

An additional peculiarity of all biometric methods is that they cannot rely on perfect agreement between the stored template and the newly acquired data. They have to tolerate a certain amount of variation in order to make allowances for natural fluctuations of the biometric trait. This is in stark contrast to knowledge and possession based methods where a perfect match to the value stored in the system database is mandatory. Therefore, all biometric systems can only produce probability estimation to what extent the new and the stored template correspond to each other. Each of the biometric system has its strength and weaknesses, and the choice of what type to be used depends on the application. One of the most popular types is fingerprint biometric system.

II. FINGERPRINT BIOMETRIC SYSTEM

Fingerprint biometric system, the technology that automatically identify individuals based on their fingerprint characteristic has been increasingly applied for positive verification process since they cannot be misplaced or forgotten and they also represents a tangible component that will identify a person's identity. Figure 1, shows the general framework of fingerprint biometric system. Every biometric system consists of four basic modules:

A. Enrollment Module

During enrollment, the biometrics of the user is captured and registers individuals into the biometric system database. During this phase, a biometric reader scans the individual's biometric characteristics to produce its digital representation.

B. Feature Extraction Module

The Feature Extraction Unit processes the input sample to generate an extracted feature i.e. compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

C. Matching Module

This matching module compares the current input with the template stored in the database. 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).

D. Assessment Maker

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

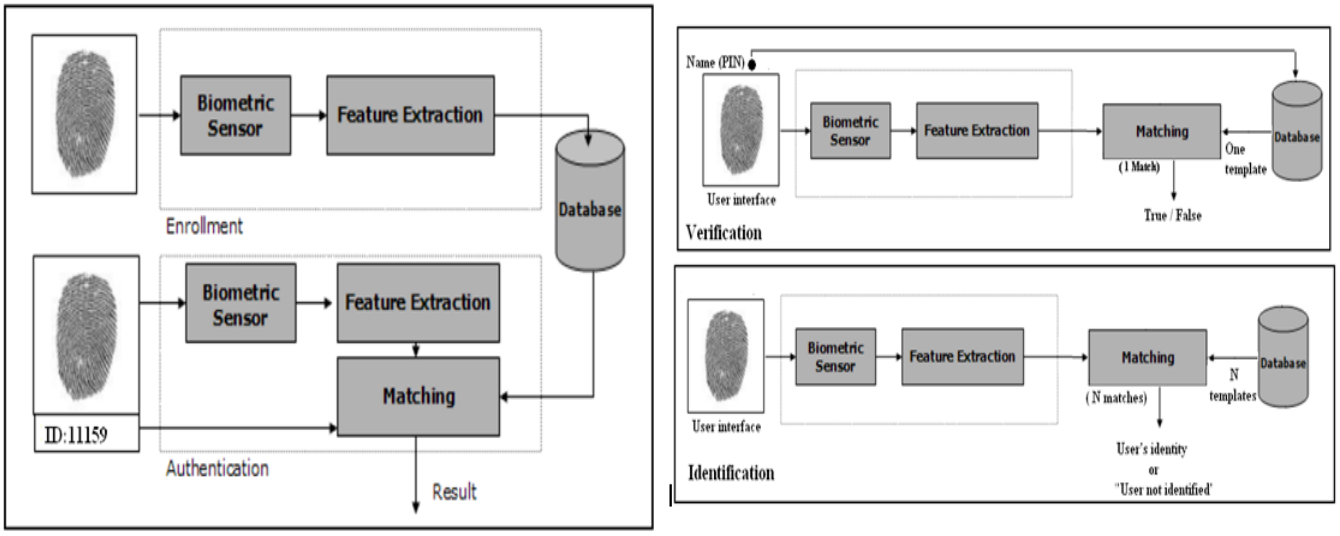

Figure 1: General Framework of Fingerprint Biometric System

In general, biometric verification consists of two stages (Figure 1): (i) Enrollment and (ii) Authentication. During enrollment, the biometrics of the user is captured and the extracted features (template) are stored in the database. During authentication, the biometrics of the user is captured again and the extracted features are compared with the ones already existing in the database to determine a match. The specific record to fetch from the database is determined using the claimed identity of the user. The fingerprint representation that has already being extracted then is matched against the fingerprint representation previously stored in the system's database either to determine or verify the identity of one person.

III. ATTACKS ON FINGERPRINT BIOMETRIC SYSTEM

While fingerprint biometric system can help to authenticate one person's identity, there are still some weak points of the system that are vulnerable to attacks, which can decrease the security of the system. The attacks on fingerprint biometric system can be categorized into eight classes. The attacks are shown in the Figure 2, below along with the components of a typical biometric system.

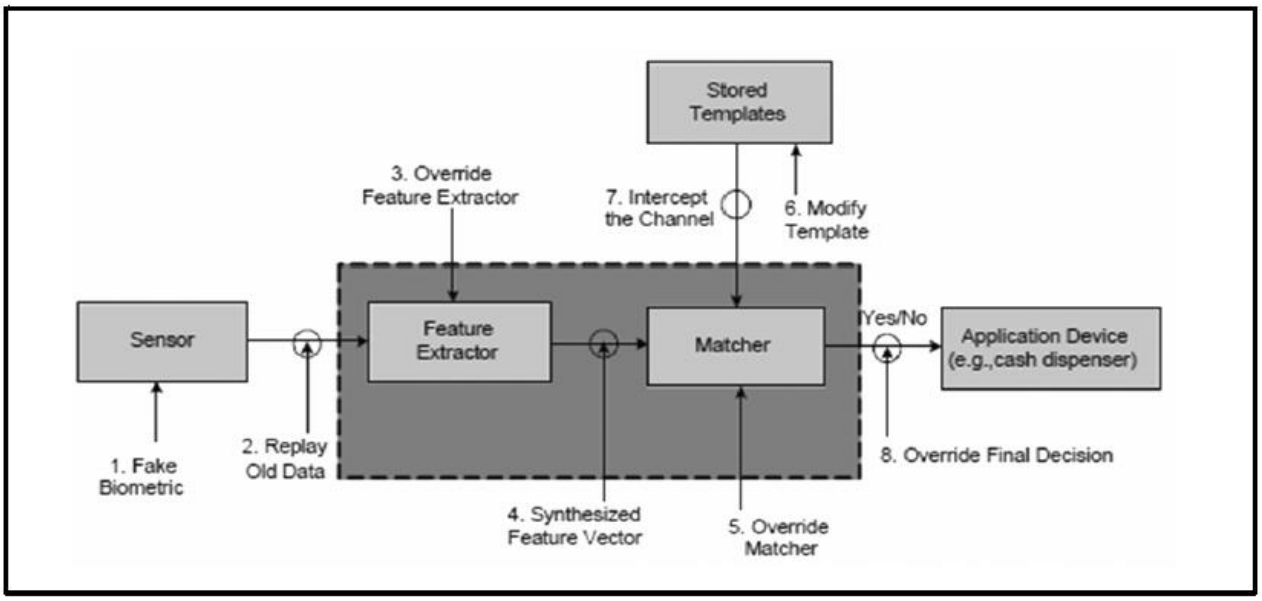

Figure 2: Vulnerabilities in a Biometric System

(i) Type one 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. In this type of attack, the unwanted person may produce a biometric claim at the sensor and will be presented in the system means 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

(ii) Type Two 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. Means in this type of attack, the recorded fingerprint images is used and replayed into the system to bypass the sensor.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

(iii) The third type 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 virus , so that it would produce a feature sets chosen by the hacker.

(iv) The fourth type attack is known as "Attack on the Channel between 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. This threat can only be possible if the system is using a remote matcher for example the fingerprint feature is transmitted over the Internet.

(v) The Fifth type of attack is known as "Attack on the matcher". The attacker replaces the matcher with a Trojan horse, so the matcher can be modified by the unwanted attacker to produce a highly matching score i.e. 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.

(vi) The Sixth type of attack is known as "Attack on the system database". In this attack, the stored templates may be tampered by the attacker. Compromises the security of the database where all the templates are stored. Furthermore, the databases might also be distributed over several servers and 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.

(vii) The Seventh type 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.

(viii) The Eighth type 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. We can also say the overridden decision is the eight attacks. The final outcome of this attack is chosen by the hacker and this could be dangerous. Even the actual pattern recognition system that is in very good performance, it may be rendered useless by simply overriding the result.

In order to promote the wide spread utilization of biometric techniques, an increased security of biometric data, especially fingerprint images, seems to be necessary. One possible solution to gratify this problem is by using fragile image watermarking techniques which will embed as additional information into the fingerprint template. The embedded information (watermark) will be used as the second authentication item to verify whether the fingerprint templates in the database are genuine or already has been tampered.

IV. FRAGILE IMAGE WATERMARKING

One category of transparent watermarks is fragile image watermarking. A fragile watermark is a mark that is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation [8]. Fragile marks are not suited for enforcing copyright ownership of digital images; an attacker would attempt to destroy the embedded mark and fragile marks are, by definition, easily destroyed. The sensitivity of fragile marks to modification leads to their use in image authentication. That is, it may be of interest for parties to verify that an image has not been edited, damaged, or altered since it was marked. The fragile watermark is specially designed to detect slight changes to the watermarked images with high probability. The framework for embedding and detecting a fragile mark is similar to that of any watermarking system. An owner (or an independent third party authority) embeds the mark into an original image .see Figure 3..

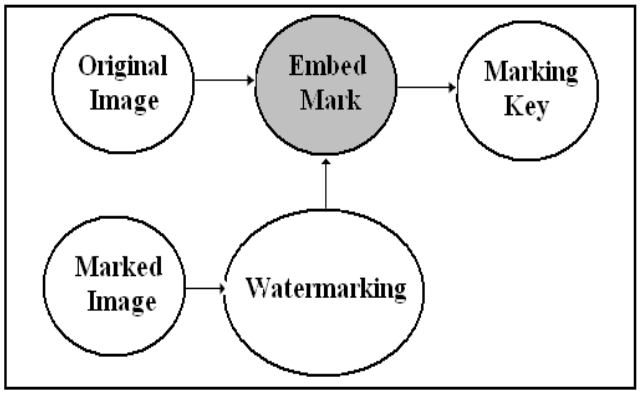

Figure 3: Watermarking Embedding

The marking key is used to generate the watermark and is typically an identifier assigned to the owner or image. The original image is kept secret or may not even be available in some applications such as digital camera. The marked image may be transmitted, presented, or distributed. The marked image is perceptually identical to the original image under normal observation. When a user receives an image, they use the detector to evaluate the authenticity of the received image, see Figure 4. The detection process also requires knowledge of "side information." This side information may be the marking key, the watermark, the original image, or other information. The detector is usually based on statistical detection theory whereby a test statistic is generated and from that test statistic the image is determined to be authentic. If it is not authentic then it would be desirable for the detector to determine where the image has been modified. The side information used by the detector is very important in the overall use of a fragile watermark. Techniques that require that the detector have the original image are known as private watermarks while techniques that do require the detector to have the original image are known as public watermarks. To be effective a fragile watermarking system must be a public technique. In many applications the original image may never be available since it might have been watermarked immediately upon creation.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

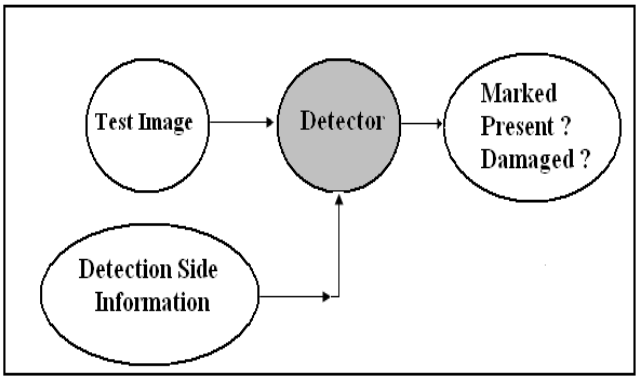

Figure 4: Watermarking Detection

V. FEATURES OF FRAGILE WATERMARKING HELPS IN PROTECTING TEMPLATE

There are several features of fragile image watermarking that have to be known with the notification that the importance of these features are relatively depending on the application that uses this technique. Some applications may have different requirements from the others according to their main purposes of the usage. All of the features were listed and presented as below:

1. **Detect tampering.** A fragile marking system should detect (with high probability) any tampering in a marked image. This is the most fundamental property of a fragile mark and is a requirement to reliably test image authenticity. In many applications it is also desirable to provide an indication of how much alteration or damage has occurred and where it is located.
2. **Perceptual Transparency.** An embedded watermark should not be visible under normal observation or interfere with the functionality of the image [11]. In most cases this refers to preserving the aesthetic qualities of an image, however if an application also performs other operations on marked images (such as feature extraction) then these operations must not be affected. Unfortunately there is not a lot of information how the "noise" introduced by marking process affects other image processing operations [16]. This is an open research problem. Also, transparency may be a subjective issue in certain applications and finding measures, which correlate well with perceived image quality, may be difficult.
3. **Detection should not require the original image.** As mentioned above the original image neither may nor exist or the owner may have good reason not to trust a third party with the original (since the party could then place their own mark on the original and claim it as their own.)
4. **Detector should be able to locate and characterize alterations made to a marked image**. This includes the ability to locate spatial regions within an altered image which are authentic or corrupt. The detector should also be able to estimate what kind of modification had occurred.
5. **The watermarks generated by different marking keys should be "orthogonal" during watermark detection**. The mark embedded in an image generated by using a particular marking key must be detected only by providing the corresponding detection side information to the detector. All other side information provided to the detector should fail to detect the mark.
6. **The marking key spaces should be large.** This is to accommodate many users and to hinder the exhaustive search for a particular marking key even if hostile parties are somehow able to obtain both an unmarked and marked versions of a particular image.
7. **The marking key should be difficult to deduce from the detection side information.** This is particularly important in systems that have distinct marking and detection keys. Usually in such systems the marking key is kept private and the corresponding detection side information may be provided to other parties. If the other parties can deduce the marking key from the detection information then they may be able embed the owner's mark in images that the owner never intended to mark.
8. **The insertion of a mark by unwanted parties should be difficult**. For an image watermark to be efficient the insertion and removal of a watermark should be difficult This feature is important since the unwanted person may remove a watermark from a marked image and subsequently inserting it into another image.
9. **The watermark should be capable of being embedded in the compressed domain.** This is not the same as saying the watermark should survive compression, which can be viewed as an attack. The ability to insert the mark in the compressed domain has significant advantage in many applications.

VI. 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 Fragile watermarking principles to enhance the integrity of biometric templates. A fragile image watermarking techniques which will embed as additional information into the fingerprint template. The embedded information (watermark) will be used as the 'second authentication item to verify whether the fingerprint template in the database are genuine or already has been tampered.

REFERENCES

[1] A.K. Jain, A. Ross and S. Prabhakar,"An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology, Special issue on Image- and Video-Based Biometrics*, Vol. 14(1), pp. 4-20, Jan. 2004.

[2] A. K. Jain, A. Ross, and S. Pankanti. "A prototype hand geometry-based verification system," in *Proc. AVBPA'99*, Washington, D.C., USA, March 1999, pp. 166–171.

[3] R. Christian and J.L. Dugelay. "A Survey of Watermarking Algorithms for Image Authentication." *EURASIP Journal on Applied Signal Processing*, vol. 2002(6), pp. 613-621, Jun. 2002.

[4] D.Maltoni, D. Maio, A.K.Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. New-York: Springer-Verlag, 2003.

[5] S.C.Sharat. "Online Fingerprint Verification System", M.S. Thesis, Department of Electrical Engineering, State University of New York, Buffalo, USA, 2005.

[6] J. D. Woodward. "Biometrics: Privacy's foe or privacy's friend?," *IEEE Journal (Special Issue on Automated Biometrics)*, vol. 85, pp. 1480–1492. Sep. 1997.

[7] B.Ruiz-Mezcua, P. Domingo-Garcia. et al. "Biometrics verification in a real environment," in *Proc. IEEE/ICCST International Carnahan Conference on Security*,1999, pp. 243-246.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

[8] M. Yeung and F. Mintzer, "Invisible watermarking for image verification," *Journal of Electronic Imaging*, vol. 7, no. 3, pp. 578-591, July 1998.
[9] A. Ross, A.K. Jain. et al. "A hybrid fingerprint matcher." *The Journal of Pattern Recognition*, vol. 36, pp. 1661-1673, Nov. 2002.
[10] L.C.Ferri, A. Mayerhofer. et al. "Biometric authentication for ID cards with hologram watermarks," in *Proc. SPIE, Security and Watermarking of Multimedia Contents IV*, vol. 4675, Jan. 2002, pp. 629–640.
[11] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual Watermarks for Digital Images and Video", *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108- 1126, July 1999.
[12] A.K. Jain, S. Pankanti. et al. "Biometrics: A Grand Challenge," *in Proc. IEEE International Conference on Pattern Recognition ICPR-2004*, vol. 2, 2004, pp. 935-942.
[13] A. Ross and A.K. Jain. "Multimodal biometrics: An overview," *in Proc. of 12th European Signal Processing Conference (EUSIPCO)*, 2004, pp.1221–1224.
[14] U. Uludag, S. Pankanti, and A.K. Jain. "Fuzzy vault for fingerprints*," in Proc. 5th International Conference, AVBPA 2005, vol. 3546, Springer*, 2005, pp. 310-319.
[15] B. Schneider, Applied Cryptography. New York: Wiley, 1996, ch. 4.
[16] S. Pankanti and M. Yeung, "Verification watermarks on fingerprint recognition and retrieval," Proceedings of the IS&T/SPIE Conference on Security and Watermarking of Multimedia Contents, pp. 66-78, San Jose, California, January 1999.
[17] M. D. Swanson, M. Kobayashi. et al. "Multimedia data-embedding and watermarking technologies." *In IEEE Journal (Special Issue on Multimedia Signal Processing)*, vol. 86, pp. 1064–1087, Jun. 1998.
[18] J. Fridrich. "Applications of Data Hiding in Digital Images," in *Proc. of the Fifth International Symposium on Signal Processing and its Applications*, vol. 1, 1999, pp.24-31.
[19] I.S. Moskowitz and Neil F. Johnson. *A Detection Study of an NRL Steganographic method*. Washington DC: Naval Research Laboratory, 2002.