International Journal of Security (IJS)

Book: 2008 Volume 2, Issue 1
Publishing Date: 28-02-2008
Proceedings
ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Table of Contents

Volume 2, Issue 1, February 2008.

Pages

Biometrics Security using Steganography

Chander Kant ckverma@rediffmail.com

Faculty, Department of Comp. Sc. and Applications

K.U. Kurukshetra, Haryana (INDIA)

Rajender Nath rnath_2k3@rediffmail.com

Faculty, Department of Comp. Sc. and Applications

K.U. Kurukshetra, Haryana (INDIA)

Sheetal Chaudhary sheetalkuk@rediffmail.com

Research Scholar, Department of Comp. Sc. and Applications

K.U. Kurukshetra, Haryana (INDIA)

Abstract

A biometric system is at risk to a variety of attacks. These attacks are intended to either avoid the security afforded by the system or to put off the normal functioning of the system. Various risks have been discovered while using biometric system. Proper use of cryptography greatly reduces the risks in biometric systems as the hackers have to find both secret key and template. It is notified that still fraudrant goes on to some extent. Here in this paper a new idea is presented to make system more secure by use of steganography. Here the secret key (which is in the form of pixel intensities) will be merged in the picture itself while encoding, and at decoding end only the authentic user will be allowed to decode.

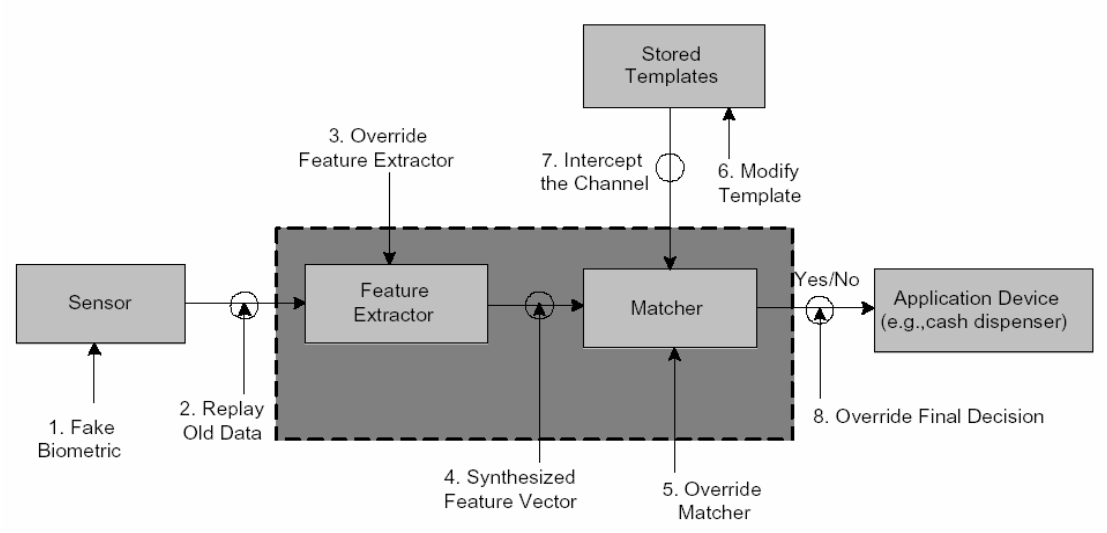
Keywords: biometric, steganography, cryptography, encoding, decoding

1. Introduction

There are basically two kinds of biometric systems [1] Automated identification systems, operated by professionals. The purpose of such systems is to identify an individual to find a criminal of a crime according to trails left on the crime scene. The operators of these systems do not have any reason to cheat the system used by ordinary users to gain a privilege or an access right. Securing such a system is much more complicated task; such systems cannot cope with the situations when the biometric measurements are disclosed, because biometrics cannot be changed (unless the user is willing to have an organ transplant). Moreover, the user will not learn that his/her biometric is disclosed. People leave fingerprints on everything they touch, and the iris can be observed anywhere they look. Biometrics definitely is sensitive data and therefore should be properly protected, but they cannot be considered secret. So the security of the system cannot be

based on knowledge of the biometric characteristics [2]. A solution to this problem presented here that beside fingerprint template, a secret data is also tagged which is secret [3]. By applying steganography technique biometric system can enhance user convenience and boost security; it is also protected to various types of threats.

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*.



(Fig1. Vulnerable in biometric system)

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, in biometric system several different levels of attacks [3] that can be launched (Figure 1):

(i) A fake biometric trait such as an artificial finger may be presented at the sensor [4], (ii) illegally intercepted data may be resubmitted to the system, (iii) the feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets, (iv) legitimate feature sets may be replaced with synthetic feature sets, (v) the matcher may be replaced by a Trojan horse program that always outputs high scores thereby defying system security, (vi) the templates stored in the database may be modified or removed, or new templates may be introduced in the database, (vii) the data in the communication channel between various modules of the system may be altered, and (viii) the final decision [5].

2. Problem Formulation

Imposter Attack

An “exact match” occurs when the digital representation of the live sample extracted from the capture device is identical to the stored biometric template to which it is compared. In most applications, an exact match is a good thing, but in biometrics, it is cause for suspicion. There is natural variability in the sample capture process that makes exact matches unlikely for many biometric technologies. When one occurs, it may be indicative that someone has improperly obtained the biometric template and is staging a replay attack [6].

A potential solution is to reject exact matches, thereby requiring the user to provide another sample. If the user is a valid one, then the variability in the sample capture process should lead to something other than an exact match on the second authentication attempt. On the other hand, if the user is an imposter who is in possession of the signed reference template only, then it may be difficult for the imposter to produce a different sample on the second attempt. There are so many types of attacks when the biometrics is under suspicious case [7], like (i) *Circumvention*: An impostor 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. (ii) *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. (iii) *Covert acquisition*: An impostor may secretly 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. (iv) *Collusion*: An individual with wide super-user privileges (such as an administrator) may deliberately modify system parameters to permit incursions by an intruder. (v) *Coercion*: An impostor may force a legitimate user (e.g., at gunpoint) to grant him access to the system.

3. Use of Steganography in Biometrics

In many cases, the appropriate use of cryptography also reduces this threat [8]. The Security Administrator will configure the biometric system to encrypt and digitally sign all biometric data before it is transmitted from one physical device to another.

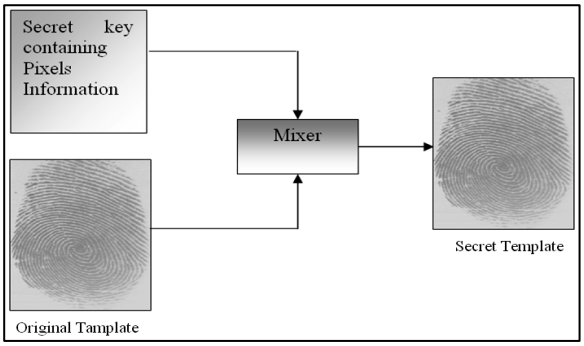


Figure 2. Use of Steganography for creating secret Templates

Steganography can greatly reduce these attacks because attackers must have to obtain the system's private data in addition, to breaching the security of the capture device or biometric storage. This makes these attacks considerably more difficult to achieve But steganography is more secure than cryptography because there is no separate key (Figure 2) in steganography rather key is inbuilt in the template [9].

4. How to Apply Steganography in Biometrics

4.1 Algorithm for insertion of message bit 'b' [10, 11].

(i) Find pseudo-random location 'l' in image from secret key to insert the message bit b. (ii) Check whether at location 'l', pixel value is 00000000 or 11111111, called boundary values. If yes, ignore this location and go to step (i). Here we are ignoring these boundary values because the change may be +2 or -2 in pixel values, which is to be avoided.

(iii) Check whether at location 'l'

a) 6th and 7th bits are b, b? If yes, then no change at 'l' is required. Message bit is already there. Go to End.

b) 6th and 7th bit are $\overline{b}$, b or b, $\overline{b}$? If yes, then see that whether it is possible to make 6th and 7th bits as b, b by adding or subtracting 1 to pixel value?. If yes, do it and go to End. Otherwise ignore the location 'l' and go to step (i).

c) 6th and 7th bits are $\overline{b}$, $\overline{b}$? If yes, then see whether it is possible to make 6th and 7th bits to b, b by adding or subtracting 1? If yes, do it and go to End. Otherwise change them to b, b or b, b by adding or subtracting 1 and go to (i).

(iv) End.

4.2 Algorithm for retrieval of message bit 'b'

(i) Trace out the location 'l' from the same secret key as used in insertion algorithm.

(ii) Pixel value is equal to one of the boundary values, i.e., 00000000 or 11111111? If yes, then it is invalid address. Go to step (i).

(iii) Check whether at location 'l'

a) 6th and 7th bits are different, i.e., $\overline{b}$, b or b, $\overline{b}$? If yes, then it is invalid address go to step (i).

b) 6th and 7th bits are same i.e. b, b then b is the message bit.

(iv) End.

The main results we got from our insertion algorithm are [12].

- 49% chances, that message bit will be inserted at pseudorandom location at first chance.
- 50% chance, that when message bit is inserted, no change in pixel value is required.
- 12.5% chances, that change in pixel value is required, when we are ignoring the location.

5. Summary and Future Prospectus

We have discussed various types of attacks that can be launched against a biometric system. We discuss the importance of steganography principles to enhance the integrity and security of biometric templates. 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 there is a tendency 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 cause several challenges, and it is necessary that further research be conducted in this direction.

REFERENCES

[1] A. K. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers, 1999.

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

[3] A. K. Jain, Arun Ross and U. Uludag "Biometrics Template security: Challenges and solutions" in *Proc. of* European Signal Processing Conference September 2005.

[4] U.K. Biometric Working Group, "Biometric security concerns," Technical Report, CESG, September 2003, http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricSecurityConcerns.pdf.

[5] A. Adler, "Can images be regenerated from biometric templates?," in *Biometrics Consortium Conference*, (Arlington, VA), September 2003.

[6] 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.

[7] 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.

[8] C. Soutar, "Biometric system security," White Paper, Bioscrypt, http://www.bioscrypt.com.

[9] 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.

[10] Neil F. Johnson, Sushil Jajodia, "Steganalysis of Images Created Using Current Steganography Software", Lecture Notes in Computer Science, vol 1525, 1998, Springer-Verlag.

[11] Parvinder Singh, Sudhir Batra, HR Sharma, "Evaluating the Performance of Message Hidden in 1st and 2nd Bit Plane", WSEAS Transactions on Information Science and Applications", issue 8, vol 2, Aug 2005, pp 1220-1227.

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA