

# On the Vulnerability of Biometric Security Systems

Marcos Faúndez-Zanuy  
*Escola Universitaria Politècnica de Mataró*

## ABSTRACT

**This paper presents an overview of the weakness of biometric security systems and possible solutions to improve it. Different levels of attack are described, and the strengths and weaknesses of the main biometric system is emphasized. Solutions are provided with special emphasis on cryptography and watermarking techniques.**

## INTRODUCTION

As a general rule concerning security matters, a constant update is necessary to keep being protected. A suitable system for the present time can become obsolete if not periodically improved, so it is important to know the main different attack levels that it can suffer, and actual solutions or trends for the future. Thus, protecting systems must be kept one step ahead of the piracy systems. Usually, the combination of systems and security mechanisms are key factors.

Authentication methods by means of biometrics are a particular portion of security systems, and thus, they are not an exception. Although the advantages of biometrics in front of other authentication methods are well-known, there are also drawbacks (see Table 1).

## ATTACK LEVELS

In order to see the vulnerable aspects of a biometric system, we can study the block diagram [1, 2] shown in Figure 1. We will focus on those situations where an impostor tries to access a system or enter a facility, instead of the genuine user. Another situation is when a person tries to avoid identification. This last situation is more related to police applications, suspect identification, etc., and is a fully different problem not considered in this paper.

Obviously, some of these levels do not apply to particular environments, so it depicts the most general case. Eight different levels are summarized:

### 1. Sensor Level

In this level, a fake biometric characteristic is presented at the sensor. Table 2 summarizes the main biometric technologies, their vulnerability options, and how to overcome them.

For instance, in a speaker recognition system, it can be fooled using a tape recording of the genuine speaker, but if the biometric system is operated on a text-dependent mode [3], this is not possible, because it would imply the use of a speech synthesizer. Current systems can synthesize any text in real-time, but it is not yet possible to use whoever the speaker nor to apply a voice conversion (transformation) system [4] among speakers with enough quality. Perhaps these systems will be available in the future, and then more sophisticated authentication algorithms can be applied.

### 2. Transmission Between the Sensor and the Feature Extractor

In this level, the attack consists on the resubmission of digitally stored biometric data. Obviously this possibility is especially important in remote applications where there is a client computer that provides biometric data and a remote host system that performs biometric authentication. In this kind of application, the fraudulent acquisition of biometric data by third parties is also possible. These attacks are especially important for internet applications. Anyway, this is the same problem that must be faced for e-commerce with the electronic submission of VISA, AMEX, etc., credit card information. Obviously, with biometric data, there is an additional problem: while it is possible to obtain a new card number, it is *not* possible to replace biometric data.

One way to avoid this problem is through the use of watermarking [7-8].

### 3. Feature Extractor Level

At this level, the feature extractor can be forced to produce feature values chosen by the attacker, instead of the real values extracted from the original signal acquired by the sensor. A program can disguise itself as the feature extractor, and bypass the genuine feature extractor. This is probably not the easiest point at which to attack the system.

---

This work has been supported by the Spanish Grant CICYT TIC-2003-08382-C05-02.

---

Authors' Current Address:  
M. Faúndez-Zanuy, Escola Universitaria Politècnica de Mataró, Avda. Puig i Cadafalch  
101-111, 08303 Mataró, (Barcelona) Spain.

Manuscript received November 28, 2003.

0885/8985/04/ \$17.00 © 2004 IEEE

**Table 1. Advantages and Drawbacks of the Three Main Authentication Method Approaches**

<b>Authentication Method</b>	<b>Advantages</b>	<b>Drawbacks</b>
<b>Handheld tokens</b> (card, ID, passport, etc.)	A new one can be issued. It is quite standard, although moving to a different country, facility, etc.	It can be stolen. A fake one can be issued. It can be shared. One person can be registered with different identities.
<b>Knowledge-based</b> (password, PIN, etc.)	It is a simple and economical method. If there are problems, it can be replaced by a new one quite easily.	It can be guessed or cracked. Good passwords are difficult to remember. It can be shared. One person can be registered with different identities.
<b>Biometrics</b>	It cannot be lost, forgotten, guessed, stolen, shared, etc. It is quite easy to check if one person has several identities. Can provide a greater degree of security than others.	In some cases, a fake one can be issued. It is not replaceable, nor secret. If a person's biometric data is stolen, it is not possible to replace it.

**Table 2. Vulnerability Options for Different Biometric Characteristics at Sensor Level**

<b>Biometric technology</b>	<b>Vulnerability</b>	<b>Solutions</b>
<b>Fingerprint</b>	Synthetic or dismembered fingers.	To use thermal scanners to detect the temperature. Detection of a perspiration pattern over the fingertip skin can identify the vitality of a fingerprint [5].
<b>Voice</b>	A tape recording of an authorized user.	To use a text-dependent system (different for each trial.)
<b>Iris</b>	Prosthetic eye.	Infrared system for checking veins will look at flows of warm blood [6].
<b>Face</b>	Another person can be characterized trying to imitate.	Combined with other biometric technology (multimodality). The use of facial termographies.

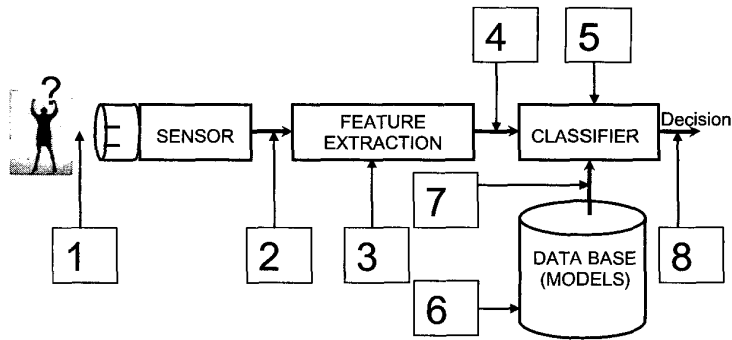


Fig. 1 Different attack points in a general biometric authentication system

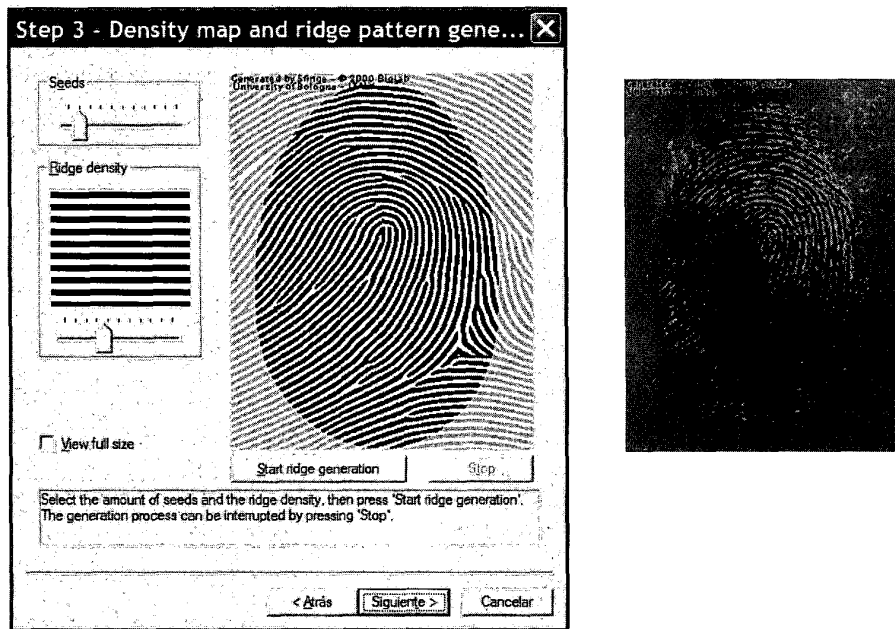


Fig. 2. Synthetic fingerprint generation. On the left, a screen snapshot of the [9] software; on the right, the final result

#### 4. Transmission of the Extracted Features

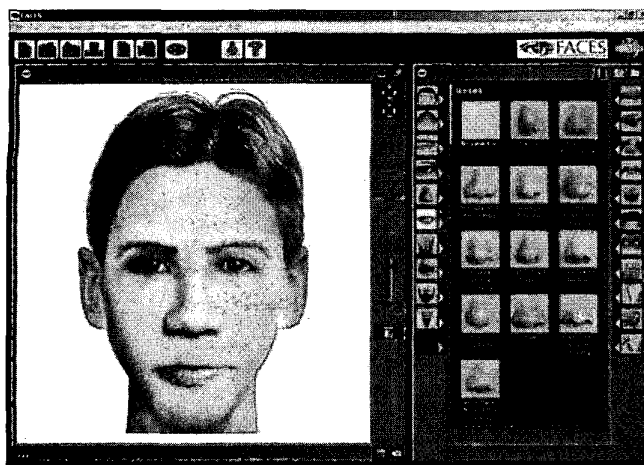
This attack consists of the replacement of the original features by fake ones, or a set of features that have been illegally acquired previously. This kind of attack is especially important for remote authentication applications. It is the same situation as in Level 2. A biometric system can be designed thinking of the transmission of a speech or image signal (for example, wave or bmp file) or the useful information for recognition purposes can be extracted and all irrelevant information discarded. The advantage of this approach is that the amount of information to be sent from the client to the remote host can be significantly smaller. The easiest way to protect this information from piracy is the use of a time stamp information and data encryption. The time stamp can be a method to detect if these biometric features have been previously stored or if they are actual. This solution also applies to Level 2, and is discussed in more detail next.

#### 5. Classifier Level

At this level, the classifier is attacked in order to produce lower or higher scores, regardless of the input feature set. It is a similar situation to Level 3.

#### 6. Data Base





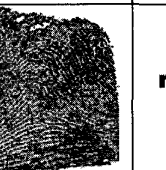

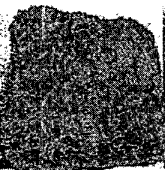
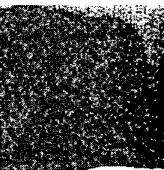

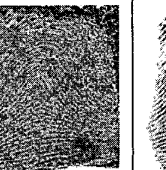
The authentication result depends on the comparison between the stored templates in the database and the features of the input sample. If the database is altered in some manner, the system will be permanently fooled. Alternatively, the database content cannot be altered but the stored templates can belong to a fake user. In the first case, special care must be taken to assure the integrity of the database, and that it is not modified from the outside. This could imply frequent backups, no writing permissions except for new data, etc. In the second case, special care must be taken during the enrollment of users, with strong supervision of the whole process by authorized persons.



**Fig. 3. Synthetic Face Generation**



**Fig. 4. Hand-Geometry Biometric System**

original	Extracted bits				Watermark + Result
					
	b7	b6	b5	b4	
					
	b3	b2	b1	b0	

**Fig. 5. Original Image, Extracted Bits, Watermark, and Reconstructed Image**

## 7. Transmission of the Database Templates to the Classifier

At this level the system can be fooled into replacing the templates of the database with fake ones. This level is analogous to Levels 2 and 4, but is probably less important. The database used to be in the same computer or device that executes the classifier algorithm, so this connection is difficult to be cracked.

It can be a problem when the database is in a remote host. For instance, a biometric authentication system with a unique database remotely shared by several clients that acquire the biometric information of the user, consult the remote database, and perform the classification.

## 8. Decision Level

This last level consists of skipping the whole biometric system and replacing the decision. For instance, a biometric

system for access control can be implemented with a sensor connected to a computer that performs the identification and produces one output signal that opens (or not) a given door. One way to fool the system is as simple as cutting this control wire and replacing the signal by an appropriate one in order to open the door.

Mainly attacks can be split into two categories: against communication channels (2, 4, 7 and 8), which can be named "replay attacks," and against system modules (1, 3, 5 and 6).

If the communication links are not secured, a replay attack is possible. It consists of resubmission of previously intercepted biometrics or biometric feature sets. This possibility can be reduced with the time stamp watermarking method described in the next section.

Another type of attack which is also possible with password-secured systems, is the brute force attack. It consists of trying with a huge set of random synthetic images. This is analogous to repeating several attempts with different words

**Table 3. Commercial Products for Digital Watermarking**

Products	Website
Stego, EzStego for Java & Stego Online	<a href="http://www.stego.com">http://www.stego.com</a>
White noise storm	<a href="ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/wns210.zip">ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/wns210.zip</a>
S-tools	<a href="ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools4.zip">ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools4.zip</a>
Hide and seek	<a href="ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/hdsk41b.zip">ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/hdsk41b.zip</a>
Jpeg-Jsteg version 4	<a href="ftp://ftp.funet.fi/pub/crypt/steganography">ftp://ftp.funet.fi/pub/crypt/steganography</a>
Picturemarc	<a href="http://www.digimarc.com">http://www.digimarc.com</a>
Suresign	<a href="http://www.signumtech.com">http://www.signumtech.com</a>

contained in a dictionary for cracking password-secured systems. Anyway, [2] estimates that a fingerprint is as difficult to guess by brute force attack like a nonsense 16-characters-long password. Figure 2 shows an application that can produce synthetic fingerprints. This program can be freely downloaded from [9]. Figure 3 shows a similar result for face synthesis. An example of a program for this purpose is FACES 4.0 [10]. Obviously, for synthetic speech synthesis, there are also applications like Elan synthesizer [11]. Anyway, their ability to synthesize different voices is quite limited.

This problem can be relieved with a limit on the maximum trials permitted to access an account in a pre-defined time slot. However, this does not avoid the problem of attacking several accounts with the same fake biometric signal in order to access one account.

## DATA ENCRYPTION AND WATERMARKING

In compact system where all the blocks and information are embedded in the same package, it is difficult to attack the system, except for the first and last levels. This is the case of the hand-geometry recognition system shown in Figure 4, where it is obvious that it is not easy to access the internal blocks of the device without being seen. In some cases, the templates can be stored in a smart card (look at the card reader in Figure 4) instead of a database, constituting a distributed database. In this case, it can be interesting to encrypt the information after enrollment. This implies that the encrypted templates must be decrypted before generating the matching result with the biometric data obtained online. As a consequence, the encrypted templates are secured since they cannot be utilized or modified without decrypting them with the correct key, which must be kept secret.

One problem with encryption is that the data are no more protected once the key is cracked or the data are decrypted. Thus, if there is a possibility that decrypted data could be intercepted, encryption does not address the overall security of the biometric data [1].

Another security mechanism is to use watermarking techniques [7-8]. Their usefulness is twofold:

- a) A time-stamp can be included in the biometric data, to setup an expire-date. Thus, if the data is intercepted by a hacker, it will be worthless for the future. Typically, this watermark cannot be removed or replaced without making the data useless.
- b) The biometric data can be hidden in a host signal, which can be any image or another biometric signal. For instance, [1] proposes a system where the eigenface coefficients for face recognition are hidden inside a fingerprint image.

Obviously, watermarking and cryptography can be combined in a single system, in order to obtain higher protection levels.

In order to illustrate how watermarking works, a very simple method is shown in Figure 5, known as least significant bit (LSB) substitution. This information can be a monochrome image or just the necessary bits to encode the watermark (binary code of the time stamp). It is also applicable to speech files, and as its name indicates, consists of the extraction of the LSB and its replacement by the information that you want to hide. It is interesting to observe the noisy aspect of the lower bits, and their small contribution to the final luminance.

For gray-scale images encoded at 8 bits per pixel, the luminance of each pixel can be represented as:

$$I = \underbrace{b_7}_{MSB} \times 2^7 + b_6 \times 2^6 + b_5 \times 2^5 + b_4 \times 2^4 + b_3 \times 2^3 + b_2 \times 2^2 + b_1 \times 2^1 + \underbrace{b_0}_{LSB}$$

and the LSB can be replaced without altering significantly the image quality. This method can be improved if the hidden information is introduced in a pseudo-random order that can be

deduced using a pseudo-random number generator (obviously the seed and the algorithm must be kept secret for third-parties).

Table 3 shows the websites of some commercial products for watermarking. A good example is the Digimac technology included in Corel Draw and Adobe Photoshop, which introduces a given information that cannot be removed without destroying image quality. This can be useful for time-stamp data inclusion in a fingerprint, face image, etc. in order to avoid the use of a biometric data that has been previously used and, as a consequence, has already expired.

Obviously, the lesser available information on how the data has been watermarked, the higher difficulty for hackers to crack the system.

## REFERENCES

- [1] A.K. Jain and U. Uludag, November 2003,  
Hiding biometric data,  
IEEE Trans. on Pattern Analysis and Machine Intelligence,  
pp.1494-1498, Vol. 25, No. 11, November 2003.
- [2] N.K. Ratha, J.H. Connell and R.M. Bolle, June 2001,  
An Analysis of Minutiae Matching Strength,  
Proc. Int'l. Conf. Audio- and Video-Based Biometric  
Person Authentication, pp. 223-228, June 2001.
- [3] D. O'Shaughnessy, 2000,  
Speech Communications: Human and Machine, 2<sup>nd</sup> Edition,  
IEEE Press, 2000.
- [4] B. Gold and N. Morgan, 2000,  
Speech and Audio Signal Processing,  
John Wiley & Sons, Inc., 2000.
- [5] R. Derakhshani et al., February 2003,  
Determination of Vitality from a Non-Invasive Biomedical  
Measurement for Use in Fingerprint Scanners,  
Pattern Recognition, Elsevier 36, pp.383-396,  
February 2003.
- [6] B. Miller, February 1994,  
Vital signs of identity,  
IEEE Spectrum, pp.22-30, February 1994.
- [7] W. Bender et al., 1996,  
Techniques for Data Hiding,  
IBM Systems Journal, Vol. 35, Nos. 3 and 4,  
pp.313-336, 1996.
- [8] N.F. Johnson and S. Jajodia, February 1998,  
Exploring Steganography: Seeing the Unseen,  
IEEE Computer, pp.26-34, February 1998.
- [9] [http://bias.csr.unibo.it/research/biolab/sfinge2\\_5\\_download.html](http://bias.csr.unibo.it/research/biolab/sfinge2_5_download.html).
- [10] [http://www.iqbiometrix.com/products\\_faces\\_40.html](http://www.iqbiometrix.com/products_faces_40.html).
- [11] <http://www.elanspeech.com>.