Design and Implementation of an Electronic Identification Card

J. Flores-Escalante*[1], J. Pérez-Díaz[2], R. Gómez-Cárdenas[3]

[1,2] Instituto Tecnológico y de Estudios Superiores de Monterrey,
Campus Cuernavaca, Autopista del Sol km 104, Colonia Real del Puente,
C. P. 62790, Xochitepec, Morelos, México.
* joel.flores.escalante@gmail.com
[3] Instituto Tecnológico y de Estudios Superiores de Monterrey,
Campus Estado de México.
Carretera Lago de Guadalupe Km 3.5, Atizapán de Zaragoza,
C.P. 52926, Estado de México, México.

ABSTRACT
In this paper we present an "Electronic Identification Card" (EIC). This EIC is designed to provide a high degree of security for user authentication using *biometrics, cryptography* and *steganography*. The EIC encrypts the user's personal information as well as his fingerprint and then embed it in a photograph of the user's face. Two factors of authentication are used in the process: "something the user knows" and "something the user has", in order to provide layers of security to shield the card. The EIC gives the flexibility to operate in database systems, storage media like chips for smart cards or digital passports. We also developed schemes to authenticate users through the EIC, like remote authentication by a Web interface and the authentication in a local machine.

Keywords: Authentication, steganography, criptography, security, fingerprints.

RESUMEN
En este artículo se presenta una "Credencial de Identificación Electrónica" (CIE) cuya función será proveer un alto grado de seguridad al autenticar a los usuarios haciendo uso de *biométricas, criptografía* y *esteganografía.* La CIE cifra la información personal del usuario así como la huella dactilar del mismo para después incrustarla en una fotografía del rostro del usuario. Se utilizan dos factores de autenticación (algo que se sabe y algo que se tiene) en el proceso anterior; todo esto para proporcionar capas de seguridad que blinde la credencial. Ésta ofrece flexibilidad para funcionar en sistemas de base de datos, en medios de almacenamientos como chips para tarjetas inteligentes o pasaportes digitales. También se desarrollaron esquemas para llevar a cabo la autenticación de usuarios por medio de la CIE como la autenticación vía remota por medio de una interfaz y la autenticación en una máquina local.

Palabras clave: Autentificación. esteganografía, criptografía, seguridad, huellas digitales.

1. Introduction

For public and private organizations is a matter of vital importance the authentication of people that request access to their facilities and resources because, if their confidential information falls into the wrong hands, their interests would be in risk. In the digital world, knowing with whom you are doing business is the basis for secure transactions. Prevention of crimes related to identity theft is important for our leaders. In Mexico, data provided by Condusef [1] shows us that the loss resulting from this type of crimes was of 215 million pesos, according to640 complaints reported solely in the year 2006. IAFCI (International Association of Financial Crimes Investigators) [2] provides data which reports losses of about 5 thousand million pesos.

These problems involve user authentication that is the process through which the user's identity is verified and which ensures that an individual is, in fact, who he claims to be [3]. The mechanisms that

allow us to verify the above are called authentication factors. There are three classical authentication factors: something the user knows, something the user has and something the user is [3][4].

The authentication based on "something the user has" lies in a physical object that the user owns and in somehow it provides authentication to him. For example, we can mention intelligent cards, magnetic striped cards, etc.

The most widely used form of authentication is the one based on "something the user knows". This depends on some kind of knowledge stored inside the system. The user enters this knowledge and the system compares it with the one stored. Passwords to access a system, or PINs (Personal Identification Numbers) for credit cards, are examples of this type of authentication.

The authentication based on "something the user is" lies in the physical and biological characteristics of a person. This technique is also known as biometric. This technique carries out a physical measurement and then does a match with a previously stored profile. Among the most frequently used characteristics we can mention are the fingerprint, the eye's iris and the hand geometry.

To face problems related to user authentication several techniques have been used. Some of them belong to the field of biometrics. Depending on the application context, biometric systems are classified as [5]

• Verification systems: they authenticate the identity of a person comparing the captud biometric characteristic versus a biometric pattern previously stored. This implies are 1:1 comparison to determine if the identity claimed by a person is true. The system answers the question: Am I who I say I am?

• Identification systems: They recognize an individual looking into all the patterns stored in a database until they find a match. This involves making comparisons 1:N to determine the identity of a person. A verification system determines the identity of a person without that person claiming an identity (or fails if the subject is not registered in the database system), answering the question: Who am I?

Every day, new and more sophisticated systems to deal with these problems are developed. The aim of this paper is to propose and innovate in this area with techniques such as encryption and steganography, using a biometric system along with another authentication factor.

1.1 Related work

There are several studies that propose to use the user's fingerprint to create an electronic card.

The Bogosian system [6] proposed a solution to bank frauds. This system builds a credit card that stores the user's fingerprints on the magnetic stripe. The user provides his/her fingerprint which is compared versus the one stored in the magnetic stripe and versus one stored in the company database. Additionally, a description of the surface of the card embedded in the magnetic band is compared with one in the hands of the company.

Piosenka et al. created the "Unforgeable personal identification system" [7] consisting in a portable memory device which stores information such as facial photo, retina scan, voice and fingerprint. When the user wants to be authenticated, he/she presents the device with the encrypted information and provides the required biometric.

Paul Burger designed his "Biometric authentication system" [8] in which the template of the fingerprint is stored in a chip card. This template is compared with the fingerprint provided by the

user. When the person is authenticated, the encrypted information is sent.

The NIDe [9] of the Spanish government is a smart card that serves as the National Identity Document (NID) and has a cryptographic chip using 3DES and RSA key management. It provides authentication by PIN, biometric fingerprint, among others.

The Bogosian system only works for credit cards and is slow due to the comparisons that it has to perform. It also has a serious security flaw: if someone stole the card, it would be easy to extract the fingerprint because it does not have a cryptographic protection. The Piosenka system has the disadvantage that it uses a complicated cipher system based on asymmetric cryptography in which the institutions that want to authenticate their employees or that have access to some information must have their key pair and provide the public one. If there are many institutions interested in accessing the information, the system becomes slow. Burger's design does not specify the algorithm used to encrypt the user's information. All previously mentioned systems only used one factor of authentication to verify the identity of the user, which does not lead to a robust authentication. The EIC proposal is not subject to operate solely on a chip card, it can work either on database systems or network environments. With the great revolution in computing and the increase in processing speed, the work of cryptanalysis gets easier every day, so it is important not only to encrypt but also to hide the information. That is why our work adds another layer of security using steganography to protect the encrypted data.

2. Criptography and steganography

Cryptography and steganography are the techniques we use to provide security to our data.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [10]. With this technique, we transform the message by making its meaning obscure, in such a way that is impossible to be read by non-authorized entities.

Digital steganography is the art of secretly hiding information inside a multimedia signal in such a way that its existence is hidden [11]. Its main objective before preventing that intruders know the information is to suggest that the information even exists.

The steganography is used to hide information. If two parties (sender and receiver) engage in a communication using cryptography, a third party (the spy) may suspect that valuable information is being exchanged and will try to carry out an attack, trying to break the system or modify it. So the objective is to create a secret communication which is totally unknown to the opponent. The hidden information in a seemingly innocent cover does not raise any suspicion. Table I shows the differences between these two techniques.

Steganography	*Cryptography*
Prevents the discovery of the communication	Prevents the discovery of the content
The message transfer is unknown	The message transfer is known
Little known technology. Still being developed for certain formats	Common technology. Most algorithms known
Does not alter the message's structure	Alters the message's structure

Table 1. Differences between steganography and cryptography.

The steganographic system (stego-system) that we used was the "secret key steganography". In this, we do

$$S_k = I(c,m) \quad (1)$$

Where S is the stego-object, *k* is the stego-key, *I* is the steganographic technique that receives cover c and message *m,* as parameters (see Figure 1).

There are several steganographic methods; in Table II, we show the characteristics of some of the most important. It shows the characteristics of techniques like *least significant bit substitution* (LSB), *palette-based images, discrete cosine transform* (DCT, by modulation and least significant bit substitution in the transform) and discrete Fourier transform (DFT). From this table we select the "least significant bit substitution in the discrete cosine transform technique" [12] to be used in our work. This algorithm works with JPEG compression, so the storage size is minimal unlike the LSB technique that works with bmp images. This feature is important for image storage. JPEG is a common file on the network so it does not raise suspicion as it would a bmp file. By using the LSB substitution on the quantified coefficients in the discrete cosine transform (qDCT), the distortion of the cover is null, therefore it is preferable instead of algorithms like color palette (which tends to distort the picture). It also has enough embedding capacity for our data. The previous characteristics make its complexity of implementation to be average (in comparison with the DFT algorithm), which makes it the ideal algorithm for our work. In the following section, we are going to explain the basic operation of this algorithm. For more information about steganographic techniques refer to [1] [14] [15].

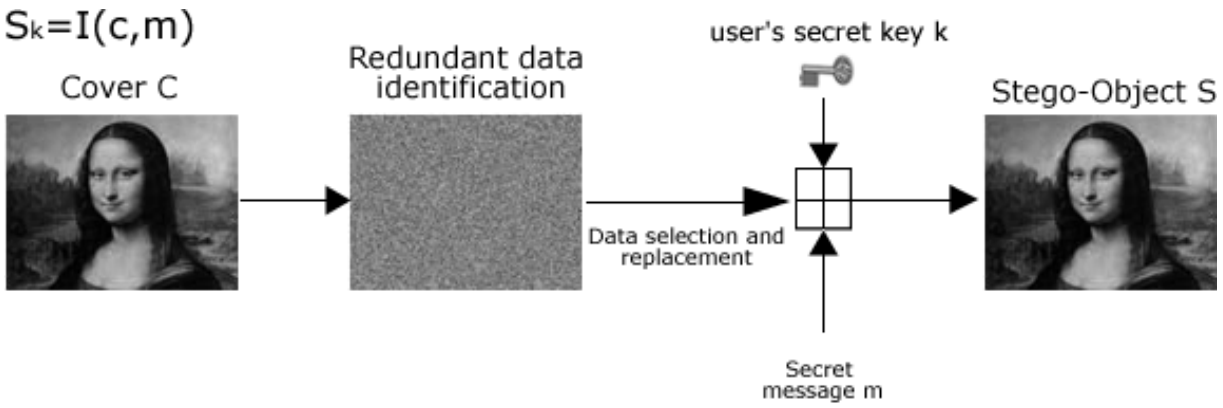

Figure 1. Embedded process in secret key steganography.

	LSB	*Palette Based*	*DTC by modulation*	*DTC by LSB*	*DFT*
Domain	Space	Space	Transformation	Transformation	Transformation
Media distortion	Low	High	Low	Null	Low/Medium
Embedding capacity	High	Low	Low	Medium	MediumHalf
Robustness	Null	Null	Null	Medium	Medium
Suspicious	High	Medium	Null	Null	Null
Compression	No	No	No	Yes	Yes
Implementation complexity	Low	Low	Low	Medium	Medium

Table 2. Comparison between the steganographic techniques.

2.1 LSB in the DCT coefficients

This technique proposes to utilize the LSB in the qDCTs. The embedding process happens between the *quantification phase and codification phase* of the JPEG process (for the JPEG process refer to [16]). This means that our information is embedded after the lossy compression phases, which guarantees us that the information will not be lost.

The procedure is the following: After the phase of *image preparation*, the JPEG image is divided into subimages of 8x8 coefficients, representing the separated components *YCbCr*. The next *image transformation* phase uses Formula (2) to perform the discrete cosine transform, in every sub image of each component.

$$F(u,v) = \frac{1}{4}C(u)(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\Pi}{16}\cos\frac{(2y+1)v\Pi}{16}\right] \qquad (2)$$

Where *u* represents the matrix rows and *v* the matrix columns. And *C* is the normalization function where *n* represents *u* or *v* in *C*, then *C(n)* is defined by (3):

$$C(n) = \begin{cases} \sqrt{\frac{1}{2}} & if\ n = 0 \\ 1 & otherwise \end{cases} \quad (3)$$

In the next step called *quantization phase*, the obtained matrices from the transformation will be quantified. The quantization consists in dividing the *F(u,v)* by a quantization matrix, this is done by Equation (4). The quantization matrix will be chosen depending on the component (Y, Cb or Cr) and the quality of image that we want. In the JPEG process, the suggested quantization matrices are shown in Table III for the Y component and Table IV for the Cb and Cr component. After the division, the result is rounded to the nearest integer.

$$F^{Q}(u,v) = round\left(\frac{F(u,v)}{Q(u,v)}\right) \quad (4)$$

(u,v)	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

Table 3. Quantization table for Y component

(u,v)	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*
0	17	18	24	47	99	99	99	99
1	18	21	26	66	99	99	99	99
2	24	26	56	99	99	99	99	99
3	47	66	99	99	99	99	99	99
4	99	99	99	99	99	99	99	99
5	99	99	99	99	99	99	99	99
6	99	99	99	99	99	99	99	99
7	99	99	99	99	99	99	99	99

Table 4. Quantization table for Cb, Cr components components

Then we can replace the least significant bits to hide the information. The LSBs that may be used are those which belong to the quantified coefficients that are different from zero and one (due the amount of zeros and ones that exist, changing zeros for ones, or vice versa, will affect the rate of compression) [17]. For this, we apply algorithm [12]:

```
Input: message, shared secret, cover image
  Output: stego image
  while data left to embed do
    if DCT <> 0 and DCT <> 1 then
      get next LSB from message
      replace DCT LSB with message LSB
    end if
    insert DCT into stego image
  end while
```

Then proceed to the last step of the JPEG process, the *coding phase,* where entropy coding is employed to reduce the information. This is a lossless compression; therefore, our embedded data will not be lost.

The images that utilize lossless compression (bmp, png) are susceptible to visual alterations when the LSBs are modified. This is not the case for LSBs in the DCT, since changes occur in the frequency domain instead of the spatial domain, then there will not be visual changes in the image [18].

3. System design

3.1 Electronic Identification Card

Our cryptographic/steganographic process is called "Electronic Identification Card" (EIC). The card has flexibility to operate in database systems, media storage like chips for smart cards and digital passports.

To meet our goal of creating a highly reliable card, we must achieve the following characteristics:

Robust authentication

Robust authentication is achieved by combining two or more factors of authentication. Those used in the EIC creation are something that the user knows and something that the user is.

Factor "something that the user knows" refers to the password only known by the user, this will not be stored nowhere in the system. Not storing the password avoids that even people from inside of the organization facilitate the password to other people. The password functions are the following:

The biometric selected for this work as factor "something that the user is" was the user's fingerprint because it is the most mature biometric and it is easy to implement. This information (the characteristic vector of the fingerprint and the user's personal information) is saved in message *m.*

Information confidentiality

The information confidentiality is related to that information that can be accessed only by authorized entities. This is the cryptography's field.

With cryptography, we establish the first security layer to our system. The algorithm chosen for our symmetric cryptosystem is the AES (Advanced Encryption Standard) [19] because it is the current security standard. The key length is 256 bits, this guarantees the security of the cryptosystem. This is performed by doing: $m_1 = AES_k(m)$, where m_1 is the resulting message from ciphering the user's information.

Information integrity

The information integrity is related to verifying that the information has not suffered changes in some way. This is the field where the hash functions work.

In our system, the hash is useful to verify that the EIC has not been altered. We used a 256 bits SHA2 algorithm. We performed the hash operation doing: $m_2 = SHA_2(m)$, where m_2 is our message digest.

Information secrecy

The study of communications security includes not just encryption but also traffic security, whose essence lies in hiding information [20]. One branch of this is steganography.

This technique was applied in the photograph of the user. This layer of security is used to hide the user's data (fingerprint and personal information) into the cover, it also has the functionality to

present the face of the user that can be used as a plus in the process of authentication, while not being suspicious.

With the secrecy, we get our EIC through:

$$CIE = DTC_k(C, AES_k(m) + SHA_2(m)) \qquad (5)$$

Where *C* is the photograph of the user acting as a cover.

Information availability

Information availability refers to the fact that the card is available when needed.

In order to test the functionality of the card, we need to store it in an electronic media. To test the authentication scheme locally and remotely, we will use a database where we have stored the user's ID, the ICE and hash. The database adds an extra security layer since not everyone has access to the database and we can configure accounts with access permissions, etc.

We also offer availability of information when we design our EIC to be carried anywhere, for example on an electronic smart card or on digital passports. This feature is important in the EIC.

EIC model

The general model of our EIC is noted in Equation (6) and in Figure (2). The main idea represented in the figure is to get the user's personal information as well as his fingerprint. With this information, we create a cryptogram (configured by the secret key *k*) $m_1 = AES_k(m)$ and then we got a hash $m_2 = SHA_2(m)$ From the concatenation of m_1 and m_2, the secret message m'. results, which is the message to be incrusted. In the other side of the image, we have our cover *C* (the user's face photograph) in which we are going to apply the steganographic technique *(DTC)* in function of *k, C* and *m'*. As a result, we obtain the stego-object S (a JPEG image with a secret message incrusted).

$$CIE = DTC_k(C, AES_k(m) + SHA_2(m)) \qquad (6)$$

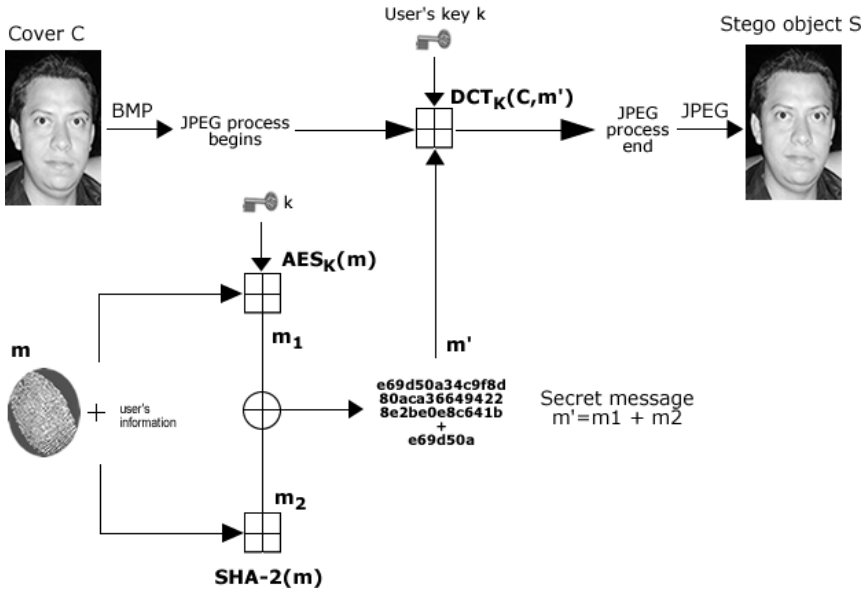

Figure 2. EIC general model.

3.2 Authentication system

We designed an application capable of answering the premise of authentication:"How do I know that you are who you claim to be?" Our authentication system responds to this question through two steps: first of all, providing the key needed to extract the user's fingerprint stored on the photograph and comparing it with a new one provided by the user. The authentication works in two different ways:

• *Locally.* In the local way, the system is able to verify a user that provides his fingerprint and password on a local machine (Figure 3). This mode may be implemented in systems that request user authentication, for example physical access in private buildings, validation of voters in elections, and so on. This form must also be able to authenticate an EIC in a portable media, see Figure 4.
•*Remotely.* The fingerprint and password are provided via Web interface. This allows the process to be remote. If the password is correct and the fingerprint matches, the server authenticates the user positively, otherwise, it rejects it. This mode is "thinking" about the security of authentication systems that need to validate users to remotely access the website, make online payments, claim privileges, etc (see Figure 5).

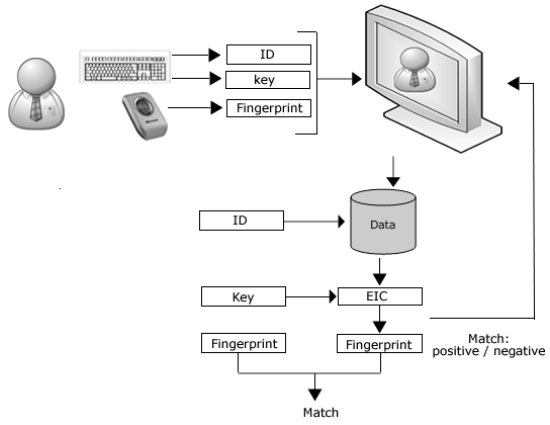

Figure 3. Local way of authentication.

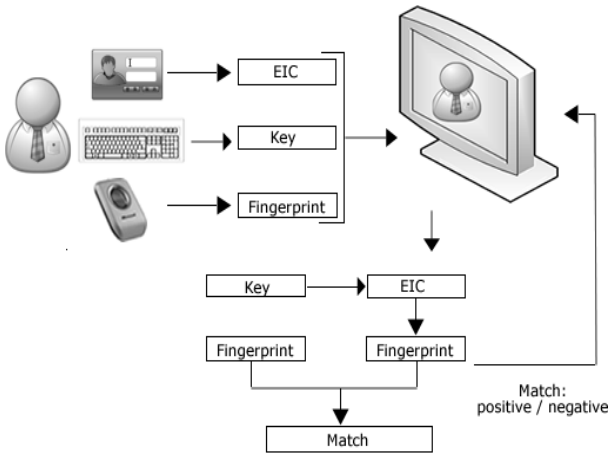

Figure 4. Local portable way of authentication.

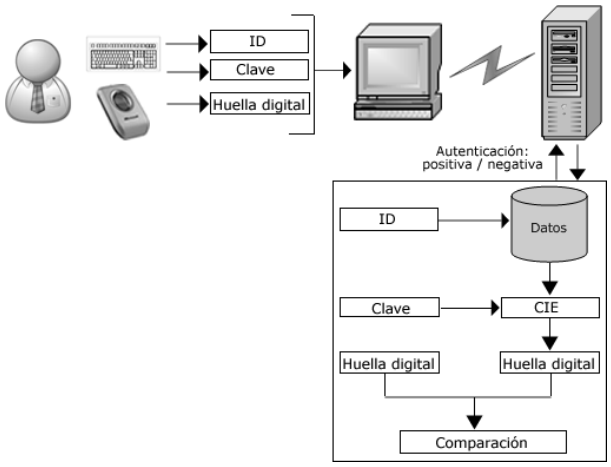

Figure 5. Remote way of authentication.

4. Implementation

4.1 Hardware and software

The hardware used to develop and test the system was

• *Laptop Toshiba Satellite A105.* Centrino Duo, 1024 mb in RAM, 120 Gb of HD, Windows Xp Professional. In this laptop, the application was

developed and it also acts as server in the remote way.

• *Laptop Dell Inspiron 5100.* Pentium IV, 756 mb in RAM, 60 Gb de Hd, Windows Home Edition. It is a client machine used in the remote tests.

• *Microsoft Fingerprint Reader.* It captures the user's fingerprint for the EIC creation and also for the matching in the authentication.

The following software was used to deploy the EIC: Java as a programming language, MySQL for database management and Tomcat (SSL-enabled) as Web server. The libraries used in the implementation of the program were

• *JCA / Bouncy Castle.* The Java Cryptography Architecture (JCA) is used to implement the cryptographic functions using Bouncy Castle as provider.
• *Java Advanced Imaging (JAI).* This is a library that lets us manipulate images, for example, by opening buffers, getting images bits, getting the image RGB representation, etc. It is useful in the image preparation phase.
• *Jpeg 6a library and the James R. Weeks* adaptation of it. This library works in the transformation and quantification phase. It was developed by an independent JPEG group. We made some modifications to this library for meeting our goals.
• *Fingerprint SDK Java 2007 by Griaule.* This is used to manipulate the fingerprint reader and get the fingerprints' characteristics.

4.2 Test environment

The goal is to provide a test scheme to monitor the operation of the EIC. We studied the behavior, characteristics and process time of the card. Two tests were designed.

Test-1

In this test we
• perform the extraction of the fingerprints' characteristics.
• make the stego-object: JPEG conversion, and the process of embedding information.
• save the stego-object in the database.
• do the user authentication.

In this test, we used the FVC2004 fingerprint database. The database consists in four sets of fingerprints. Three of them are real fingerprints, and the last one is synthetic. These sets are markedly difficult for authentication tests, due to the perturbations deliberately introduced in the fingerprint.

During the implementation of these steps, there were measured parameters such as data embedded, qDCT coefficients that are generated in each image, how many of these coefficients can be modified, the percentage of space used and the time that the process took.

Every set has 100 subsets of 8 fingerprints of the same finger. In total, we have 400 subsets with 3,200 fingerprints.

Therefore, we have fingerprints to create 400 cards, embedding the first finger of each subset in the EIC. The rest of the subset is used to conduct the matching tests.

As the users' photographs, we used the database of "computational visual" from [21]. These pictures are in JPEG format with a size of 896x592.

During the execution of these steps, we gathered parameters like embedded data size, the number of qDCT coefficients in each image, how many of them we can modify, the percentage of used space and the process time for the creation of the EIC.

Test-2

The idea of test-2 is to use a sample of users and authenticate them with a card stored on the computer. Then, intentionally, we make a sub sample of these users provide a wrong fingerprint, or replace the identity of another user; all of this to verify that they are rejected by the system. In this test the interesting factors are

- False Acceptance Rate, FAR: Authenticate and non-authorized users.
- False Rejection Rate, FRR: Rejected and authorized users.

5. Results

5.1 Test-1

From test-1, we obtain results concerning the fingerprints' quality, quantity of coefficients, space used and process time.

In the fingerprint embedded process, two fingerprints could not be embedded; therefore, 398 CIEs were successfully created.

Space

In average, the quantity of coefficients in each image was 795,648 from which 86,599 are useful for embedding information. This means that we can modify 10.8% of the coefficients; this is enough space to embed our information, as we show in the following results.

In average, the available space for embedding information was 10,824 bytes. The amount of space required for embedding information was in average 1,432 bytes. That is only the 13.2% of available space, see Figure 6.

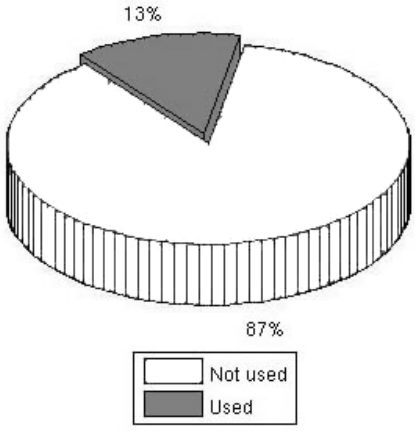

Figure 6. Amount of used space in the EIC.

Time

The total process time of the whole test was 29 minutes and 21 seconds. The reading of the 400 prints took 1 minute 3 seconds, the cryptographic/steganographic process lasted 28 minutes with 16 seconds, which gives us an average of 4.2 seconds per stego-object; the saving at the database took 4 seconds. The graphic representation can be observed in Figure 7.

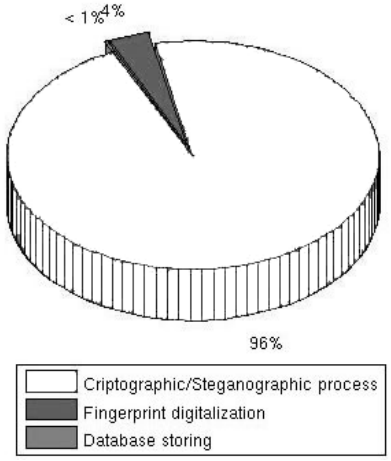

Figure 7. Process time for the EIC.

Authentication

In the authentication step, from the 398 EICs, 18 of them (4.5%) completely failed, this is, every of the seven test fingerprints cannot be successful authenticated. Then 380 CIEs (95.5%) were successfully authenticated.

Failures in authentication are caused by the difficulty of the fingerprints database that we used, and not because of the EICs generation and validation process. Actually, the failure occurs because of the matching process and the hysterisis parameters of the matching process.

5.1 Test-2

For this test, 100 users gave us each of their 10 fingerprints, making a total of 1000 samples. For each user, a total of 10 EICs were made. In the authentication process, there were only three failures (0.3% of FRR). There were anomalies in the registration process with 11 fingerprints that had difficulties because the users did not place the finger on the fingerprint reader properly.

6. Conclusions

In this work, we have created an Electronic Identification Card with a high degree of security. The card is capable of operating in local environments, with Web access or on portable devices without losing security. The users were successfully rejected or authenticated.

Not only the steganographic technique was investigated but cryptographic techniques were also used. The reason for merging these two techniques is to enhance security, while affirming that these disciplines are not competing with each other, rather they are complementary to achieve more complex and secure mechanisms.

Two schemes were created to test authentication, the local one and the remote one. Both schemes were tested and statistics on their performance were collected.
Future work:

• To explode the portability by implementing the EIC on a smart card.
• To choose the best between three samples at the time of collecting the user's fingerprint
• To get more than one fingerprint of a different finger of the user so that in case of any inconvenience suffered in a finger, the user can provide a second one.

References

[1] Condusef. *Comisión nacional para la protección de los usuarios de servicios financieros.* http://www.condusef.gob.mx/. Nov. 2007.

[2] IAFCI. *Asociación internacional de investigadores de crímenes financieros*. http://www.iafci.org/, Nov. 2007.

[3] Kay, R. *Authentication.* Computerworld 34 (2000), 77.

[4] O'Gorman, L. *Comparing passwords, tokens, and biometrics for user authentication.* Proceedings of the IEEE 91, 12 (2003), 2021-2040.

[5] Jain, A. K., and Maltoni, *D. Handbook of Fingerprint Recognition*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[6] Bogosian, J., and Charles, A. *System for verifying use of a credit/identication card including recording of physical attributes of unauthorized users.* United States Patent 5513272, Apr.1996.

[7] Piosenka, G. V., and Chandos, *R. V. Unforgeable personal identication system.* United States Patent 4993068, Feb. 1991.

[8] Burger, P. M. *Biometric authentication system.* United States Patent 6219439, Apr. 2001.

[9] DNI electrónico. *Documento Nacional de Identidad del Gobierno Español.* http://www.dnielectronico.es/, Aug. 2008.

[10] Menezes, A. J., Vanstone, S. A., and Oorschot, P. C. V. *Handbook of Applied Cryptography.* CRC Press, Inc., Boca Raton, FL, USA, 1996.

[11] Mersereau, R. M., and Alturki, F. *Secure blind image steganographic technique using discrete fourier transformation.* In ICIP (2) (2001), pp. 542-545.

[12] Provos, N., and Honeyman, P. *Hide and seek: An introduction to steganography.* IEEE Security and Privacy 1, 3 (2003), 32-44.

[13] Wayner, P. *Disappearing Cryptography: Information Hiding: Steganography and Watermark* ing (2nd Edition). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2002.

[14] Flores-Escalante, J. C. *Diseño e implementación de una credencial de identificación electrónica.* Master's thesis, Instituto Técnologico y de Estudios Superiores de Monterrey, Dec. 2008.

[15] Katzenbeisser, S., and Petitcolas, F. A., Eds. *Information Hiding Techniques for Steganography and Digital Watermarking.* Artech House, Inc., Norwood, MA, USA, 2000.

[16] Miano, J. *Compressed image file formats: JPEG, PNG, GIF, XBM, BMP.* ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 1999.

[17] Kharrazi, M., Sencar, H., and Memon., N. *Image steganography: Concepts and practice* WPS Lectures Notes Series (April 2004).

[18] Provos, N., and Honeyman, P. *Detecting steganographic content on the internet.* Tech. rep., In ISOC NDSS 02, 2001.

[19] Landau, S. *Communications security for the twenty-first century: the advanced encryption standard*. Notices of the AMS 47, 4 (April 2000), 450-459.

[20] Petitcolas, F., Anderson, R., and Kuhn, M. *Information hiding - a survey*. Proceedings of the IEEE 87, 7 (1999), 1062-1078.

[21] California Institute of Technology. *Computational visión of Technology,* Aug. 2008. ***http://www.vision.caltech.edu/***.

Authors´ Biography

Joel C. FLORES-ESCALANTE

He studied computer systems engineering at the Universidad Autónoma de Campeche in Mexico from 2000 to 2005. He got his master's degree in computer science from the ITESM-Campus Cuernavaca in Mexico in 2008. He researched in the field of network security. His areas of interest are networks, computer security, distributed systems and software development.

Jesús Arturo DÍAZ -PÉREZ

He obtained his B.Sc. degree in computer science from the Universidad Autónoma de Aguascalientes in Mexico in 1995. He got his PhD degree in computer science from the Universidad de Oviedo in Spain in 2000. He researched in the field of mobile agents. He became a full associate member of the European founded research project AgentLink. Nowadays, he is a researcher and professor at the ITESM–Campus Cuernavaca Mexico. He has been awarded by the CIGRE and by Intel for the development of innovative systems. His research fields focus in network security and wireless communications.

Roberto GÓMEZ-CÁRDENAS

He studied electronic systems engineering at ITESM-CEM from 1983 to 1987 and a received a master's degree in computer science. He got his PhD in computer science with specialization in distributed systems from the Université de Paris 8 in France in 1995. From 1995 to date, he has been a professor-researcher at ITESM-CEM. His research fields focus on operating systems, distributed systems, cryptography and network security. He is a columnist and editorial board member of the BSecure magazine and member of the conference organizing committee OPODIS.