RFID Identification Cards At 13.56 Mhz Using Biometric Techniques

BÁRBARA EMMA SÁNCHEZ RINZA,

BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA, PUEBLA, PUE. MÉXICO, BRINZA@HOTMAIL.COM

OTTO HERNÁNDEZ GONZÁLEZ

BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA, PUEBLA, PUE. MÉXICO, OTTO.HDZ@GMAIL.COM

ABSTRACT

In this work we show a system capable of identifying people from the fingerprint image, using an 8K RFID card that works wirelessly. The fingerprint images are processed through a series of techniques that improve their quality. From this template it is possible to verify the identity of the user with a 95% of accuracy.

Keywords: Tags, RFID, Fingerprints,

1. INTRODUCCIÓN

With the advance of technology, each day more and more tasks are performed in an automated fashion. Within the broad range of possibilities offered by technological development and innovation, we have observed that people authentication systems are becoming an emerging area, and consequently, biometrics is positioned as the focus of these systems.

Biometrics refers to the use of distinctive anatomical traits (in this case fingerprints), called biometric identifiers, that can automatically recognize individuals. Biometrics is becoming an essential component of effective solutions for identification, because biometric identifiers cannot be shared or lost. In addition, they represent inherently the identity of the body of an individual. The recognition of a person's body is a very powerful identity management with enormous potential.

This paper proposes using an RFID tag and with the help of people who have biometrics authentication card

2 FINGERPRINT

Fingerprints are fully formed around the seven months of fetal development and configuration of the edges of the fingers does not change during the life of the individual except due to some accidents such as scrapes or cuts. Moreover, they have the quality to be relatively stable over time. Therefore, the probability of finding two similar fingerprints is 1.9x10-15 (Badler, et, 1991)

Today fingerprints represent one of the most mature biometric technologies. A fingerprint is the representation of the surface morphology of the epidermis of a finger. It has a set of parallel lines (ridges) which are formed before birth and remain without the time to generate some kind of change or modification (Maltoni, 2009) .

In this paper we use the Galton method for checking the local characteristics as it is one of the methods in which more work has been done and several algorithms exist with relatively low computational complexity.

The method of local characteristics is based on comparison of minutiae. Minutiae or Galton's characteristics (see Figure 1) are local discontinuities in the fingerprint pattern corresponding to the lines of the fingerprint. There are different types of minutiae, but the two most important are the bifurcations and terminations, as other types of

minutiae are formed with a combination of both. For this reason, the feature extraction stage detects two types of minutiae (Komarinski, et,2005).

Figure 1. Types of minutiae in a fingerprint

To conclude, whether two fingerprints match or not, the same person performs a procedure that begins with the classification of the fingerprint till the minutiae of both tracks match.

3. BASE OF THE ACQUISITION

For an efficient biometric system, the indicators or personal traits under study must meet the following qualifications:
Permanence: the characteristic should not change with time, or do so very slowly.
Uniqueness: the existence of two people with identical property should have a very small probability.
Universality means any person should have that feature.
Quantification: the property can be measured quantitatively (Romàn, et.,2006).
The work was carried out following the steps shown in the diagram in Figure 2, which is explained below:

1.- Acquisition of the footprint that will be used to create the template which will be stored on the card.
2.- Image enhancement provide the benefit of having a better collection of minutiae.
3.- Processing of images to extract some characteristic points, which represent the essential information of each track.
4.- Identification by comparing fingerprint minutiae stored in the card.

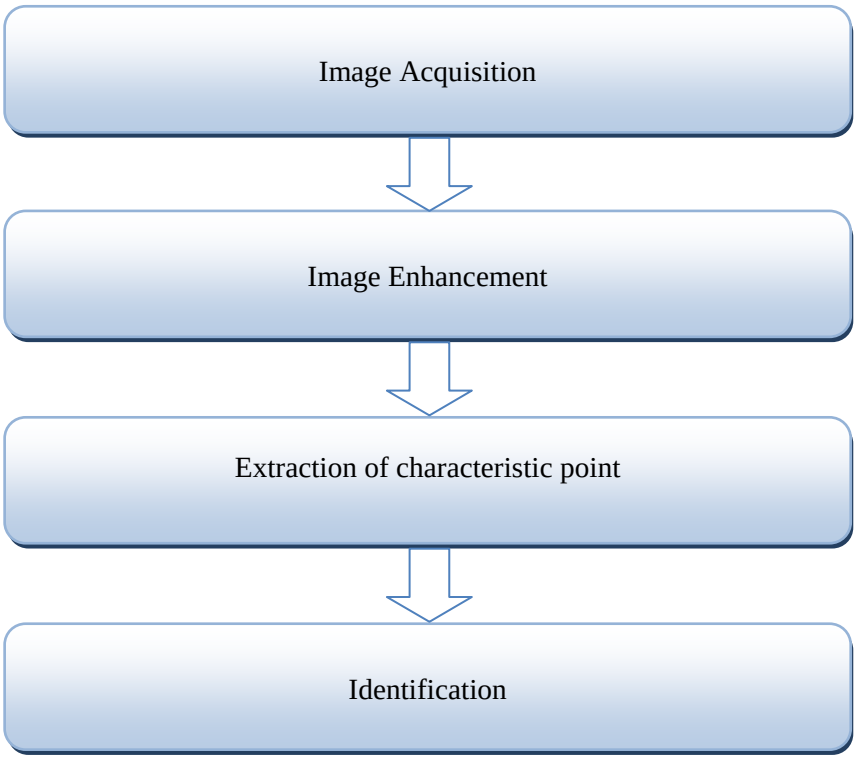

Figure 2. Diagram of steps followed by the system

4. ACQUISITION OF IMAGES

To get the image of the acquired fingerprint the "U.are.U4500 Person model" digital reader is used with the following characteristics (see Figure 3).

• Blue LED.

• Works well with dry or wet fingerprints.

• Compatible with Windows ® Vista, XP Professional, Windows Server 2000 and 2000, 2003, 2008.

• Pixel resolution: 512 dpi (on the scan area).

• Capture area: 14.6 mm (width in the center) 18.1 mm (length).

• 8-bit grayscale (256 levels of gray).

• Reader size (approximate): 65 mm x 36 mm x 15.56 mm.

• Compatible with USB 1.0, 1.1 and 2.0 (High speed).

It was decided to use this model because of the quality of reading and friendly handling.

Figure 3. Reader Digital Persona fingerprint mark

Figure 4 shows tests performed with the reader to obtain fingerprints.

Figure 4. Fingerprints acquired.

5. IMAGE PROCESSING

The main objective of digital image processing is to extract a vector of characteristics that identify the individual. As mentioned above the method used for the comparison of fingerprints is with local characteristics (Tico, et,2000)]. Obtaining minutiae has been performed in 4 steps, as shown in Figure 5.

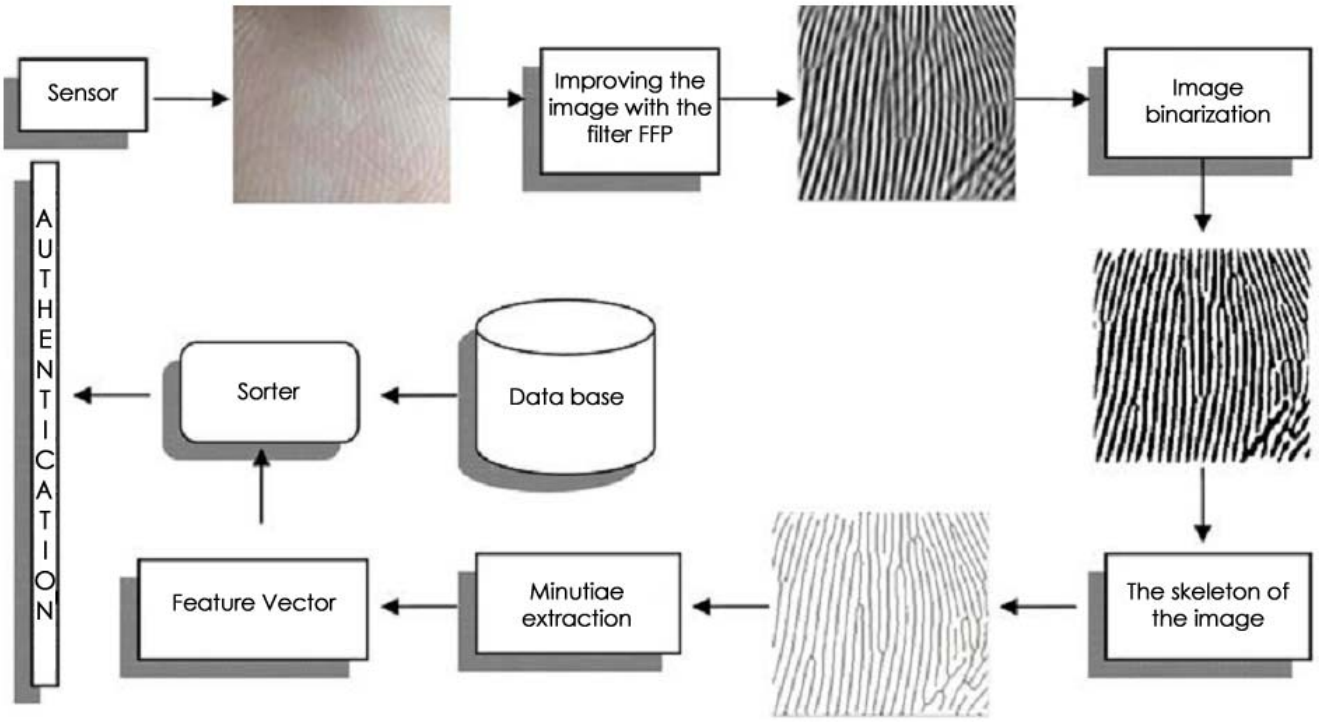

Figure 5. Steps of the algorithm to acquire the vector feature.

The feature vector was obtained from the fingerprint image that was taken with digital fingerprint reader. These images have been digitally processed to enhance the minutiae. These lines form the descriptor of the fingerprint. A classifier based on a threshold and the Pearson correlation coefficient verifies whether a new mark belongs to the claimed identity. The results show a 95% confidence for a 50 people sample.

Defining information for the system: The first to be defined before the program had started, was the way in which data would be stored inside the card. It was decided that XML should be utilized because it allows that information to be stored and transferred from card system in a structured manner.

The way in which information is structured is shown in Figure 6.

```
<?xml version="1.0" encoding="utf-8" ?>
<Persona>
  <Nombre>OTTO HERNANDEZ GONZALEZ</Nombre>
  <CURP>HEGO830511HPLRNT04</CURP>
  <IFE>2001092134241</IFE>
  <ServicioMedico>SEGURO SOCIAL</ServicioMedico>
  <NoServicioMedico>001</NoServicioMedico>
  <Licencia>99999999999999</Licencia>
  <CartillaMilitar>123456789</CartillaMilitar>
  <Cedula>6242060</Cedula>
  <Informacion>NO ES ALERGICO A NINGUN MEDICAMENTO</Informacion>
  <Imagen>Foto.jpg</Imagen>
</Persona>
```

Figure 6. XML File Structure

Then, after having studied the concepts and algorithms behind fingerprints, the system programming is performed.

6. PROGRAMMING

For the realization of the system programming, C # language is employed because it facilitates interaction with the digital fingerprint reader and RFID card reader (Klaus et, 2003), (Syed, et, 2008).
The first thing that works is the creation of the XML file, containing information identifying the person.
Figure 7 indicates the window where fingerprint images are captured. Due to the nature of the employed algorithms it is necessary to obtain four samples of the same footprint with the aim of obtaining better feature extraction footprint. Moreover, a photo and details of the person to be identified are added.
Having the vector of characteristics of the fingerprint, the XML file and the photograph of the person, obtained from a webcam, we made the introduction of the files within the RFID tag, for which you use the Memory-Stream class in C # for an array of bytes.
After storing the files in the RFID card, to start extracting process, was made the stored procedure in reverse.
Once you are able to extract data from the card is now possible to compare the fingerprint template of the fingerprint taken in this way is possible to validate whether the person is the same as it is stored.

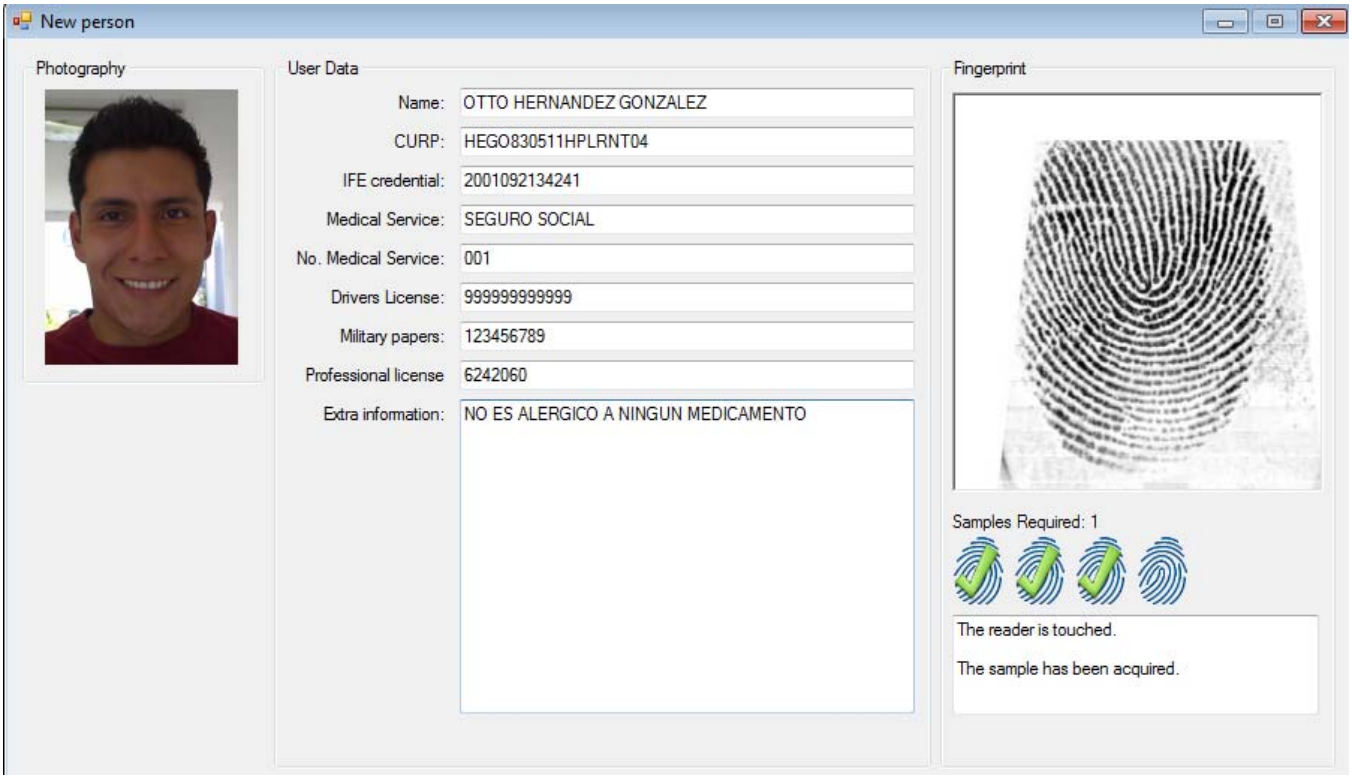

Figure7. People capture window

The feature vector is stored in a file which is stored within the RFID card, which has a capacity of 8K and whose characteristics are:

•Mifare Model
• Frequency 13.56MHz

• Protocol ISO14443A
• 8192 Byte Size
• PVC Material
• Temperature -20 - +50
• Dimension 54 × 85.6 × 0.86 (mm)

To store information on it so it is necessary to take into account the size of the information is stored. Having the vector of features, validation is performed for people with their fingerprints, the first thing you need is to load the fingerprint template, and the system returns a feature vector and compares it with the stored information for validation. Figures 8 and 9 show a positive and a negative validation.

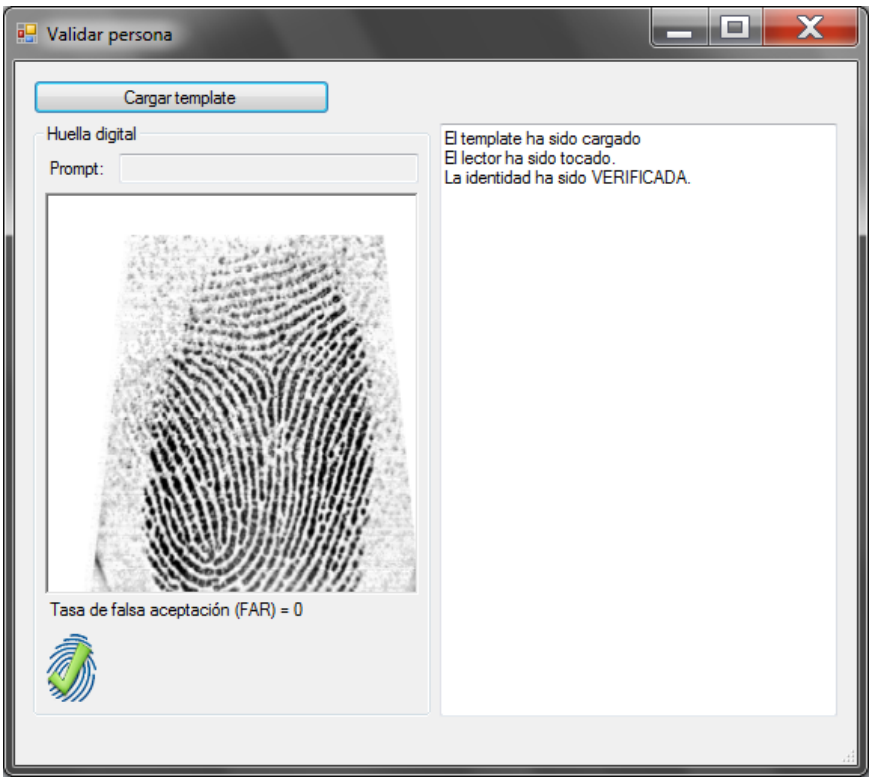

Figure 8. Validation window with the person people validated.

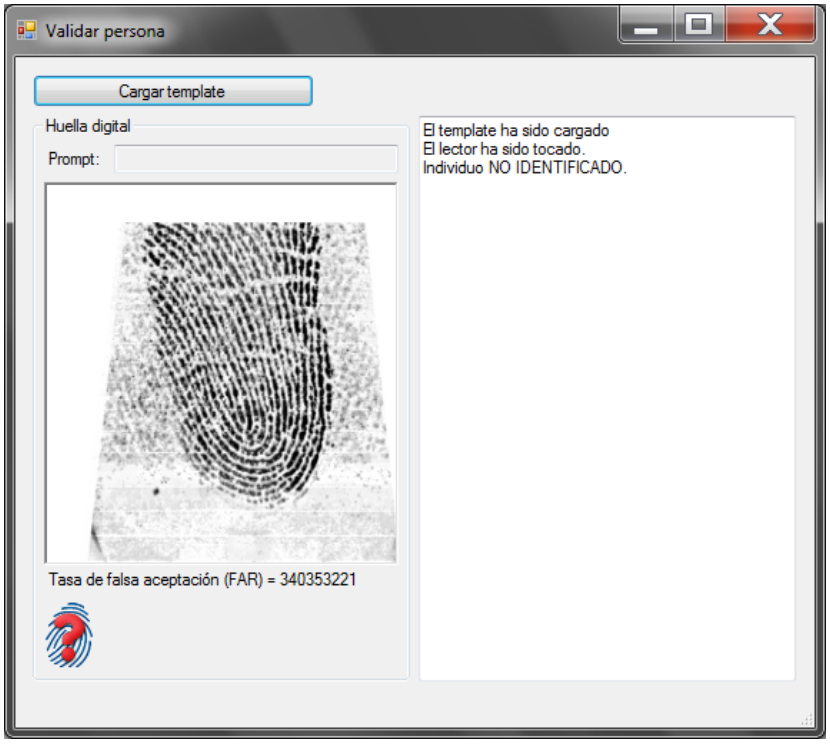

Figure9. People confirmation window with the person not validated

Once the fingerprint validation is completed, the RFID card is tested. The employed RFID system is as follows (see Figure 10):

• Model SL500
• Frequency 13.56MHz
• Protocol ISO14443A, ISO14443B, ISO15693
• USB Interface
• Temperature -20 - +50
• Dimension 110 × 80 × 26 mm
• Weight 100 g
• Windows System 98 \ 2000 \ XP \ NT \ ME \ Vista
• Maximum Range 5cm.

Figure 10: RFID Card Reader.

As with the reading of the fingerprints it was decided to use programming language C # (Bill., et,2006).

The following window has been created where the following operations are performed (see Figure 11):
• Connect the card reader
• Get the serial number on the card
• Read the information stored
• Write the information inside the card.

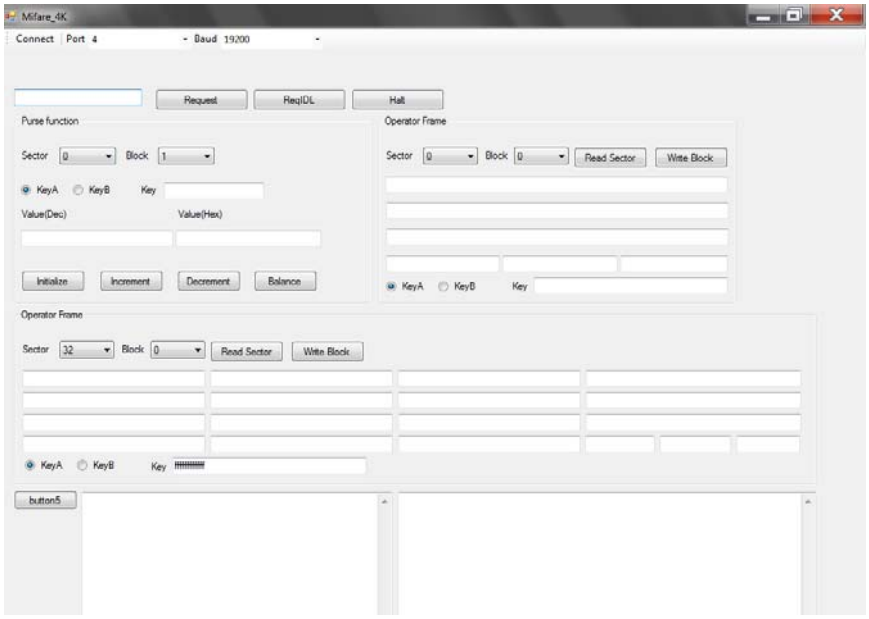

Figure 11. Window for testing the RFID card

8 CONCLUSIONS

In this work we have developed a system capable of identifying people from the fingerprint image, using an 8K RFID card that works wirelessly. The fingerprint images are processed through a series of techniques that improve their quality. From this template it is possible, with a classifier based on similarities to verify the identity of the user with a 95% of accuracy. The future work is to encrypt the information of the person to protect sensitive data.

REFERENCES

[1] Bill Glover and Himanshu Bhatt, "*RFID Essentials*", Ed. O'Reilly, Year 2006, 1-19.

[2] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, "*Handbook of Fingerprint Recognition*", Springer, Year 2009

[3] Fabio Román Arbelo, Carlos Manuel Travieso González, Jesús Bernardino Alonso Hernández, "*Autenticación De Personas A Partir De La Biometría De La Región Dígito Palmar*", Vector plus: miscelánea científico – cultural, Fundación Universitaria de Las Palmas, Nº. 27, 2006, pags. 27-34

[4] Klaus Finkenzeller, "*RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*", Ed. John Wiley & Sons, Year 2003.

[5] Marius Tico, Pauli Kuosmanen, "*An Algorithm for Fingerprint Image Postprocessing"*, Signals, Systems and Computers, 2000, vol.2, Year 2000, pages. 1735 - 1739

[6] Peter Komarinski, "*Automated Fingerprint Identificacion*", Elsevier, Year 2005

[7] Syed Ahson, Mohammad Ilyas, *"RFID Handbook: Applications, Technology, Security, and Privacy"*, Ed. CRC Press, London New York, Year 2008, Pages 13-15.

[8] W. Badler. *"Dermatoglyphics"*,Science transition. Vol. 9. 1991. pp. 95.

Autorización y Renuncia

Los autores autorizan a LACCEI para publicar el escrito en las memorias de la conferencia. LACCEI o los editores no son responsables ni por el contenido ni por las implicaciones de lo que esta expresado en el escrito