Smart card with iris recognition for high security access environment

Mohammed A. M. Abdullah F. H. A. Al-Dulaimi
Computer Engineering Department,
University of Mosul,
Mosul, Iraq
m.am_86@yahoo.com

Waleed Al-Nuaimy Ali Al-Ataby
Department of Electrical Engineering and Electronics,
University of Liverpool.
Liverpool, L69 3GJ, UK
wax@liv.ac.uk

Abstract— **Smart cards are increasingly being used as a form of identification and authentication. One inherent problem with smart cards, however, is the possibility of loss or theft. Current options for securing smart cards against unauthorized use are primarily restricted to passwords. Passwords are easy enough for others to steal so that they do not offer sufficient protection. This has promoted interest in biometric identification methods, including iris recognition. The iris is, due to its unique biological properties, exceptionally suited for identification. It is protected from the environment, stable over time, unique in shape and contains a high amount of discriminating information.**

This paper proposes a method to integrate iris recognition with the smart card to develop a high security access environment. An iris recognition system and smart card programming circuit with its software have been designed. Template on card (TOC) category has been employed. Hence, the extracted iris features stored in smart card are compared against the data acquired from a camera or database for authentication. The proposed algorithm has superior performance in terms of security, accuracy and consistency compared with other published technology.

Keywords- Iris recognition; Wavelets; biometrics; smart card.

I. INTRODUCTION

Smartcards are currently used as a secure and tamper-proof device to store sensitive information such as digital certificates, private keys and personal information. Access to smartcards has historically been regulated by a trivial means of authentication: the Personal Identification Number (PIN). A user gains access to a card if he/she enters the right PIN. Experience shows that PINs are weak secrets in the sense that they are often poorly chosen and easy to lose [1]. Moreover, many actual implementations that use the PIN consider the channel between host and smart-card to be secure. So, they simply send the PIN in a clear communication. This implies many easy attacks [2]. A simple Trojan on the host could easily sniff the PIN and store it for future usage. Biometric technologies have been proposed to strengthen authentication mechanisms in general by matching a stored biometric template to a live biometric template [3]. In case of authentication to smartcards, intuition imposes the match to be performed by the smartcard but this is not always possible because of the complexity of biometric information, such as fingerprints or iris scans, and because of the yet limited computational resources offered by currently available smartcards. In general, three strategies of biometric authentication can be identified [3]:

- Template on Card (TOC). The biometric template is stored on a hardware security module. It must be retrieved and transmitted to a different system that matches it to the live template acquired by special scanners from the user.
- Match on Card (MOC). The biometric template is stored on a hardware security module, which also performs the matching with the live template. Therefore, a microprocessor smartcard is necessary, which must be endowed with an operating system running suitable match applications.
- System on Card (SOC). This is a combination of the previous two technologies. The biometric template is stored on a hardware security module, which also performs the matching with the live template, and hosts the biometric scanner to acquire, select and process the live template.

II. IRIS RECOGNITION SYSTEM

The iris is the colored portion of the eye that surrounds the pupil as shown in Fig. 1. It controls light levels inside the eye similar to the aperture of a camera. The round opening in the center of the iris is called the pupil. The iris is embedded with tiny muscles that dilate and constrict the pupil size. It is full of richly textured patterns that are distinct from person to person, and in fact are distinct from left eye to right eye of the same person. Compared with other biometric features such as face and fingerprint, iris patterns are highly stable and unique as the probability for the existence of two irises that are same has been estimated to be very low, *i.e.* one in 10^{72} [4].

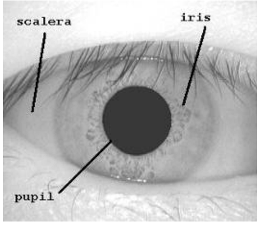

Figure 1. Image of the eye.

Generally, an iris recognition system is composed of many stages as shown in Fig. 2. Firstly, an image of the person's eye is captured and preprocessed. Secondly, the image is localized to determine the iris boundaries. Thirdly, the iris boundary coordinates are converted to the stretched polar coordinates to normalize the scale and illumination of the iris in the image. Fourthly, features representing the iris patterns are extracted based on texture analysis. Finally, the person is identified by comparing his/her features with an iris feature database.

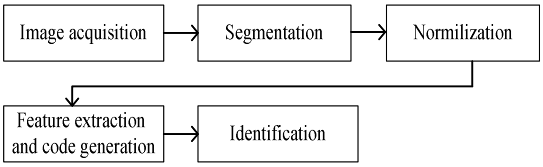

Figure 2. Block diagram of an Iris Recognition System

978-1-4244-7000-6/11/$26.00 ©2011 IEEE

A. Segmentation

The part of the eye carrying information is only the iris part. It lies between the scalera and the pupil. Hence the next step after acquiring the image is to separate the iris part from the eye image. The image was filtered using Gaussian filter, which blurs the image and reduces effects due to noise. The iris inner and outer boundaries are located by finding the edge image using the Canny edge detector, then using the Hough transform to find the circles in the edge image. For every edge pixel, the points on the circles surrounding it at different radius are taken, and their weights are increased if they are edge points too, and these weights are added to the accumulator array. Thus, after all radiuses and edge pixels have been searched, the maximum from the accumulator array is used to find the center of the circle and its radius according to the equation:

$$X^2 + Y^2 = r^2 \qquad (1)$$

Where *X, Y* are the center of the circle and *r* is the radius of the circle. The highest two points in the Hough space correspond to the radius and center coordinates of the circle best defined by the edge points. Fig.3 shows the segmented eye image.

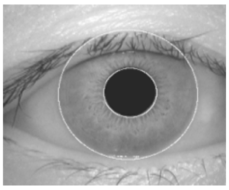

Figure 3. Segmented Eye Image.

The main advantages of the Hough transform technique are its tolerance for gaps in feature boundary descriptions and robustness to noise [5]. However, Hough transform is computationally intensive. This drawback is overcome by using C++ language for performing the Hough transform after scaling the image down by 60%. Moreover, The Hough transform is performed for the iris outer boundary using the whole image, and then for the pupil only instead of the whole eye, because the pupil is always inside the iris.

B. Normalization

Once the iris region is segmented, the next stage is to normalize this part, to enable generation of the "iriscode" and their comparisons. Since variations in the eye, like optical size of the iris, position of pupil in the iris, and the iris orientation change person to person, it is required to normalize the iris image so that the representation is common to all with similar dimensions. Normalization process involves unwrapping the iris and converting it into its polar equivalent as shown in Fig. 4 [6].

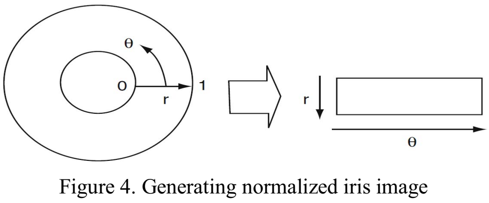

Figure 4. Generating normalized iris image

The remapping of the iris region from the Cartesian coordinates to the normalized non-concentric polar representation is modeled as:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \qquad (2)$$

with:

$$x(r,\theta) = (1-r)x_p(\theta) + rx_i(\theta) \qquad (3)$$

$$y(r,\theta) = (1-r)y_p(\theta) + ry_i(\theta) \qquad (4)$$

where *I(x,y)* is the iris region image, *(x,y)* are the original Cartesian coordinates, *(r,θ)* are the corresponding normalized polar coordinates, and x_p, y_p and x_i, y_i are the coordinates of the pupil and iris boundaries along the θ direction. In this model a number of data points are selected along each radial line (defined as the radial resolution) [7]. The previous normalization process is demonstrated by Fig. 5.

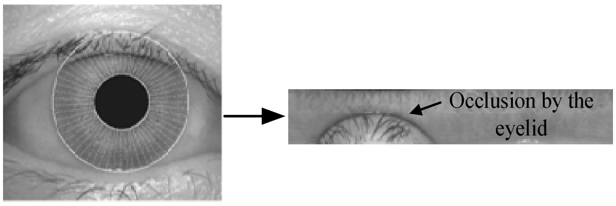

Figure 5. Normalized iris image

Since in most cases the upper and lower parts of the iris area are occluded by eyelid, it was decided to use only the left and right parts of the iris area for iris recognition. Therefore, the whole iris [0, 360°] is not transformed in the proposed system. Experiments were conducted by normalizing the iris from [-32, 32°] and [148, 212°], ignoring both upper and lower eyelid areas as indicated in Fig. 6.The size of the rectangular block is reduced accordingly. Left and right images each one of size 112×60 are obtained. By applying this approach, detection time of upper and lower eyelids and 64.4% cost of the polar transformation are saved. Results have shown that information in these portions of iris is subjective for iris recognition.

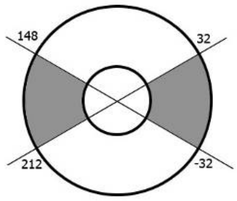

Figure 6. Ignoring upper and lower part of iris

C. Feature extraction

The Wavelet transform is used to extract features from the enhanced iris images. Haar wavelet is used as the mother wavelet. The Wavelet transform breaks an image down into four sub-sampled images. The results consist of one image that has been high-pass filtered in the horizontal and vertical directions (*HH* or diagonal coefficients), one that has been low-pass filtered in the vertical and high-pass filtered in the horizontal (*LH* or horizontal coefficients), one that has been low-pass filtered in the horizontal and high-pass filtered in the vertical (*HL* or vertical coefficients), and one that has been low-pass filtered in both directions (*LL* or details coefficient).

In order to generate the binary data, feature vector is encoded by using two and four level quantization as shown in Fig. 7, which shows the process used for obtaining the feature vectors with the optimized dimension. Here, *H* and *L* refer to the high-pass and the low-pass filter, respectively, and *HH* indicates that the high-pass filter is applied to the signals of both axes.

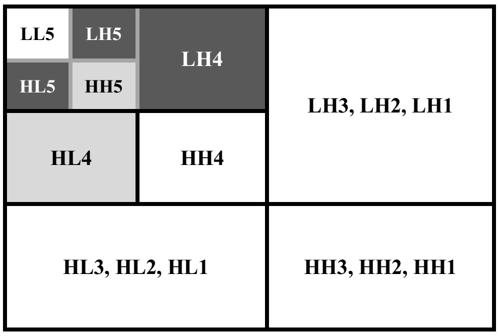

Figure 7. Organization of feature vector (Black indicates 4 levels quantization, grey indicates two levels quantization)

D. *Identification*

The last module of an iris recognition system is used for matching two iris templates. Its purpose is to measure how similar or different the templates are and to decide whether they belong to the same individual or not. An appropriate match metric can be based on direct point-wise comparisons between the phase codes [8]. The test of matching is implemented by the XOR operator that is applied to the encoded feature vector of any two iris patterns. The XOR operator detects disagreement between any corresponding pair of bits. The system quantifies this matter by computing the percentage of mismatched bits between a pair of iris representations, *i.e.*, the normalized Hamming distance. Let *X* and *Y* be two iris templates to be compared and *N* be the total number of bits so, *HD* is equal to the number of disagreed bits divided by *N* as shown in equation 5.

$$HD = \frac{1}{N}\sum_{j=1}^{N} X_j \oplus Y_j \qquad (5)$$

In order to avoid rotation inconsistencies which occur due to head tilts, the iris template is shifted right and left by 8 bits. It may be easily shown that scrolling the template in polar coordinates is equivalent to iris rotation in Cartesian coordinates [9]. The system performs matching of two templates several times while shifting one of them to four different locations. The smallest HD value amongst all these values is selected, which gives the matching decision.

III. BIOMETRIC SMART CARD

Biometric technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics. Biometric technologies, when used with a well-designed ID system, can provide the means to ensure that an individual presenting a secure ID credential has the absolute right to use that credential. Smart cards have the unique ability to store large amounts of biometric and other data, carry out their own on-card functions, and interact intelligently with a smart card reader. Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology. According to the definition smart card is "a device that includes an embedded integrated circuit that can be either a secure microcontroller or intelligent equipment with internal memory" [10].

A. *Employed Smart Card*

A well known type of smart cards is the Fun Card. The Fun card belongs to microprocessor-contact smart card. It consists of the AT90S8515 microcontroller which is a low-power CMOS 8-bit microcontroller and the AT24C64 EEPROM which provides 65,536 bits (8KB) of serial electrically erasable and programmable read only memory [11].

B. *Smart Card Programmer*

The smart card programmer has been designed to enable read/write from/to the smart card. The programmer is connected to the PC using the parallel port, due to its higher speed compared with serial port and the ability to generate multiple signals at the same time.

The block diagram shown in Fig. 8 consists of four parts which are: signal selection circuit, voltage interfacing circuit, connection pins to the parallel port, and connection pins to the smart card. Where C1-C8 are the pins of the smart card and S0-S2 are the selecting signals.

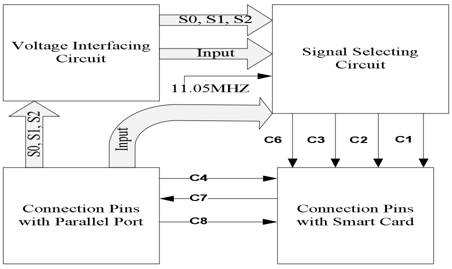
Voltage Interfacing Circuit
S0, S1, S2
Input
11.05MHZ
Signal Selecting Circuit
S0, S1, S2
Input
C6
C3
C2
C1
C4
C7
C8
Connection Pins with Parallel Port
Connection Pins with Smart Card

Figure 8. The block diagram of designed programmer

Table 1 shows the function of each pin in the used smart card.

TABLE 1. DESCRIPTION OF EACH PIN USED IN SMART CARD

Pin No.	Name	Function	Direction
C1	Vcc	Power supply 5 VDC	In
C2	Reset	CPU Reset line	In
C3	XTAL	Main clock up to 11 MHz	In
C4	MOSI	SPI master input	In
C5	Vss	Power Ground	In
C6	Nc	Not Connected	–
C7	MISO	SPI Master output	Out
C8	SCK	SPI serial clock	In

C. *Integrating Iris Recognition with Smart Card*

After extracting data from iris image, it is saved in the smart card's flash memory using the smart card programmer. Extracted iris features stored in smart card are compared against the acquired data from the camera or the database to confirm that a person is authenticated or not. In order to protect the data against manipulation, a signature of the data has been generated using the MD5 hash function [12], which produces 18 bytes signature, and then saved in the smart card. Hence, in the identification process, the system generates the biometric template and its signature from the acquired data and compare them against the smart card contents. In case of finding any difference between the generasted and the saved template or signature, the identification is rejected. Fig. 9 shows the block diagram of the designed system.

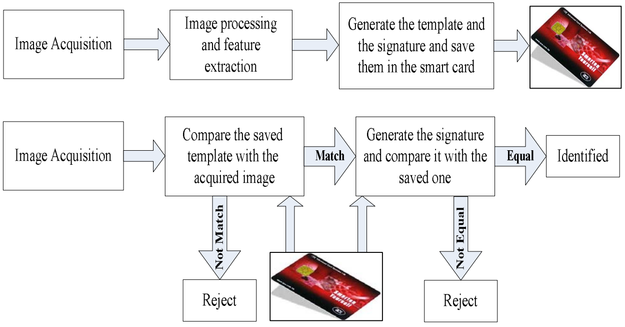
Image Acquisition
Image processing and feature extraction
Generate the template and the signature and save them in the smart card
Image Acquisition
Compare the saved template with the acquired image
Match
Generate the signature and compare it with the saved one
Equal
Identified
Not Match
Not Equal
Reject
Reject

Figure 9. The block diagram of the designed system.

IV. RESULTS

Iris images are obtained from the Chinese Academy of Sciences Institute of Automation CASIA Ver. 1 database [13]. The database consists of 756 iris images from 108 classes. Experiments were performed using different combinations of wavelet coefficients and the results are compared to find the best as shown in Table 2. The selected combination gives the best Correct Recognition Ratio (CRR) for a minimum feature vector of length 236 bits only.

After pre-processing and feature extraction, the template is saved in the card's EEPROM using the designed card programmer. Concurrently, a signature for the template has been generated using the MD5 hash function, and saved on the smart card. Table 3 shows the time of reading, writing of the smart card programmer and the memory utilization.

TABLE 2. COMPARISON AMONG MULTIPLE WAVELET COEFFICIENTS.

Combinations	Quantization	CRR	Vector Size
CH4 (D&V)[a]	2 bits	67%	112 bits
CH4 (V&H)	2 bits	72%	112 bits
CH4 (D&H)	2 bits	68%	112 bits
CH4 (D&V) + CH5 (V)	2 bits	75%	126 bits
CH4 (D&V) + CH5 (H)	2 bits	80%	126 bits
CH4 (D&V) + CH5 (D&V)	2 bits	81%	140 bits
CH4 (D&V&H)	2 bits	84%	162 bits
CH4 (H) + CH5 (H)	4 bits	90%	140 bits
CH4 (H) + CH5 (V)	4 bits	88%	140 bits
CH4 (H) + CH5 (V&H)	4 bits	94%	168 bits
CH4 (D) + CH5 (V&H)	4 bits	70%	168 bits
CH4 (V) + CH5 (V&H)	4 bits	66%	168 bits
CH4 (D&H)	4 bits	90.5%	224 bits
CH4 (D&V)	4 bits	60%	224 bits
CH4 (V&H)	4 bits	86.5%	224 bits
CH5 (V&H)	4 bits	52%	224 bits
CH5 (V&D)	4 bits	47%	224 bits
CH4 (V&H) + CH5 (V)	4 bits	89%	252 bits
CH4 (V&H) + CH5 (H)	4 bits	92.5%	252 bits
CH4 (D&V) + CH5 (D&V)	4 bits	63%	280 bits
CH4 (V&H) + CH5 (V&D)	4 bits	88%	280 bits
CH4 (V&H) + CH5 (V&H)	4 bits	94.5%	280 bits
CH4 (V&D&H)	4 bits	89%	336 bits
CH4 $(H)_4$ + CH4 $(V)_2$ CH5 $(V)_4$ + CH5 $(H)_4$ + CH5$(D)_2$	2 bits and 4 bits	98.6%	236 bits

a. *D*: REPRESENTS DIAGONAL COEFFICIENTS, *H*: REPRESENTS HORIZONTAL COEFFICIENTS AND *V*: REPRESENTS VERTICAL COEFFICIENTS.

TABLE 3. READING TIME, WRITING TIME AND MEMORY UTILIZATION

Smart card writing time	6 Sec.
Smart card reading time	3 Sec.
Memory utilization	380[a] bits out of 8KB (4.63%)

a. 236 BITS FROM THE FEATURE VECTOR + 144 BITS FROM THE HASH FUNCTION

V. CONCLUSION

The experimental results clearly demonstrate that the feature vector consisting of concatenating *LH4*, *HL4*, *LH5*, *HL5*, and *HH5* gives the best results. On the other hand, the Haar wavelet is particularly suitable for implementing high-accuracy iris verification/ identification systems, as the feature vector length is at least with respect to other wavelets. In identification mode, the CRR of the proposed algorithm was 98.6% with template size of 236 bits. Such vector size can be easily stored on smart cards and participate to reduce the matching and encoding time tremendously.

The proposed system is characterized by having less computational complexity compared to other methods. Based on the comparison results shown, it can be concluded that the proposed method is promising in terms of execution time and performance of the subsequent operations due to template size reduction.

REFERENCES

[1] G. Bella, S. Bistarelli, and F. Martinelli, "Biometrics to Enhance Smartcard Security". Lecture Notes in Computer Science, vol. 3364, 2005.

[2] M. Bond, and P. Zielinski, "Decimalization table attacks for pin cracking". Technical Report UCAM-CL-TR-560, University of Cambridge, Computer Laboratory, 2003.

[3] L. Bechelli, S. Bistarelli, and A. Vaccarelli, "Biometrics authentication with smartcard". Technical Report, CNR, Istituto di Informatica e Telematica, Pisa, 2002.

[4] H. Proença, and A. Alexandre, "Towards noncooperative iris recognition: A classification approach using multiple signatures". IEEE Trans. vol. 29, pp. 607-612, 2007.

[5] S.K. Pedersen, "Circular Hough Transform". Aalborg University, Vision Graphics and Interactive Systems, 2007.

[6] M. Nabti, and A. Bouridane, "An effective and fast iris recognition system based on a combined multiscale feature extraction technique". Pattern Recognition, vol. 41, pp. 868–879, 2008.

[7] J. Daugman, "How Iris Recognition Works". IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21-30, 2004.

[8] R. Schalkoff, "Pattern Recognition: Statistical, Structural and Neural Approaches". John Wiley and Sons, ISBN: 0471529745, 2003.

[9] J. Daugman, "Statistical Richness of Visual Phase Information :Update on Recognizing, Persons by Iris Patterns". International Journal of Computer Vision, Vol. 45, Issue 1, pp. 25-38, 2001.

[10] Smart Cart Alliance Identity Council. Identity and Smart Card Technology and Application Glossary, 2007. Available online: http://www.smartcardalliance.org

[11] Atmel Cooperation, AT90S8515 Microcontroller Datasheet. Available online: http://www.atmel.com/dyn/resources/prod_documents/doc0841.pdf

[12] The MD5 Message-Digest Algorithm. RFC 1321, section 3.4, "Step 4. Process Message in 16-Word Blocks", page 5.

[13] Center of Biometrics and Security Research, Iris Database, CASIA V1. Available online: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp