Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, No. 2, October : 2023

HIGH PERFORMANCE OF SMARTCARD WITH IRIS RECOGNITION FOR HIGH SECURITY ACCESS ENVIRONMENT IN PYTHON TOOL

SUDHAKAR ALLURI[1], Karnati Mahidhar[2], Kalluru Kavya[3], Dulam Srija[4] P.Venkatapathi[5]
[1,2,3,4,5] Department of ECE, CMR Institute of Technology, JNTU Hyderabad, Telangana state, India.
sudhakaralluri709@gmail.com, mahidhar.12393.km@gmail.com, kavya1712003@gmail.com, srija.dulams4165@gmail.com, pvpathi@gmail.com

Abstract
Smartcards are used for authentication and identifying purposes. The risk of loss or theft associated with smartcards, however, is a significant issue. Passwords are currently the only real solution for protecting smartcards against unauthorized use. Passwords don't provide enough security because they are simple enough for others to obtain. This has increased interest in iris recognition and other biometric identification techniques. Due to its special biological characteristics, the iris is ideally suited for identification. It has a high concentration of discriminating information, is highly stable over time, is sheltered from the environment, and has a distinctive shape. This research suggests a technique for creating a high security access environment by fusing iris recognition with the smart card. A smart card programming circuit and iris recognition system have been developed. The TOC category, or template on card, has been used. The hash of the data obtained from a camera or database is compared to the hash of the extracted iris features saved in the form of a smartcard for authentication. Results indicate that when compared to other technology (MD5), the SHA safe hash algorithm performs better in terms of security, accuracy, and consistency.
Keywords: Smartcard, Iris, MD5, SHA, Python & Arduino.

I. Introduction

The conventional smartcard, created in 1974 [1], has through numerous development stages over time. These days, the card comes with a CPU, memory, and input/output handler and is the size of a credit card. Smart cards become more secure media, appropriate for use in a variety of applications that allow biometric methods of identification, when unique traits of persons are added to the smart card chip. UK's Asylum Seekers are one such instance.

Both a fingerprint template and a photo are kept on the card's smartcard chip for biometric identification [2]. Regarding their basic technological characteristics and the forms of authentication they offer, we may distinguish between three types of smartcards in the biometric identification process. Template-on-card (TOC), Match-on-card (MOC), and System-on-card (SOC) are the three different types of smart cards [3]. In this piece, Hash data is stored on smartcards of the TOC type. A smart card is described as "a device that includes an embedded integrated circuit that can either be a secure microcontroller or intelligent equipment with internal memory" [4].

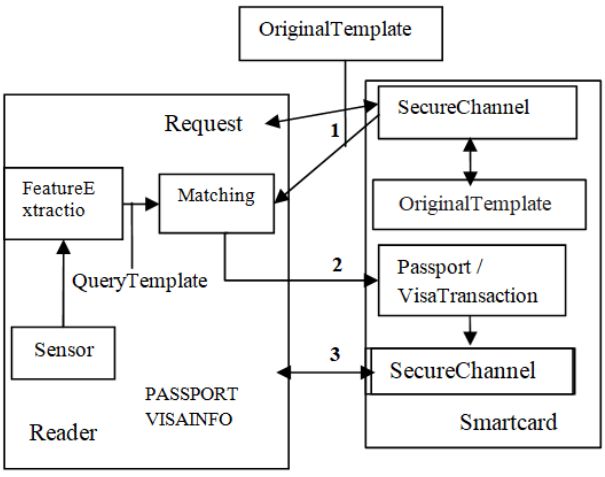

Figure 1 Authentication Process in a TOC System

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, No. 2, October : 2023

Currently, critical data like digital certificates, private keys, and personal information are kept on smartcards, which are safe and impervious to tampering. A has historically controlled smartcard access. The Personal Identification Number (PIN) is a simple authentication method. If a user enters the proper PIN, they can access a card. PINs are weak secrets, according to experience, as they are frequently picked carelessly and are simple to forget [5]. Furthermore, a lot of PIN implementations in practice believe the communication path between the host and the smart card to be safe. So they simply communicate the PIN in a simple manner. This suggests a lot of simple attacks [6]. On the host, a straightforward Trojan could quickly sniff the PIN and store it for later use. By comparing a saved biometric template to a live biometric template, biometric technologies have been proposed to increase authentication processes generally [7]. In the case of smartcard authentication, common sense dictates that the smartcard must perform the match, but this is not always possible due to the complexity of biometric data, such as fingerprint or iris scans, and the currently available smartcards' still-limited computational capabilities. Three basic methods of biometric authentication can be found [7]. ToC , MOC, and SOC stand for Template on Card, Match on Card, and System on Card, respectively. This phase focused mostly on the Template on Card (TOC).

Biometric Technology: A biometric system automatically recognizes a person based on some form of distinctive feature or attribute the person possesses.

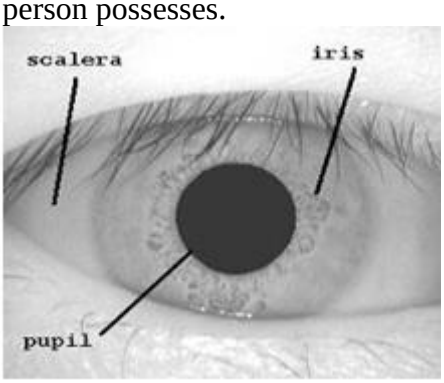

Fig. 2 shows the human eye from the front.

The iris, which is the colorful area of the eye that encircles the pupil and is depicted in Figure 2 as a thin, circular diaphragm, is located between the cornea and the lens of the human eye. The pupil size can vary from 10% to 80% of the iris diameter, and the average iris diameter is 12 mm [8]. The biometric sample is then converted into a biometric template utilizing some kind of mathematical function. This will give the feature a normalized, effective, and representation that may then be compared with other templates in an unbiased manner.

II. **IRIS RECOGNITION SYSTEM**

As seen in picture 1, the iris is the colorful area of the eye that encircles the pupil. An iris recognition system is made up of several stages, starting with the preprocessing and collection of an individual's ocular picture. The iris boundaries are then determined by localizing the image a second time. Thirdly, the scale and lighting of the iris in the image are normalized by converting the iris border coordinates to stretched polar coordinates. Fourthly, depending on the study, characteristics that represent the iris patterns are retrieved. The code is then produced. The individual is then recognized by matching his or her code with an iris database. As shown in Fig. 3, these steps are image acquisition, segmentation, normalization, feature extraction, and code creation.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, No. 2, October : 2023

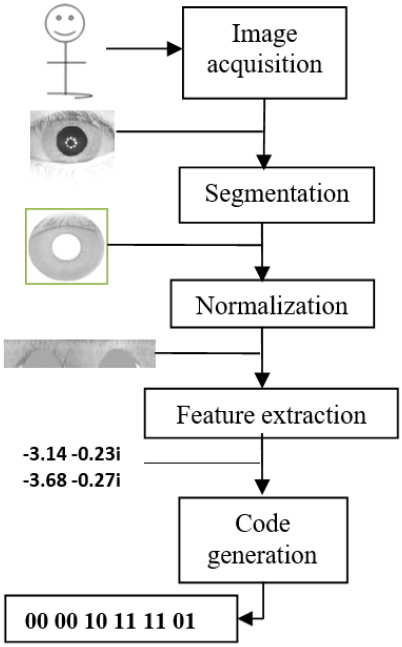

Fig.3IrisRecognitionSystem

2.1 Segmentation

Isolating the actual iris region in a digitized eye image is the first step in iris identification. The quality of the eye pictures imaging will determine how well segmentation works. Due to the use of near infrared light for illumination, the images in the CASIA iris database [10] do not have specular reflections. By segmenting, Canny does this. Edge Detection by Canny is a multi-step edge detection process that goes like this

$$g(m,n)=G_\sigma(m,n)*f(m,n)$$

Where

$$G_\sigma = (1/\sqrt{(2\pi\sigma^2)}\exp\left[-(m^2+n^2)/2\sigma^2\right.$$

Compute gradient of g(m,n) using any of the gradient operations(Roberts, Sobel, Prewitt, etc)

$$\text{To get } M(n,n) = \sqrt{(g_m{}^2(m,n) + g_n{}^2(m,n))}$$

$$\theta(m,n)=\tan^{-1}[g_n(m,n)/g_m(m,n)]$$

Threshold M:

$$M_T(m,n)= \begin{cases} M(m,n) & \text{if } M(m,n)>T \\ 0 & \text{otherwise} \end{cases}$$

where T is so chosen that all edge elements are kept while most of the noise is suppressed.
Neglecting the Upper and Lower Iris It was determined to solely use the left and right regions of the iris area for iris recognition because the upper and lower parts of the iris area are typically covered by eyelids. Therefore, the whole iris [0, 3600] is not transformed in the proposed system. Experiments are to be conducted by normalizing the iris from [-32, 320] and [148, 2120], ignoring both upper and lower eyelid areas as indicated in fig 4.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, No. 2, October : 2023

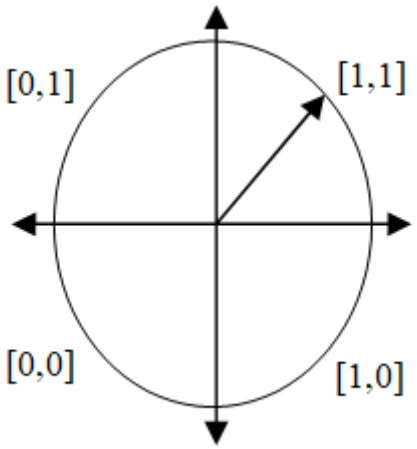

Fig.4 Generating Normalized Iris Image

2.2 Normalization

The Hough transform is a common computer vision method that can be used to identify the properties of basic geometric objects like lines and circles that are visible in a picture. The radius and center coordinates can be determined using the circular Hough transform.

Rubber Sheet Model the homogenous rubber sheet model devised by Daugman [8], [9] remaps each point within the iris region to a pair of polar coordinates (r,θ) where r is on the interval [0,1] and θ is angle [0,2π]

The rectangular block is appropriately shrunk in size. Each image on the left and right is 11260 in size. Utilizing this strategy, upper and lower eyelid detection times can be shortened.

2.3 Proposed System

1. To establish a highly secure and effective access control solution, the project suggests integrating iris recognition technology with smart card systems.
2. The project intends to improve the authentication process, guaranteeing that only authorised people have access to secure areas by fusing the distinct biometric qualities of the iris with the adaptability of smart cards.
3. To complete this integration, an iris recognition system, a smart card programming circuit, and related software will be designed and put into use.
4. For authentication, the project uses the Template on Card (TOC) category, in which iris features are extracted, safely stored on the smart card, and compared with information obtained from a camera or database

2.4 Feature Extraction

Gabor filters can offer the best joint representation of a signal in both spatial frequency and space. A sine/cosine wave is modulated with a Gaussian to create a Gabor filter. Since a sine wave is perfectly localised in frequency but not in space, this can offer the best combined localization in both of those areas. It is possible to decompose a signal using a quadrature pair of Gabor filters. The Gabor filter has the drawback that whenever the bandwidth exceeds an octave, the even symmetric filter will have a DC component [15].

A Log-Gabor filter's frequency response is given as

G() = exp (log (/0)z), where f stands for the centre

The iris region is remapped as follows from Cartesian coordinates to the normalized non-concentric polar representation:

I (x (r,), y (r,)) I (r,) where I(x,y) is the iris region image, (x,y) are the original cartesian coordinates, (r,) are the corresponding normalized polar coordinates, and xp, yp, and xi, yi are the coordinates of the pupil and iris boundaries along the direction.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, No. 2, October : 2023

III Iris Coding

The radial resolution in this model is the number of data points chosen along each radial line.
2(log (/0) z represents the frequency, and represents the filter's bandwidth. Field [15] examines the Log-Gabor filter's specifics.
Code Iris
Once the iris feature has been recovered, the output will be used to create the iris code using the phase quantization technique. If both the real and imaginary components of the phase quantization are positive, the number 11 is allocated. When both the real and imaginary components are negative, the value 00 is assigned. Additionally, if the imaginary component is -ve and the real part is +ve, the value 10 is assigned.

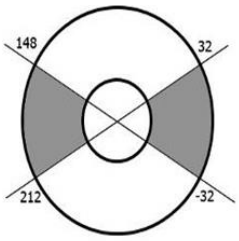

Fig.5 Ignoring Upper and Lower Part of Iris

The fifth version of the message digest algorithm is known as MD5, or the Message-digest Algorithm 5. The theory behind this technique was presented in a document named "The MD5 Message-Digest Algorithm" by Ronald L. Rivest to the IETF (The Internet Engineering Task Force) in August 1992. MD, MD2, MD3, and MD4 were used to create MD5 [17]. Any length of data can be compressed into a 128-bit message digest, and this segment message digest frequently asserts to be a digital fingerprint of the contents. To perform the circular operation, this approach employs a number of non-linear algorithms, making it impossible for crackers to recover the original data. Such an algorithm is referred to as an irreversible algorithm in cryptography. Can successfully stop data leakage brought on by inverse operation. Because the usage of the MD5 algorithm requires no royalties payments, takes less time, and costs less money, both the theory and practise have high levels of security.

IV SECURE HASH ALGORITHM

The use of cryptographic hash functions is crucial in contemporary cryptography. In many different applications, including password protection, secure protocols, digital signatures, and others, they are frequently employed.
The National Institute of Standards and Technology (NIST) has released a number of cryptographic hash functions under the name Secure Hash Algorithm (SHA). Federal Information Processing Standard Publication (FIPS PUB) 180 was the title of NIST's 1993 proposal for the SHA-0, and the organization later unveiled the SHA-1, an updated version.
SHA-0 in 1995 was replaced by SHA-160) in FIPS PUB 180-1 as a standard [19]. The NIST released SHA as FIPS PUB 180-2 [20] in 2001, which included the four algorithms SHA-160, SHA-256, SHA-384, and SHA-512. In 2004, NIST revised FIPS PUB 180-2 [21], adding SHA-224.that is the same length as the 3DES key [22].When implemented in parallel, RARSHA-256 [23] is quicker than SHA-256 since it uses the SHA-256 compression mechanism.
Block ciphers SHACAL and SHACAL-2 [24] are built on SHA-1 and SHA-256, respectively. The 42-round SHACAL-2 is based on a related-key rectangle attack that takes 2243.38 related-key selected plaintexts and runs for 2488.37 milliseconds [25]. In SHA-256, also known as SHA-256-XOR, Yoshida and Biryukov replaced all arithmetic adds with XOR operations. They discovered that SHA-256-XOR has a pseudo-collision resistant weakness up to 34 rounds [26].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 10, No. 2, October : 2023

V CRYPTING BIOMETRIC TEMPLETE

This method makes use of the iris database from the CASIA V3.0 (Chinese Academy Of Sciences Institute Of Automation). In order to assess the performance of the iris recognition system, 400 samples of CASIA-Iris-Interval eye photos were gathered, and the same samples were also tested for message digest algorithms like MD5 and SHA-512. All of the images are 8-bit gray-level JPEG files that were collected under near infrared light. Using phase quantization techniques and information taken from the original eye image, the iris recognition system creates the iris code (template). After that, the iris code, which was derived from the iris, is fed into a message digest algorithm like MD5 (Message Digest 5) or SHA (Secure Hash Algorithm), which creates a hash and stores it in the smartcard.

5.1 MD5 ALGORITHM

The iris code is sent into the MD5 method, which outputs a 128-bit hash by adding padding bits, length, and initializing the MD buffer before processing the message in blocks of 16 words. The output of MD5 is shown in figure 6

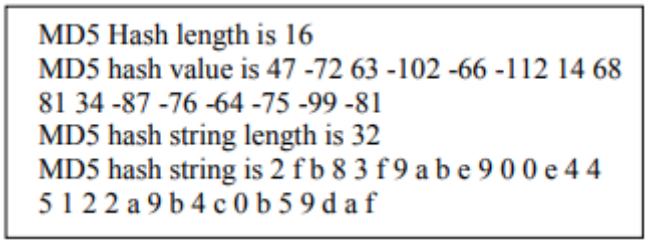

Fig.6 MD5 result

in comparison to MD5 Because of its collision and the possibility of finding collision for the compression function, MD2 is not appropriate for this experiment.

5.2 SHA 512- ALGORITHM

Padding, parsing, initializing the eight working variables and for-loop operation, computing the ith intermediate hash values, setting the initial hash values, constants, Boolean expressions and functions, and message schedule are all steps in the SHA-512 process. The picture 7 defines the SHA-512 algorithm.

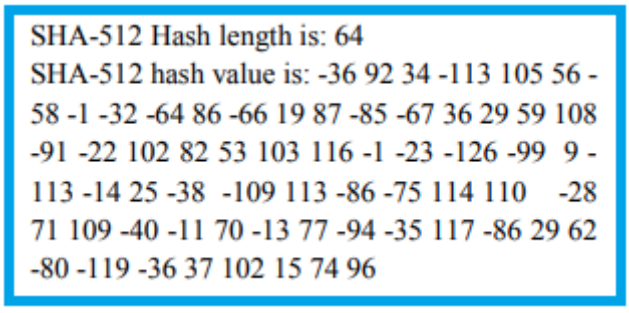

Fig.7ResultofSHA-512

SHA-512 offers higher security than the other algorithms when compared to the SHA family. Hence, the SHA-512.

The hash is stored in the card's EEPROM using the specially built card programmer after feature extraction and the SHA-512 message digest technique, and it is then saved on the smart card. Table 2 displays the memory usage as well as the reading and writing times for the smart card programmer.

Table 1Result Comparison of SHA

Algorithm	SHA-1	SHA-256	SHA-384	SHA-512
Hash Length	20	32	48	64
Hash String Length	40	64	96	128

VI BIOMETRIC SMARTCARD

The Fun card is a type of smart card with microprocessor contact. It is made up of the AT90S8515 microcontroller, a low-power CMOS 8-bit microcontroller, and the AT24C64 EEPROM, a serial electrically erasable and programmable read-only memory chip with 65,536 bits (8KB) of capacity [28].

Programmer for smart cards

The read/write capabilities of the smart card are enabled by the smart card programmer. Due to its faster speed compared to serial ports and capacity to generate several signals at once, the parallel port is used to connect the programmer to the computer.

Iris Recognition and Smartcard Integration

A smart card programmer is used to save the extracted iris image on a smart card. To verify that a person is who they claim to be, extracted iris features are matched to data from the camera or database.

6.1 Integrating Iris Recognition with Smartcard

A smart card programmer is used to save the extracted iris image on a smart card. To determine whether or not a person is verified, extracted iris features are matched against the data collected from the camera or database. The data has been signed using SHA-512, which creates a signature of 18 bytes, and then saved in the smartcard in order to protect it.

The signal selection circuit, which chooses the input signals, the voltage interfacing circuit, which supplies power, the connection pins to the parallel port, and the connection pins to the smart card are the four components that make up the smart card.

Table 2 Reading Time , Writing Time and Memory Utilization

Smart card writing time	8 Sec.
Smart card reading time	4 Sec.
Memory utilization	512 1720bits (86*20).

VII CONCLUSION

An iris-based smartcard security has been discussed in this research. An iris recognition system that provides the iris code was first introduced. Phase quantization was used to recognize irises based on information recovered from the original eye image. The claimed performance of the iris recognition system was tested using CASIA V3.0 [29] eye images. The message digest algorithm, such as MD5 or SHA-512, is then given the recognized iris template as input to produce the hash string. When compared to these cryptographic techniques, SHA-512 offers greater security than the others. Therefore, the SHA-512 is modified in this study to obtain the iris code hash. Then, using the special card programmer, the hash is put in the smartcard's EEPROM. With a minimum writing time of 6 seconds and a minimum reading time of 3 seconds, the smartcard reader ACR120S is used to read and write data to and from smartcards. Future work could involve integrating iris features into smart cards to create applications for identity, banking, financial services, mobile devices, secure network access, and healthcare.

References

[1] M. A. M. Abdullah, F. H. A. Al-Dulaimi, W. Al-Nuaimy and A. Al-Ataby, "Smart card with iris recognition for high security access environment," 2011 1st Middle East Conference on Biomedical Engineering, Sharjah, United Arab Emirates, 2011, pp. 382-385, doi: 10.1109/MECBME.2011.5752146.

[2] W. Rankl, W. Effing, "Smart card HandBook", Wiley &Sons, New York, 1999.

[3] The Industry Journalfor Security & Business Professionals, "Hi-Tech Security Solutions", Available online: http://www.securitysa.com.

[4] Y. W. Yun, Ch. T. Pang, "An Introduction to Biometric Match-On-Card", Available online: http://www.itsc.org.sg.

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

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

[7] S. Alluri, M. Dasharatha, B. R. Naik and N. S. S. Reddy, "Design of low power high speed full adder cell with XOR/XNOR logic gates," 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2016, pp. 0565-0570, doi: 10.1109/ICCSP.2016.7754203.

[8] M. V. S. Nandam and S. Alluri, "High Performance 32 bit Dadda Multiplier Using EDA," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-5, doi: 10.1109/ICSSS49621.2020.9201958.

[9] S. Alluri, B. R. Naik and N. S. S. Reddy, "Mapping of five input wallace tree using cadence tool for low power, low area and high speed," 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2016, pp. 0304-0310, doi: 10.1109/ICCSP.2016.7754144.

[10] Alluri, S., Mounika, K., Balaji, B., Mamatha, D."Optimization of multiplexer architecture in VLSI circuits",AIP Conference Proceedingsthis link is disabled, 2021, 2358, 040004

[11] Alluri, S., Mounika, K., Balaji, B., Mamatha, D."A novel implementation of 4 bit parity generator in 7nm technology",AIP Conference Proceedingsthis link is disabled, 2021, 2358, 030002

[12] Gajula, K., Alluri, S."High performance for hybrid GSA-PSO algorithm",AIP Conference Proceedingsthis link is disabled, 2021, 2358, 080006..

[13] Mounika, K., Mamatha, D., Alluri, S.,"Generation of bitstream by moore machine from state machine",AIP Conference Proceedingsthis link is disabled, 2021, 2358, 100001.

[14] Alluri, S., Balaji, B., Cury, C."Low power, high speed VLSI circuits in 16nm technology",AIP Conference Proceedingsthis link is disabled, 2021, 2358, 030001.

[15] Mamatha, D., Mounika, K., Alluri, S.,"A novel design of 32x1 multiplexer in deep submicron technology",AIP Conference Proceedingsthis link is disabled, 2021, 2358, 060003.

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

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

[18] J. Daugman. How iris recognition works. Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002.

[19] J. Daugman. Biometric personal identification system based on iris analysis. United States Patent, Patent Number: 5,291,560, 1994.

[20] Chainese academy of Sciences – Institute of Automation. Database of 756 Greyscale Eye Images Version 3.0, available online: http://biometrics.idealtest.org/introduction.jsp

[21] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, S. McBride. A system for automated iris recognition. Proceedings IEEE Workshop on Applications of Computer Vision, Sarasota, FL, pp. 121-128, 1994.

[22] W. Kong, D. Zhang. Accurate iris segmentation based on novel reflection and eyelash detection model. Proceedings of 2001 International Symposium on Intelligent Multimedia, Video and Speech Processing, Hong Kong, 2001.
[23] C. Tisse, L. Martin, L. Torres, M. Robert. Person identification technique using human iris recognition. International Conference on Vision Interface, Canada, 2002.
[24] L. Ma, Y. Wang, T. Tan. Iris recognition using circular symmetric filters. National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, 2002.
[25] D. Field. Relations between the statistics of natural images and the response properties of cortical cells. Journal of the Optical Society of America, 1987.
[26] R. Rivest. The MD5 Message-Digest Algorithm [rfc1321], 1992.
[27] M.J.B.Robshaw, RSA Laboratories, "On Recent Results for MD2, MD4 and MD5", 1990.
[28] National Institute of Standards and Technology, "Secure hash standard", Federal Information Processing Standards Publications FIPS PUB 180, May. 1993.
[29] National Institute of Standards and Technology, "Secure hash standard", Federal Information Processing Standards Publications FIPS PUB 180-1, 19
[30] National Institute of Standards and Technology, "Secure hash standard", Federal Information Processing Standards Publications FIPS PUB 180-2, 2002.