Notice of Violation of IEEE Publication Principles

“SBBSCS: SHA Based Biometric Smartcard Security”
by V. Kovendan, Gerly Eldose
in the Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES), February 2014

After careful and considered review of the content and authorship of this paper by a duly constituted expert committee, this paper has been found to be in violation of IEEE’s Publication Principles.

This paper copies text and figures from the paper cited below. The original content was copied without attribution (including appropriate references to the original author(s) and/or paper title) and without permission.

“Smart Card with Iris Recognition for High Security Access Environment”
by Mohammed A.M. Abdullah, F.H.A. Al-Dulaimi, Waleed Al-Nuaimy and Ali Al-Ataby
in the Proceedings of the 1st Middle East Conference on Biomedical Engineering (MECBME), February 2011, pp. 382-385

SBBSCS: SHA BASED BIOMETRIC SMARTCARD SECURITY

Mr.V. Kovendan* Assistant Professor
Department of Computer Science & Engineering
Sri Venkateswaara College of Technology
Email: kovendan.cse@gmail.com

Ms.Gerly Eldose
Department of Computer Science & Engineering
Sri Venkateswaara College of Technology,
Email: e.gerly@gmail.com

Abstract-Smartcards are being used as a form of identification and authentication. One major problem with smartcards, however, is the possibility of loss or theft. Current options for securing smartcards 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. The extracted iris features stored the form of hash in smartcard are compared against the hash of data acquired from a camera or database for authentication. Results show that the SHA secure hash algorithm has superior performance in terms of security, accuracy and consistency compared with other technology (MD5).

Keyword: Biometrics; Smartcard; MD5; SHA.

I. INTRODUCTION

Smartcard

Conventional smartcard invented in 1974 [1] has gone several development phases during the years. Today it is credit-card-sized card equipped with microprocessor, memory and input/output handler. Adding individuals' unique characteristics into smart card chip, smart card becomes more secure medium, suitable for use in a wide range of applications that support biometric methods of identification. One such example is UK's Asylum Seekers Card contain photo for visual recognition and fingerprint template stored on smartcard chip for biometric identification [2]. In biometric identification process we can distinguish between three types of smartcard regarding their typical technical features and the type of authentication they support. The three types of smart card [3] are Template-on-card (TOC), Match-on-card (MOC), and System-on-card (SOC). In this work, TOC type of smartcard is used to store hash of SHA-512 shown in fig 1.

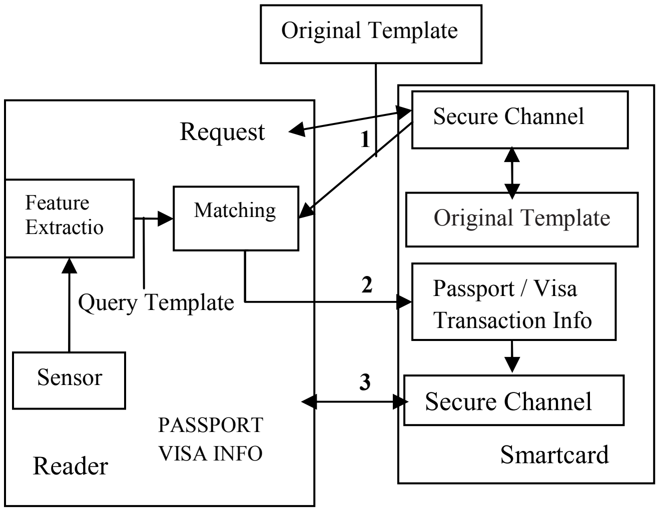


Fig.1 Authentication Process in a TOC System

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" [4].

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 [5]. 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 [6]. A simple Trojan on the host could easily sniff the PIN and store it for the future usage. Biometric technologies have been proposed to strengthen authentication mechanisms in general by matching the stored biometric template to a live the biometric template [7]. 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 [7]. They are Template on Card (TOC), Match on Card (MOC), and System on Card (SOC). In this phase we concentrated on Template on Card (TOC).

Biometric Technology: A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual.

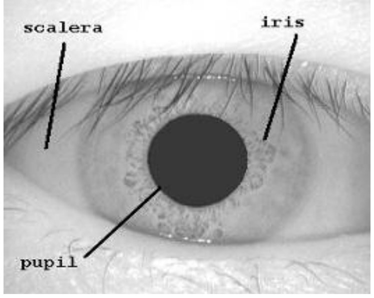


Fig.2 Front-on view of the human eye

The iris is the colored portion of the eye that surrounds the pupil is a thin circular diaphragm, which lies between the cornea and the lens of the human eye shown in fig 2. Average diameter of the iris is 12 mm, and the pupil size can vary from 10% to 80% of the iris diameter [8]. The biometric sample is then transformed using some sort of mathematical function into a biometric template. It will provide a normalized, efficient and representation of the feature, which can then be objectively compared with other templates in order to determine identity.

II. IRIS RECOGNITION SYSTEM

The iris is the colored portion of the eye that surrounds the pupil as shown in figure 1. An iris recognition system is composed of many stages as 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 the analysis. Then the code is generated. After that, the person is identified by comparing his/her code with an iris database. These processes are named as Image acquisition, Segmentation, Normalization, Feature extraction, Code generation as shown in fig 3.

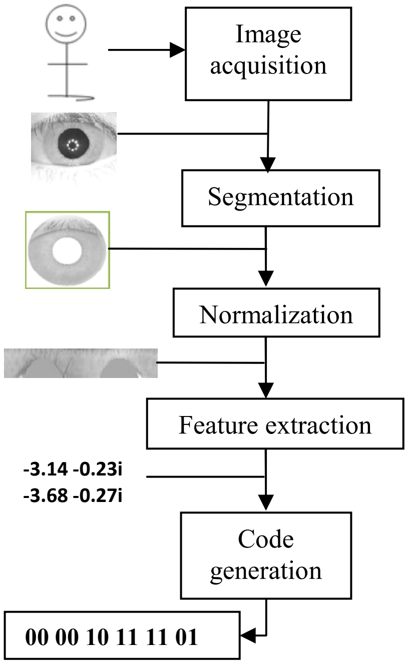


Fig.3 Iris Recognition System

Segmentation

The first stage of iris recognition is to isolate the actual iris region in a digital eye image. The success of segmentation depends on the imaging quality of eye images. Images in the CASIA iris database [10] do not contain specular reflections due to the use of near infra-red light for illumination. The segmentation is achieved by Canny Edge Detection is a multi-step edge detection procedure by Canny as follows

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

Where

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

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

To get $M(n,n) = \sqrt{(g_m^2(m,n) + g_n^2(m,n))}$ and $\theta(m,n)=\tan^{-1}[g_n(m,n)/g_m(m,n)]$

Threshold M:

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

if $M(m,n)>T$

where T is so chosen that all edge elements are kept while most of the noise is suppressed.

Hough Transform: The Hough transform is a standard computer vision algorithm that can be used to determine the parameters of simple geometric objects, such as lines and circles, present in an image. The circular Hough transform can be employed to deduce the radius and centre coordinates of the pupil and iris regions. An automatic segmentation algorithm based on the circular Hough transform is employed by Wildes et al. [11], Kong and Zhang [12], Tisse et al. [13], and Ma et al. [14].

Normalization

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].

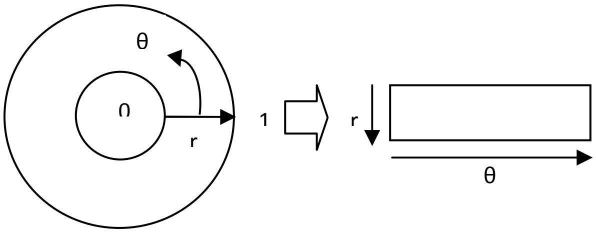


Fig. 4 Generating Normalized Iris Image

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

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

with: $x(r,\theta) = (1-r)\,x_p(\theta) + r\,x_i(\theta)$

$y(r,\theta) = (1-r)\,y_p(\theta) + r\,y_i(\theta)$

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 *xp, yp* and *xi, yi* 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).

Ignoring Upper and Lower Part of Iris 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, 360^0] is not transformed in the proposed system. Experiments are to be conducted by normalizing the iris from [-32, 32^0] and [148, 212^0], ignoring both upper and lower eyelid areas as indicated in fig 5.

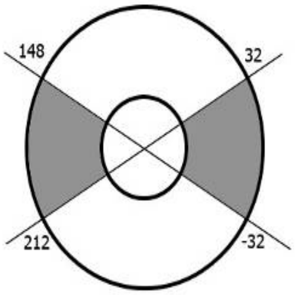


Fig.5 Ignoring Upper and Lower Part of Iris

The size of the rectangular block is reduced accordingly. Left and right images each one of size 112×60 is 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.

Feature Extraction

Gabor filters are able to provide optimum conjoint representation of a signal in space and spatial frequency. A Gabor filter is constructed by modulating a sine/cosine wave with a Gaussian. This is able to provide the optimum conjoint localization in both space and frequency, since a sine wave is perfectly localized in frequency, but not localized in space.Decomposition of a signal is accomplished using a quadrature pair of Gabor filters. A disadvantage of the Gabor filter is that the even symmetric filter will have a DC component whenever the bandwidth is larger than one octave [15]. The frequency response of a Log-Gabor filter is given as $G(f) = \exp\left(\frac{-\log(f/f_0)^2}{2(\log(\sigma/f_0)^2}\right)$ where f_0 represents the centre frequency, and σ gives the bandwidth of the filter. Details of the Log-Gabor filter are examined by Field [15].

Iris Coding

Once the iris feature is extracted the output will be given to the code generation, here we use the technique as phase quantization for generating the iris code. In the Phase Quantization, if both real and imaginary parts are +ve, 11 is assigned. If both real part and imaginary parts are –ve then the 00 will be assigned. As well as if the real part is +ve and imaginary part is –ve, 10 is assigned and if the real part is -ve and imaginary part is +ve, 01 is assigned. Based on this logic shown in fig 6 iris code is generated as 1's and 0's stream.

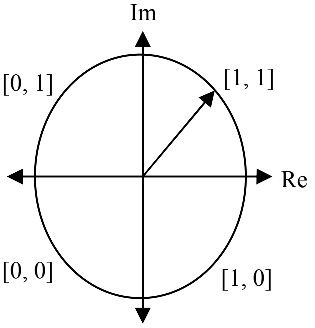


Fig. 6 Phase Quantization

III. MESSAGE DIGEST

MD5, with the full name of the Message-digest Algorithm 5, is the fifth generation on behalf of the message digest algorithm. In August 1992, Ronald L. Rivest [16] submitted a document to the IETF (The Internet Engineering Task Force) entitled "The MD5 Message-Digest Algorithm", which describes the theory of this algorithm. MD5 was developed from MD, MD2, MD3 and MD4 [17]. It can compress any length of data into an information digest of 128bits while this segment message digest often claims to be a digital fingerprint of the data. This algorithm makes use of a series of non-linear algorithm to do the circular operation, so that crackers cannot restore the original data. In cryptography, it is said that such algorithm as an irreversible algorithm, can effectively prevent data leakage caused by inverse operation. Both the theory and practice have good security, because the use of MD5 algorithm does not require the payment of any royalties, time, and cost less which make it be widely used .

IV. SECURE HASH ALGORITHM

Cryptographic hash functions play an important role in modern cryptography. They are widely used in a variety of applications such as password protection, secure protocols, digital signatures, and more.

The Secure Hash Algorithm (SHA) is a series of cryptographic hash functions published by the National Institute of Standards and Technology (NIST). NIST proposed the SHA-0 as Federal Information Processing Standard Publication (FIPS PUB) 180 in 1993 [18] and announced a revised version, the SHA-1 (also called SHA-160) in FIPS PUB 180-1 as a standard instead of the SHA-0 in 1995 [19]. In 2001, the NIST published SHA as FIPS PUB 180-2 [20] consisting of four algorithms: SHA-160, SHA-256, SHA-384 and SHA-512. NIST updated FIPS PUB 180-2 [21] in 2004, specifying SHA-224 that matches the key length of 3DES [22].RARSHA-256 [23] is composed of the SHA-256 compression function, and is faster than SHA-256 in parallel implementation.

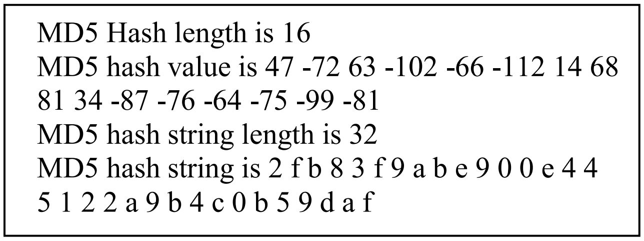
SHACAL and SHACAL-2 [24] are block ciphers based on SHA-1 and SHA-256, respectively. The 42-round SHACAL-2 is based on a related-key rectangle attack, which requires $2^{243.38}$ related-key chosen plaintexts with a running time of $2^{488.37}$ [25]. Yoshida and Biryukov replaced all arithmetic additions with XOR operations in SHA-256, calling it SHA-256-XOR, and found that SHA-256-XOR has a pseudo-collision resistance weakness up to 34 rounds [26].

V. CRYPTING BIOMETRIC TEMPLATE

This technology uses the CASIA V3.0 (Chinese Academy Of Sciences Institute Of Automation) iris database. All images are 8bit gray-level JPEG files, collected under near infrared illumination, and 400 samples of CASIA-Iris-Interval eye images are taken to test the result of iris recognition system and also tested with the same samples for message digest algorithms such as MD5 and SHA-512. The iris recognition system generates the iris code (template) by using the techniques called phase quantization based on extracted features from the original eye image. Then the extracted iris feature that is the iris code is given as input to the Message Digest algorithm such as MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) which produces the hash and stored in the smartcard.

MD5 Algorithm

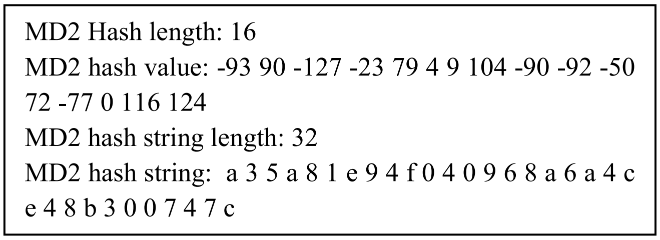
The iris code is given as input to the MD5 algorithm and it produces 128 bit of hash by the process of Append Padding Bits, Append Length, and Initialize MD Buffer, then Process Message in 16-Word Blocks, the output of MD5 is given in the figure 7.



```
MD5 Hash length is 16
MD5 hash value is 47 -72 63 -102 -66 -112 14 68
81 34 -87 -76 -64 -75 -99 -81
MD5 hash string length is 32
MD5 hash string is 2 f b 8 3 f 9 a b e 9 0 0 e 4 4
5 1 2 2 a 9 b 4 c 0 b 5 9 d a f
```

Fig.7 Result of MD5

Compared with MD5 MD2 is not suitable for this experiment, because of its collision and MD2 is possible to find collision for the compression function [27]. The result of MD2 is given in the figure 8.

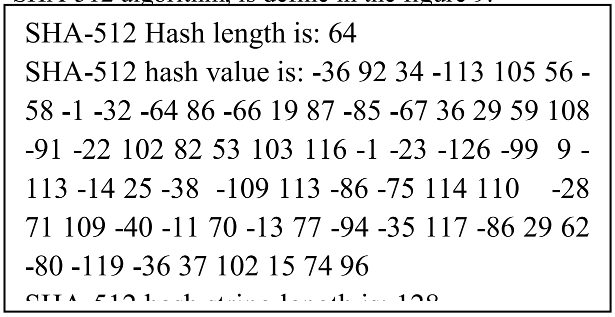


```
MD2 Hash length: 16
MD2 hash value: -93 90 -127 -23 79 4 9 104 -90 -92 -50
72 -77 0 116 124
MD2 hash string length: 32
MD2 hash string:  a 3 5 a 8 1 e 9 4 f 0 4 0 9 6 8 a 6 a 4 c
e 4 8 b 3 0 0 7 4 7 c
```

Fig.8 Result of MD2

SHA-512 ALGORITHM

The process of SHA-512 includes padding, parsing, setting the initial hash values, constants, Boolean expressions and functions, and message schedule, initializing the eight working variables and for-loop operation and computing the i^{th} intermediate hash values. SHA-512 algorithm, is define in the figure 9.



```
SHA-512 Hash length is: 64
SHA-512 hash value is: -36 92 34 -113 105 56 -
58 -1 -32 -64 86 -66 19 87 -85 -67 36 29 59 108
-91 -22 102 82 53 103 116 -1 -23 -126 -99  9 -
113 -14 25 -38  -109 113 -86 -75 114 110    -28
71 109 -40 -11 70 -13 77 -94 -35 117 -86 29 62
-80 -119 -36 37 102 15 74 96
SHA-512 hash string length is: 128
```

Fig.9 Result of SHA-512

Comparing with SHA family SHA-512 provides more security than the other algorithms. So the SHA-512 is adapted in this work to produce the hash of the iris code. The results of SHA family are shown in Table 1.

Table 1 Result 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

After feature extraction and message digest algorithm of SHA-512, the hash is saved in the card's EEPROM using the designed card programmer and saved on the smart card. Table 2 shows the time of reading, writing of the smart card programmer and the memory utilization.

VI. BIOMETRIC SMART CARD

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 [28].

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.

Integrating Iris Recognition with Smartcard

Extracted iris image, is saved in smart card's using smart card programmer. Extracted iris features 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, a signature of the data has been generated using the SHA-512, which produces 18 bytes signature, and then saved in the smartcard.

The smart card consists of four parts which are: signal selection circuit to select the input signals, voltage interfacing circuit which provides power supply, connection pins to the parallel port, and connection pins to 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

This paper has presented an iris based smartcard security. At first, an iris recognition system was presented which provides the iris code. Iris recognition was achieved through the use of phase quantization based on extracted features from the original eye image, which was tested using CASIA V3.0 [29] eye images in order to verify the claimed performance of iris recognition system. Next the recognized iris template is given as input to the message digest algorithm such as MD5 and SHA-512 which generates the hash string. Comparing with these cryptographic technologies SHA-512 provides more security than the other algorithms. So the SHA-512 is adapted in this work to produce the hash of the iris code. Then the hash is stored in the smartcard's EEPROM using the designed card programmer. The smartcard reader ACR120S is used to read/write the data from/to the smartcard and it has the minimal writing time (6 Sec) and reading time (3 Sec). As future work, after transforming the iris features into the smart card, it can be used to develop the applications like identification, financial services, cellular phones, secure network access, healthcare and banking.

REFERENCES

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

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

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

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

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

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

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

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

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

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

[11] 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.

[12] 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.

[13] C. Tisse, L. Martin, L. Torres, M. Robert. Person identification technique using human iris recognition. International Conference on Vision Interface, Canada, 2002.

[14] 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.

[15] D. Field. Relations between the statistics of natural images and the response properties of cortical cells. Journal of the Optical Society of America, 1987.

[16] R. Rivest. The MD5 Message-Digest Algorithm [rfc1321], 1992.

[17] M.J.B.Robshaw, *RSA Laboratories,* "On Recent Results for MD2, MD4 and MD5", 1990.

[18] National Institute of Standards and Technology, "Secure hash standard", Federal Information Processing Standards Publications *FIPS PUB* 180, May. 1993.

[19] National Institute of Standards and Technology, "Secure hash standard", Federal Information Processing Standards Publications *FIPS PUB* 180-1, 19

[21] National Institute of Standards and Technology, "Secure hash standard", Federal Information Processing Standards Publications *FIPS PUB* 180-2, 2002.

[22] National Institute of Standards and Technology, " Data encryption standard (DES) ", Federal Information Processing Standards Publications *FIPS PUB* 46-3, 1999

[23] PinakpaniPal and Palash Sarkar, "PARSHA-256 – A New Parallelizable Hash Function and a Multithreaded Implementation", *Proc. of Fast Software Encryption* 2003 (*FSE*2003), *LNCS* 2887, pp.347–361, Springer-Verlag, 2003.

[24] H. Handschuh and D. Naccache, "SHACAL", NESSIE, 2001. Archive available online: http://www.cosic.esat.kuleuven.be/nessie/tweaks.html

[25] Jiqiang Lu1, Jongsung Kim, Nathan Keller, and Orr Dunkelman, "Related-Key Rectangle Attack on 42-Round SHACAL-2", *Proc. of 9th Information Security Conference* (*ISC*2006), *LNCS* 4176, pp. 85–100, Springer-Verlag, 2006.

[26] Hirotaka Yoshida and Alex Biryukov, "Analysis of a SHA-256 Variant", *Proc. of 12th Annual Workshop on Selected Areas in Cryptography* (*SAC*2005), *LNCS* 3897, pp. 245–26, Springer-Verlag, 2006.

[27] N.Rogier and P. Chauvaud. The compression function of MD2 is not collision free. Presented at *Cryptography 95*, Carleton University, Ottawa, Canada. May 18-19, 1995.

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

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