Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

8th International Conference
on Electrical Engineering
ICEENG 2012

Extraction of Human Iris Patterns for Biometric keys Generation

By

Khaled Hassanain* Eman Hesham **

Abstract:

With the increasing reliance on electronic information, which needs to be exchanged across the internet or stored on open networks, cryptography is becoming an increasingly important feature of computer security. A biometric key dependent cryptosystem is proposed, to ensure the security of the whole system by using iris pattern as a key in a cryptosystem, like, Key-dependent Advanced Encryption Standard (KAES). KAES is used to ensure that no trapdoor is present in cipher and to expand the key-space to slow down attacks. The proposed system gave significant results under various tests for the key uniqueness and the system randomness.

Keywords:

AES, KAES, MD5, RNG, PRNG, SHA-1AES, KAES, MD5, RNG, PRNG, SHA-1

* Technical Research Department, Egypt (khass@idsc.net.eg)

** Faculty of computers and Information, Helwan University, Egypt (hesham.eman@gmail.com)

1. Introduction:

Cryptography is becoming an increasingly important feature for information security, and there are many available cryptographic algorithms for securing information: Symmetric and Asymmetric [1] [2] [6]. Also there are many services and applications which are offered by modern cryptography as user authentication, data authentication, data confidentiality and digital signature [13].

The strength of cryptosystem depends on many factors: key length, algorithm complexity and resistance to cryptanalysis techniques [1] [2] [6]. There are mainly two problems when using traditional password or token as a key for any cryptosystem. First, the security of the key, and hence the cryptosystem, is now only as good as the password. Due to practical problems of remembering various passwords, some users tend to choose simple words, phrases, or easily remembered personal data, while others resort to write the password down on an accessible document to avoid data loss. The second problem is the lack of a direct connection between the password and the user, as a password is not tied to a user, a system running the cryptographic algorithm is unable to differentiate between the legitimate user and an attacker who fraudulently acquires the password of a legitimate user (Authentication) [1].

An alternative to password protection, there are many approaches to bind a crypto-key with biometrics. The famous two approaches are a biometric-based key release and biometric-based key generation [2] [3]. In biometric-based key release the key is hidden into a biometric template at the enrolment phase and is available to be released at authentication phase. While the other, the key is generated directly from the biometric data using one of secure hash functions [4].

This paper introduces a biometric cryptosystem in which the key is generated from biometric data and the produced key is used in a key dependent encryption algorithm to ensure the security of the system and slow down its attacks [6][7][8][9].

The paper is organized as follows: Section 2 presents the proposed biometric key dependent cryptosystem. Section 3 explains the evaluation criteria. Section 4 discusses the experimental results. Section 5 summaries and concludes the paper.

2. A biometric key dependent KAES algorithm:

The proposed scheme replaces the secret key in a cryptosystem with a key which generated directly from one of the human biometric data (e.g. fingerprint). In general, the proposed biometric-key cryptosystem could be subdivided into three phases: biometric phase, key generation phase and encryption phase. Fig. 1 shows the overall structure of the proposed system [10].

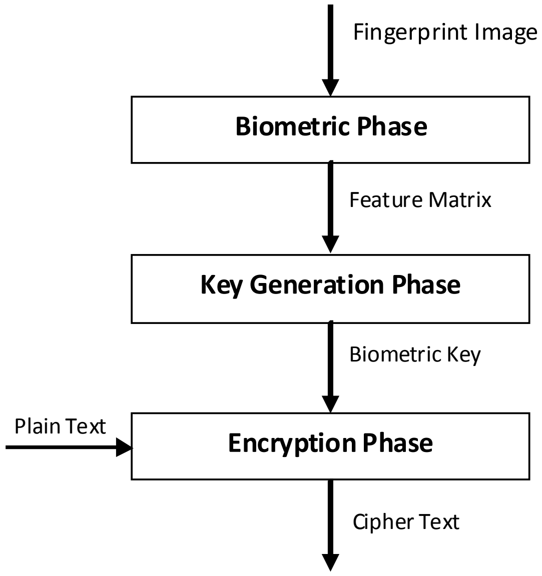


Figure (1): *The proposed biometric key dependent cryptosystem*

In the proposed system, the input to the biometric phase is human eye image which acquired from the system user's finger using fingerprint readeCASIA-Iris4 Database [11]. Through this phase some unique characteristics of the human eye image are extracted to form an iris pattern.

The produced pattern is used as an input to the next phase to generate a 128-bit key using one of cryptographic hash functions such as Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).

The plain-text is then encrypted using the generated key by one of cryptographic encryption algorithm such as Advanced Encryption Standard (AES) or Key-dependent Advanced Encryption Standard (KAES) [6] [7].

Each phase of the proposed system is described in more details in the following subsections.

A. Biometric Phase

Iris pattern recognition system is considered as the most reliable and accurate biometric identification system available [3]. Libor open-source' iris recognition system is used in order to verify both the uniqueness of the human iris and its performance as a biometric [11].

As shown in Fig. 2 the human iris can be defined as a thin circular diaphragm, which lies between the cornea and the lens of the human eye and it perforated close to its centre by a circular aperture known as the pupil. The average diameter of the iris is 12 mm, and the pupil size can vary from 10% to 80% of the iris diameter. The two eyes of an individual contain completely independent iris patterns, and identical twins possess uncorrelated iris patterns [11].

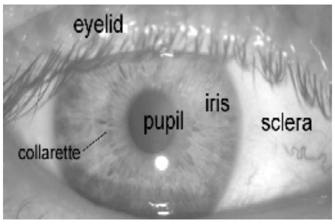


Figure (2): *Human Eye*

Fig. 3 shows that the biometric phase is composed of three steps to form a biometric iris pattern using the input human eye image [11]:

1- Segmentation.
2- Normalization.
3- Code generation.

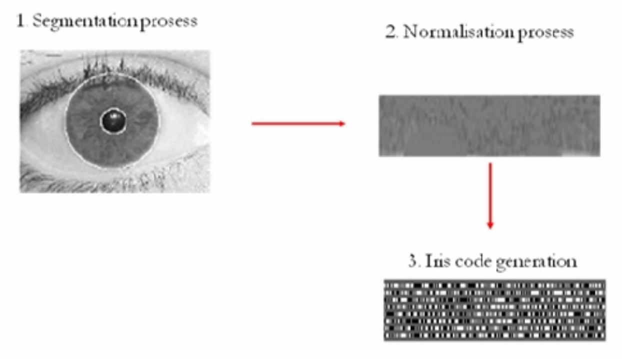


Figure (3): *Iris Recognition System*

The segmentation step runs using circular Hough transform for detecting the iris and pupil boundaries. This involves first employing Canny edge detection to generate an edge map. Gradients were biased in the vertical direction for the outer iris/sclera boundary [16]. The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. Also, some reflections can occur within the iris region corrupting the iris pattern. The segmentation technique isolates and excludes these artifacts as well as locating the circular iris region as shown in Fig. 4 [11].

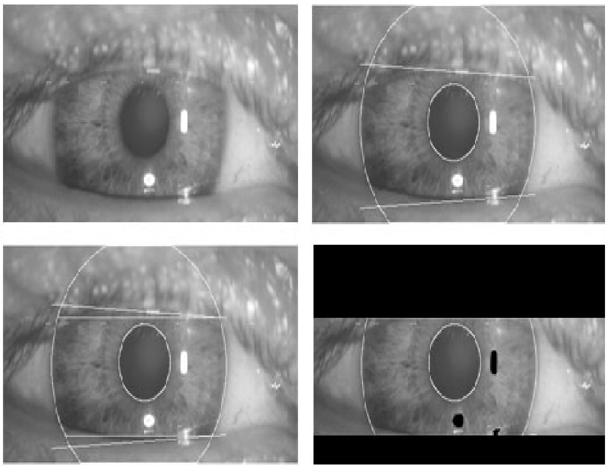
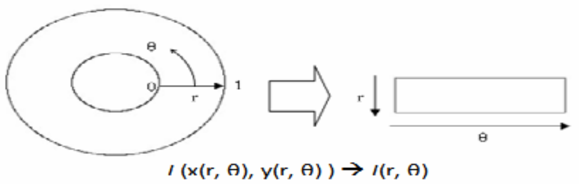


Figure (4): *The Segmentation Process*

The dimensional inconsistencies between eye images are mainly due to the stretching of the iris caused by pupil dilation from varying levels of illumination, varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket. The normalization process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location. [11].
For normalization of iris regions a technique based on Daugman's rubber sheet model was employed as in Fig. 5 [15]:

1- Remaps each point within the iris region to a pair of polar coordinates (r,θ) where r is on the interval [0"pupil",1 "iris"] and θ is angle [0,2π].
2- The centre of the pupil was considered as the reference point.
3- A number of data points are selected along each radial line and this is defined as the radial resolution. The number of radial lines going around the iris region is defined as the angular resolution.



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

$$x(r,O) - (1-r)x_p(O) + rx_i(O)$$

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

x_p and y_p are the coordinates of the pupil.

x_i and y_i are iris boundaries along the O direction.

Figure (5): *The Normalization Process*

The pattern that is generated in the feature encoding process will need a corresponding matching metric, which gives a measure of similarity between two iris templates. This metric should give one range of values when comparing templates generated from the same eye, known as intra-class comparisons, and another range of values when comparing templates created from different irises, known as inter-class comparisons [11].

At the code generation steps as in Fig. 6, the 2D normalized pattern is broken up into a number of 1D signals, and then these 1D signals are convolved with 1D Log-Gabor wavelets [11].

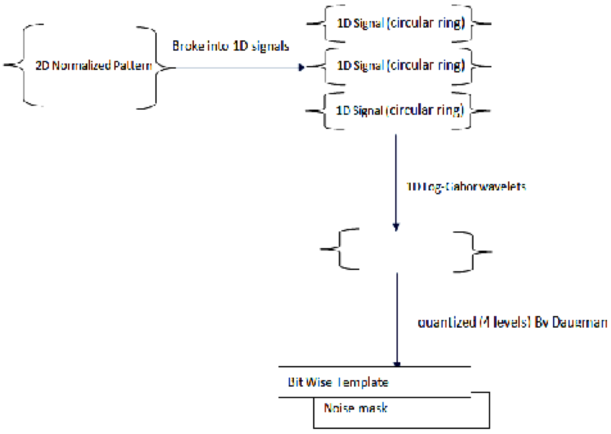

2D Normalized Pattern
Broke into 1D signals
1D Signal (circular ring)
1D Signal (circular ring)
1D Signal (circular ring)
1D Log-Gabor wavelets
quantized (4 levels) By Daugman
Bit Wise Template
Noise mask

Figure (6): *The code generation process*

The angular direction is taken rather than the radial one, which corresponds to columns of the normalized pattern, since maximum independence occurs in the angular direction. The output of filtering is then phase quantized to four levels using the Daugman method, with each filter producing two bits of data (Gray Code) for each phase. The output of phase quantization is chosen to be a grey code, so that when going from one quadrant to another, only 1 bit changes as shown in Fig. 7 [11].

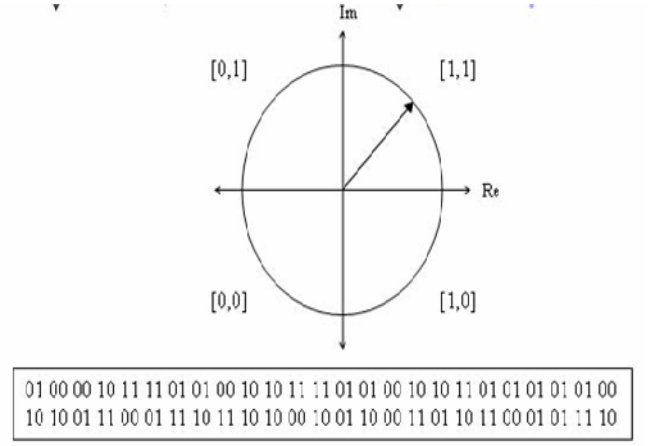


Figure (7): *Iris template*

The encoding process produces a bitwise template containing a number of bits of information, and a corresponding noise mask which corresponds to corrupt areas within the iris pattern, and marks bits in the template as corrupt. The total number of bits in the template will be:
(The angular resolution) multiple by (the radial resolution) multiple by (2) multiple by (the number of filters used) [11].

B. Key Generation Phase

There are many cryptographic hash functions that can be used to generate Bio-crypto key. Table 1 lists the common hash functions [14].
In the proposed system, MD5 is used to generate 128-bit encryption key from the generated biometric feature matrix .MD5 algorithm consist of 5 steps namely, Append Padding Bits, Append Length, Initialize MD Buffer, Process Message in 16-Word Blocks and Finalize the Output [5][14]. The output generated key from MD5 is suitable for many encryption algorithms like AES and KAES.

Table (1): *Hash Functions*

Function Name	Output Length
HAVAL	128 to 256 bits
MD2	128 bits
MD4	128 bits

MD5	128 bits
RIPEMD-160	160 bits
SHA	160 up to 512 bits
Snefru	128 or 256 bits
Tiger	192 bits
Whirlpool	512 bits

C. Encryption Phase

KAES [6][7][8][9] is a symmetric encryption algorithm that modifies AES to be key dependent algorithm. KAES is block cipher in which the block length and the key length are specified according to AES specification: 128, 192, or 256 bits and block length of 128 bits. In the proposed system, a key length of 128 bits is used. KAES involves the key in most of algorithm steps which increase the security of it rather than in AES. Through the encryption phase, KAES has been applied to encrypt the plain-text using the generated key.

3. Evaluation Criteria:

For evaluating the biometric key [10], various tests have been conducted for the following Criteria:

A. Key Stability

A major problem with biometric data is that individual's enrollment template can vary from session to session. This variation can occur for a number of reasons including different environments (e.g. the stretching of the iris caused by pupil dilation from varying levels of illumination, varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket).

At the encryption side, the user extracted iris pattern will use to generate session key. This pattern will also be saved to use in comparison with the new extracted pattern at the decryption side by referring to one of comparison technique (e.g. Hamming distance).

B. Key Uniqueness and discrimination

The discrimination is occurred when different keys are produced for different users. The uniqueness of a biometric key is determined by the uniqueness of the iris pattern used in the key. Hamming distance technique is used to decide that different users have different iris patterns which generate different keys.

C. Iris patterns Comparison Module

The Hamming distance was chosen as a metric for recognition. The Hamming distance algorithm employed also incorporates noise masking, so that only significant bits are used in calculating the Hamming distance between two iris templates. In theory, two iris templates generated from the same iris will have a Hamming distance of 0.0. In practice, this will not occur, as Normalization is not perfect, and there will be some noise that goes undetected.

By experiment on the ‘CASIA-a’ data set it found that a separation point of 0.4 a false accept rate and false reject rate of 0.005% and 0.238% respectively is achieved, which still allows for accurate recognition. So that if any two templates generate a Hamming distance value greater than 0.4, they are deemed to be generated from different irises.

D. The Pearson’s correlation coefficient

The correlation coefficient measures the strength of a linear relationship between two variables. The correlation coefficient is always between -1 and +1. The closer the correlation is to +/-1, the closer to a perfect linear relationship. The correlation is interpreted as follow:

- -1.0 to -0.7 strong negative association.
- -0.7 to -0.3 weak negative association.
- -0.3 to +0.3 little or no association.
- +0.3 to +0.7 weak positive association.
- +0.7 to +1.0 strong positive association.

Applying the Pearson’s correlation coefficient for many users keys, measures how much one of them depends on the others.

4. Experimental Results:

To simulate the proposed biometric key dependent cryptosystem, a MATLAB script was implemented for biometric phase and for AES and KAES also a java program was implemented for key generation phases. The key’s length (128 bit) was fixed for both AES and KAES algorithms.

Twenty human eye images were used from 'CASIA-a' data for five users each have four different images at different environment conditions. The proposed system used the images to produce twenty keys which are four keys for each user.

The key stability is measured by applying the hamming distance technique between the three user iris patterns according to his first pattern.

Fig. 8 shows that the most values of hamming distance between the first pattern for the user to the rest of his patterns are less than 0.4. It means that the extracted patterns for the same user are almost the same.

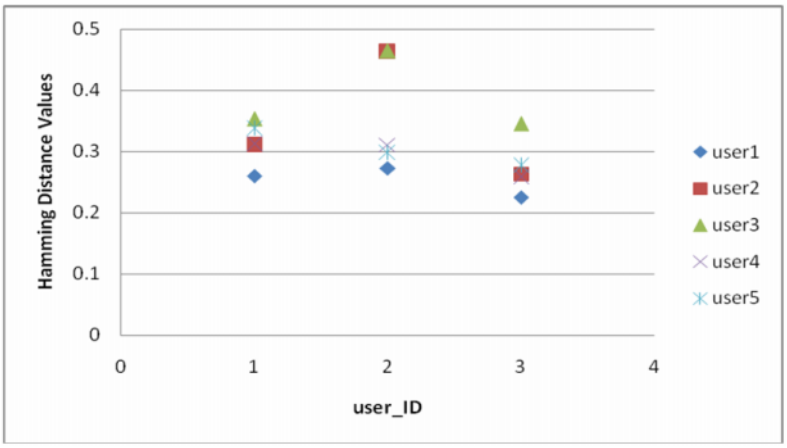


Figure (8): *The Hamming Distance (Intra-class)*

To measure the iris pattern uniqueness which means key uniqueness, the hamming distance technique between five users' patterns is applied. The results of the test are shown in Fig. 9. It could be noticed that the all values of hamming distance between different users' patterns are greater 0.4. So, every user eye image is produced different pattern.

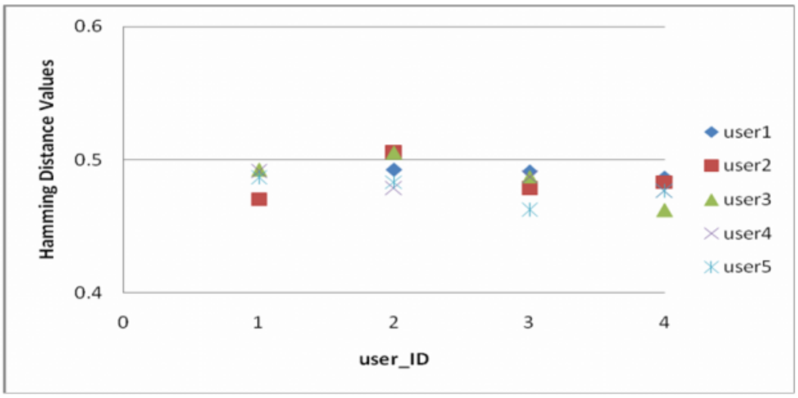


Figure (9): *The Hamming Distance (Intre-class)*

Applying the Pearson's correlation coefficient between the generated five users keys, measures how much one of them depends on the others as shown in Fig. 10. It is shown that the most of the values are in the negative area. So, it is examined that there isn't relations between produced keys form different users.

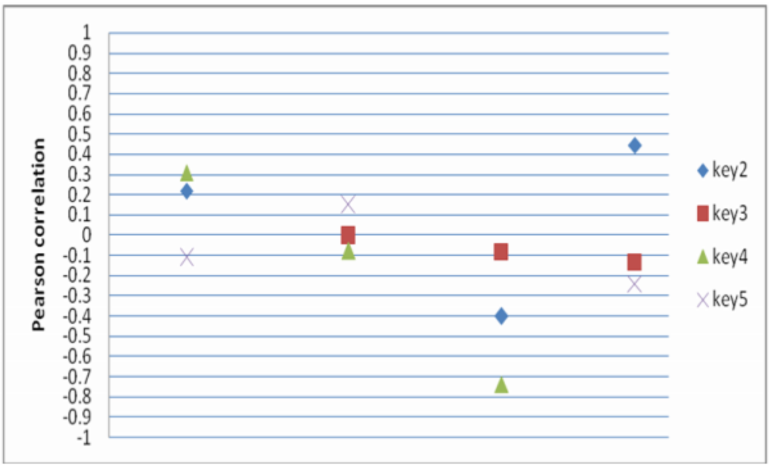


Figure (10): *The Pearson's correlation coefficient*

5. Conclusion And Future Work:

This paper presents a biometric key dependent cryptosystem by replacing the encryption key with iris pattern. KAES is improving the security of the proposed system by employing the key to be the main parameter of the encryption algorithm.

Regarding the implications of the results mentioned earlier, the randomness of the system and key stability are achieved in the most test cases of the proposed system.
As for future work, the biometric phase can be enhanced to meet the requirements of distortion tolerance, discrimination of the key. Developing one of the key agreement protocols to exchange the key between the sender and the receiver can be added in the future to the system. Also the system can be integrated with analysis modules in each phase to increase the reliability and the security of the system.

References:

[1] International Computer Security Association., & Nichols, R. K. (1999). ICSA guide to cryptography (chapter 22). New York: McGraw Hill.

[2] Stoianov, A., Information and Privacy Commissioner /Ontario., & Cavoukian, A. (2007). Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy. Toronto, Ont: Information and Privacy Commissioner, Ontario.

[3] Kresimir & Mislav(2004, June). A survey of biometric recognition methods. presented at 46th International Symposium Electronics in Marine, ELMAR-2004.

[4] Li, W., Zhan, C., & Zheng, G. (January 01, 2006). Cryptographic Key Generation from Biometric Data Using Lattice Mapping. Proceedings, 513-516.

[5] Network Working Group, R. Rivest & RSA Data Security. Retrieved July 25, 2010 from Internet FAQ Archives Web site: http://www.faqs.org/rfcs/rfc1321.html.

[6] A. Fahmy, M. Shaarawy, K. El-Hadad, G. Salama, and K. Hassanain(2005). A Total Key Dependent AES-like Algorithm. presenting at third International Conference on Informatics and Systems, Cairo University, Faculty of Computers and Information, Giza, Egypt.

[7] A. Fahmy, M. Shaarawy, K. El-Hadad, G. Salama, and K. Hassanain (2005). A Proposal For A Key-Dependent AES. Presenting at third International Conference on Sciences of Electronic, Technologies of Information and Telecommunications, TUNISIA.

[8] Faiz Yousif Mohammad, Alaa Eldin Rohiem, and Ashraf Diaa Elbayoumy(2009). A Novel S-box of AES Algorithm Using Variable Mapping Technique. Presenting at 13th International Conference on Aerospace Sciences and Aviation Technology, Military Technical College, Kobry Elkobbah, Cairo, Egypt.

[9] Krishnamurthy G N, and V Ramaswamy. Making AES Stronger: AES with Key Dependent S-Box. Published by International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008.

[10] M. Shaarawy, K. Hassanain, and E. Hesham. A Proposal for a Biometric Key Dependent Cryptosystem. Global Journal of Computer Science and Technology, GJCST Vol 10, Issue 11: August/Sept. 2010.

[11] Libor Masek, “Recognition of Human Iris Patterns for Biometric Identification”, The University of Western Australia,2003.

[12] “Portions of the research in this report use the CASIA-IrisV4 collected by the Chinese Academy of Sciences’ Institute of Automation (CASIA)” and a reference to “CASIA Iris Image Database, http://biometrics.idealtest.org/”

[13] M. Vandenwauver. Introduction to Cryptography, At Katholieke, Universities

[14] Biometrics and NSTC Subcommittee 2006. History Of Biometrics, http://www.Biometrics.gov

[15] Mr. P.P.Chitte, Prof. J.G.Rana, Prof. R.R.Bhambare, Prof. V.A.More, Mr. R.A.Kadu and M.R.Bendre. IRIS Recognition System Using ICA, PCA, Daugman's Rubber Sheet Model Together. International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 1.

[16] D. Antolovic. Review of the Hough Transform Method, With an Implementation of the Fast Hough Variant for Line Detection.Department of Computer Science, Indiana University and IBM Corporation