# An Efficient Iris Authentication Using Chaos Theory-based Cryptography for E-commerce Transactions

Arian Rahimi, Sharhriar Mohammadi, Rozita Rahimi

*Middle East Technical University, Turkey*
*K.N.Toosi University of Technology, Iran*
*Shahid Beheshti University, Iran*
*arian_rahimi@yahoo.com, smohammadi40@yahoo.com, rahimirosita@yahoo.com*

## Abstract

*E-commerce is an outcome of globalization and technology outbreak of 21st century. Increasingly, more products and services are sold over Internet; hence, there is a growing need for a combination of legislation and technical solutions to globally secure customer privacy. Credit card fraud is one of the crimes especially when it is used for web-based transaction. In this paper, a technical solution using Iris authentication technique is proposed for protecting identity theft in e-commerce transactions because Iris patterns are unique to an individual. Further, this research proposes authentication of e-commerce users by using Iris biometric technique as one of the most secure biometric algorithms. Therefore, this research proposes a web-based architecture which uses a combination of Image Processing and secure transmission of customers' Iris templates along with credit card details for decreasing credit card frauds over Internet.*

## 1. Introduction

Shopping over the Internet is another alternative to shopping at a brick-and-mortar store. Credit cards are the primary means of payment for goods and services purchased online. By means of credit card, its information is transmitted over the Internet, which may not have the same level of security as phone, mail, or fax. Security issues are maybe the most important thing in online shopping. Methods to ensure secure online payment by credit card are therefore important to the success of shopping over the Internet. In online transaction with credit card, buyers want to be assured that the provided information about credit card won't be abused or stolen (a possible fraud). Credit card fraud on the Internet is a more pervasive problem. Anybody who has access to a credit card number and expiration date can buy anything over the Internet. On the other hand, neither party can be certain of the other's identity [1]. Credit cards were designed to rely on physical signatures for authentication, a mechanism that is rendered useless in e-commerce. The online purchaser does not have to present a physical card, which may contain additional security features, e.g. additional code numbers, photographs.

So the lack of authentication of online customers is perceived. To counter this threat, the authentication of the buyer is essential. Authentication using biometrics is a secure approach that can be proposed. In fact, biometric technique is used for preventing identity theft and false authentication. Recently, human Iris recognition is recommended as approval of human identification. This organ of the eye which is well protected from the external environment is easily visible from within one meter of distance. Iris recognition is now considered as one of the best and most precise solutions to security problems for human identification because it is the most unique feature of every person which has been discovered by now [2]. So, Iris recognition can be used for authentication of online customers.

This paper proposes a web-based architecture to use encrypted Iris pattern as biometric attribute for authentication of a customer for e-commerce transactions which includes a secure biometric template transmission scheme and a high performance algorithm for Iris recognition as human identification.

## 2. Proposed web-based architecture using biometric authentication

This section which explains the proposed architecture contains two subsections: Image processing and secure template transmission scheme. In this paper, we are going to decrease online credit card frauds using both biometric template transmission scheme, as well as a new algorithm which has proposed for Iris recognition.

In this research, a technical solution is proposed to prevent credit card fraud in e-commerce transactions by using an Iris authentication technique. This method necessitates the existence of standardized Iris image capture and encryption software along with the web camera that is built in the recent computer systems. Here, a new algorithm is used to extract key characteristic features of Iris pattern of an individual. These features are encrypted using chaotic maps and steganography technique.

Copyright © 2009 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved.

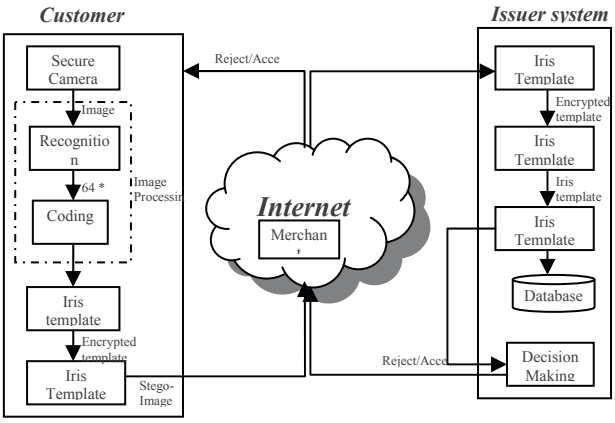



Figure 1. Proposed architecture for online credit card transaction

The result of such a combination provides not only a secure transmission of credit card details, but also achievement of high level authentication. A web-based architecture is proposed for implementing this solution. While issuing a credit card, the Iris details of an individual will be stored along with the credit card number and other personal details in the issuing agency's database. A software need to be present in all the client systems so that while doing e-commerce transactions, the Iris image of the individual can also be captured, encrypted and sent along with the name, credit card number, and expiration date. At the time of transaction the Iris image of the customer is captured using a web camera built in the client system. The Iris image is preprocessed, normalized, enhanced, and the key features of the Iris are extracted using our high performance algorithm (Figure1).

## 2.1. Image Processing

The possibility that the uniqueness of Iris of the eye could be used as a kind of optical fingerprint for personal identification was first suggested by ophthalmologists. However, John Daugman was the first person to use this idea for human identification as an algorithm [2], [3], [4], [5]. In the previous papers, the extensive amount of research has been done on Daugman's algorithm [6]. In this paper we are going to introduce an algorithm to improve the Daugman's algorithm in both speed and accuracy.

Every Iris recognition algorithm consists of 3 main sections; these sections are as follow:

1- The image is preprocessed to detect and separate Iris from the whole image

2- Features representing the Iris patterns are extracted as a code

3- Decision is made by means of matching

The basic technology of the recognition process belongs to John Daugman [5]. He encodes Iris pattern into a 256- byte Iris code by demodulating it with 2D Gabor wavelets at many different scales, while each resultant phasor angle in the complex plane is quantized. To compare each pair of Iris codes $C_j$ and $C_x$ bit-by-bit, their normalized Hamming Distance (HD) is defined as the fraction of disagreeing bits between them.

Wildes also makes isotropic band pass decomposition, derived from the application of Laplacian of Gaussian filters to the image data [7]. Also, Monro, *et al*. presented an Iris coding method based on differences of Discrete Cosine Transform (DCT) coefficients of overlapped segments from Iris images [8].

From all the algorithms that have proposed for Iris recognition, the Daugman's algorithm was the first and most famous one. That's why, all the previous models for online authentication has used the Daugman's algorithm.

In this paper, a novel algorithm is introduced for Iris feature extraction to represent a code that is invariant to translation, rotation and scale. In the following sections the new coding method is described by its matching algorithm. This is the block diagram of the Iris coding system.

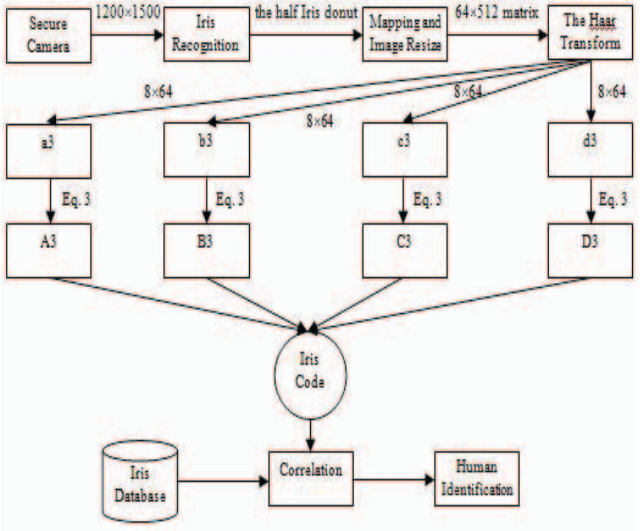



Figure 2. Iris Coding System

As we can see in Figure 2, the first part of Iris recognition process is image acquisition. This is done by means of a camera with some special conditions which apply for the camera type and the light conditions. Inappropriate lights of the environment could lead to bad results in Iris recognition. In this paper, a camera that captures images with 1200×1500 resolution is used. The output of the "Secure Camera" box is an1200×1500 image which Iris has to be extracted from it. This section is done in the "Iris recognition" box. In this box, the Iris is extracted from the whole image.

### 2.1.1 Proposed Algorithm of Iris Pattern Coding

In the new algorithm, we suggested that Iris has been detected from the whole image. Eyelids are different semi-circular arcs. Since the upper and lower eyelids always cover the Iris, it would be enough to use only half

of Iris without detection of eyelids as it is shown in equation 1.

$$R_d = R_p + \frac{R_i - R_p}{2}$$
$$P_r = round(2.\pi.R_d) \qquad (1)$$
$$V = R_d - R_p$$

Where $R_p$ and $R_i$ are the radius of the pupil and the Iris. $R_d$ has been nominated as above in order to consider half of the Iris. $P_r$ is the perimeter of the half of the Iris circle with the radius $R_d$ . $V$ also is the difference between $R_d$ and $R_p$. Now if we map the half Iris donut into matrix F, then we have matrix F in size of Pr×V as the basis image for Iris patterns, Eq. (2):

$$F(m,n) = I(x_0 + Cos(\theta_m).r_n, y_0 + Sin(\theta_m).r_n)$$
$$m = 1,2,...,Pr, \quad \Delta\theta = \frac{2\pi}{Pr}, \theta_m = m\Delta\theta \qquad (2)$$
$$n = 1,2,...,V, \qquad r_n = Rp + n$$

Where $(x_0, y_0)$ represent the center of the pupil in the eye image. By nominating F (m,n) as above, matrix F contained all pixels of half of the Iris. Due to the size of different Irises in different persons and illuminations, the size of matrix F could be different. By using the nearest neighbor interpolation, matrix F is resized to 64×512. This 64×512 matrix is the output of the "Mapping and the Image Resize" box (Figure 2). In fact, 64 circles between the outer boundary of pupil and the radius of $R_d$ were formed and in each circle, 512 points were considered. Figure 3 shows samples of Iris patterns.

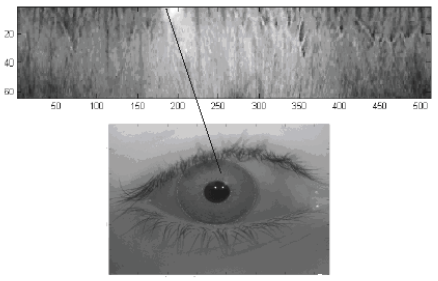
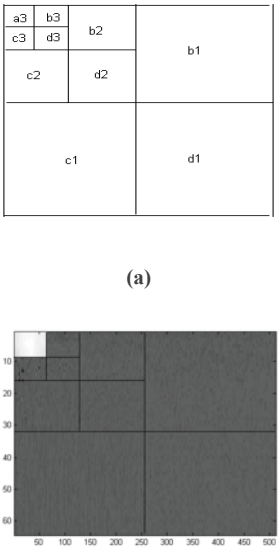


Figure 3.Sample iris and its rectangular block.

As shown in Figure 3, the half Iris donut has mapped into a 64×512 matrix. Then, the Haar Transform was applied in 3 levels to matrix F. 4 images in the first level, (a1, b1, c1, d1), 4 images in the 2nd level, (a2, b2, c2, d2), and also, 4 images in the third level, (a3, b3, c3, d3), in the size of 8×64 were formed. The blocks are shown in Figure 4.




**(a)**



**(b)**

Figure 4. a) Schematic of the Haar Transform in 3 levels b) one sample.

In this step, a3 was the third times low-pass filtered, and its values were very near to the mean value of matrix F. However, b3, c3, and d3 had negative and positive values to detect the edges in the different directions after quantization of these values by equation (3):

$$A3(m,n) = \begin{cases} 1 & a3(m,n) \geq mean(a3) \\ 0 & a3(m,n) < mean(a3) \end{cases}$$
$$B3(m,n) = \begin{cases} 1 & b3(m,n) \geq 0 \\ 0 & b3(m,n) < 0 \end{cases} \qquad (3)$$
$$C3(m,n) = \begin{cases} 1 & c3(m,n) \geq 0 \\ 0 & c3(m,n) < 0 \end{cases}$$
$$D3(m,n) = \begin{cases} 1 & d3(m,n) \geq 0 \\ 0 & d3(m,n) < 0 \end{cases}.$$

As we can see in Figure 4, after applying the Haar Transform in 3 levels to the matrix F, we have 4 blocks with the size of 8×64 and finally there were 4×8×64=2048 bits to code each Iris. As we can see in equation (3), in our Iris code, the first 512 bits, was the row-wise bits of A3, the second 512 bits was the row-wise bits of B3, the third 512 bits was the row-wise bits of C3, and the fourth 512 bits was the row-wise bits of D3. A3, B3, C3, and D3 are as equation (3).

## 2.1.2 Comparison

The last section of the Iris recognition process is to compare the Iris codes in order to authenticate the human identification. In this way, two vital points should be considered. First, the rotation of the eye in image acquisition leads to column shift in pattern matrix F. Second, some errors in recognizing the pupil and the Iris boundary in a few pixels, caused by the row shift in pattern matrix F. In order to avoid the rotation effect, the correlation operator between two Iris codes is implemented for matching instead of EXOR bit by bit. Hence, for comparison, correlation formula was applied between two Iris codes as equation (4):

$$\begin{aligned} MA_{i,j} &= \max_{(m,n)}\left[ A3_i(m,n) \circ A3_j(m,n) \right] \\ MB_{i,j} &= \max_{(m,n)}\left[ B3_i(m,n) \circ B3_j(m,n) \right] \\ MC_{i,j} &= \max_{(m,n)}\left[ C3_i(m,n) \circ C3_j(m,n) \right] \\ MD_{i,j} &= \max_{(m,n)}\left[ D3_i(m,n) \circ D3_j(m,n) \right] . \end{aligned} \quad (4)$$

Where $A3_i$ and $A3_j$ respectively belong to the ith and jth Iriscode. Two codes which belong to the same person, have a maximum MA, MB, MC and MD relation to the other codes.

### 2.1.3 Experimental Results

In this paper to avoid the obstruction problem of the iris by the eyelids, a new idea which is applied on half of the iris is suggested. Iris donut form was remapped to rectangular block in the size of 64 ×256. An efficient and simple feature extraction method which is based on the 2D-Haar Transform in 3 levels is presented which prepared 2048 bits for Iriscode by 4 images of level 3. In order to avoid the rotation effect, the correlation operator between two Iriscodes is implemented for matching instead of EXOR bit by bit. To compare the speed of the new algorithm, in MATLAB implementation, we compared the proposed algorithm with Daugman's method below:

Table1. Speed comparison between competing methods

| Method | Feature Extraction (ms) | Matching(ms) | Total(ms) |
|---|---|---|---|
| **Daugman** | 422 | 31 | 453 |
| **The proposed algorithm** | 171 | 15 | 186 |

## 2.2 Secure template transmission scheme

### 2.2.1 Problem of Encryption Algorithms

In encryption, there are two basic problems: i) hackers have historically found ways to crack encryption, in fact, obtaining the key without being a legitimate user; and ii) once a single legitimate copy of some content has been decrypted, a hacker is now free to make another copy of the decrypted data [9]. Some papers such as [1] suggest RSA as a cryptography method to encrypt biometric templates. RSA is a popular encryption algorithm among other algorithms but it encounters with some attacks such as timing attacks, adaptive chosen cipher text and branch prediction analysis attack. On the other hand, an attack against RSA is specifically possible when the message is short because brute force attack can be used to reveal the original message. This threat exists in iris template encryption because the volume of the “Iris Database” is very large and the biometrics information of every person is stored into it, so the Iriscode of every person shouldn’t be very large and every Iris template is a code with 2048 bits.

### 2.2.2 Cryptography Algorithm based on Chaos Theory

The name "Chaos theory" comes from the fact that the systems that the theory describes are apparently disordered, but Chaos theory is really about finding the underlying order in apparently random data. Chaos theory attempts to explain the fact that complex and unpredictable results can and will occur in systems that are sensitive to their initial conditions. In other words, it is possible that a very small occurrence can produce unpredictable and sometimes drastic results by triggering a series of increasingly significant events. Among the most promising applications of Chaos theory is its use in the field of “chaotic encryption” where the utilization of nonlinearities and forcing of the dynamical system to a chaotic state will fulfill the basic cryptographic requirements. Due to nonlinear mechanisms that lead to a chaotic behavior, this one is too difficult to predict by analytical methods without the secret key (initial conditions and/or parameters) being known. This would reduce a potential attack to one category that of a brute force attack, in which any attempt to crack the key depends directly upon how long the key is [10].

Classical cryptography works on discrete values and discrete time, while the crucial point in chaotic cryptography is the usage of continuous-value systems that may operate in continuous or discrete time. Chaotic maps and cryptographic algorithms have also some similar properties: sensitivity to initial conditions and parameters, random like behavior and unstable orbits with long periods, depending upon the precision of the numerical implementation. Encryption rounds of a cryptographic algorithm lead to the desired diffusion and confusion properties of the algorithm. In a similar manner, iterations of the chaotic map spread the initial

region over the entire phase space while the parameters of the chaotic map may represent the key of the encryption algorithm [10].

### 2.2.3 Process of Secure Transmission of Iris Templates

After Iris pattern coding and getting iris template using proposed algorithm, a novel chaotic secure content-based hidden transmission scheme of biometric data is used to secure transmission of it. Encryption and data hiding techniques are used to improve the security and secrecy of the transmitted iris templates. Secret keys are generated by the biometric image and used as the parameter value and initial condition of the chaotic map, and each transaction session has different secret keys to protect from the attacks. Two chaotic maps are incorporated for the encryption to resolve the finite word length effect and to improve the system's resistance against attacks. Encryption is applied on Iris codes before hiding into the cover/host image to make them secure, and then codes are hidden into the cover image. To transmit securely of Iris codes in e-commerce transactions, we have used steganography and cryptography to achieve highly secure Iris code transmission [11]. Steganography is a technique of concealed data, where a secret message is hidden within another unrelated message and then communicated to the other party. In digital realm, it involves embedding or hiding secret data into an inconspicuous cover file, such as JPEG image. The digital steganography process has three basic components: i) data to be hidden; ii) the core file, in which the secret data are to be embedded; iii) the resulting stego-file [9].

### 2.2.4 System Model for Secure Transmission of Iris codes

After capturing the eye image from the secure camera and performing the proposed algorithm for Iris coding the algorithm to extract the important features to be used to hide in the host image. To do this, two chaotic maps named Henon map and Logistic map are used to encrypt Iris code. Logistic map generates a secure pseudo random sequence, which is used as the sequence key and Henon map encrypts the Iris codes. It provides the following features: 1) resistant to the finite word length affect of the chaotic sequence; 2) very unpredictable; 3) robust against attacks; and 4) resistant to repeated group attack. In addition, the secret keys used as parameter value and initial condition of chaotic map are generated by the biometric, because biometric is very random at each enrollment of the person [9].
After encryption, the Iris code is embedded into the cover/host image and then end result of this step is a stego-image which contains encrypted and secured Iris code.

For this step, DWT-based (discrete wavelet transform) blind data hiding algorithm is used which does not require the original image to extract the iris code from the host image that contains hidden data. The reason for using DWT is due to its superior robustness against various signal processing attacks and high data compression (Figure 5(a)). To perform verification of a person's claimed identity, the stego-image is sent to the authentication server over network. At the server end, the stego-image is received and data extraction takes place from the cover/host image. After extracting the Iris code, a chaotic sequence is generated by the secret keys and applied on the extracted data to decrypt it in its actual form. The result of this step is the extracted Iris code ready to perform identification and verification in the pre-stored database (Figure 5(b))[11].

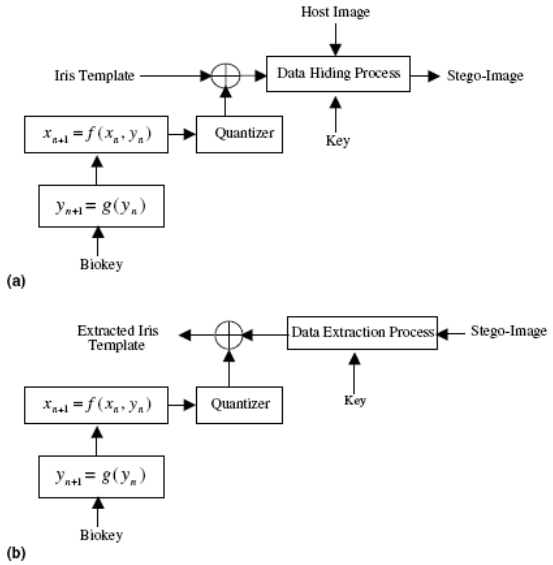



Figure 5. Iris-biometric template hiding/un-hiding process: (a) template hiding process and (b) template extraction process[12].

## 3. Conclusion

This paper has proposed a new model of architecture for online credit card transactions. There are so many algorithms that have created to help human identification through Iris recognition. The most popular one is named "Daugman". To prove this model, a program which shows better performance of Iris recognition algorithm in compare with Daugman's algorithm is created. In the new Iris coding algorithm, to avoid the obstruction problem of the Iris by the eyelids, a new idea which is applied on half of the Iris is suggested. Iris donut form was remapped to rectangular block in size 64 ×256. An efficient and simple feature extraction method which is based on the 2D- Haar Transform in 3 levels is presented which prepared 2048 bits for Iris code by 4 images of level 3. In order to avoid the rotation effect, the correlation operator between two Iris codes is implemented for matching instead of EXOR

bit by bit. Contribution of this paper can be divided to three parts as follow:

1. An extensive amount of research has been done on Daugman's algorithm. The paper shows an achievement of better speed and accuracy in compare with Daugman's algorithm. A high performance Iris recognition algorithm is proposed which makes an Iris template from Iris image of the person who conducts an online transaction by credit card.

2. Through literature review on securely transmission of Iris templates over Internet, it has been recognized that the chaos theory and steganography are appropriate techniques that can be used here. A combination of chaos theory and steganography technique is used to securely transmit Iris templates along with credit card details. Hereby, identification of customers can be archived.

3. The companionship of proposed technique of image processing and steganography-based technique can create efficient Iris recognition architecture suitable for usage in the Internet.

## 4. References


[1] Vagala,R.R, Sasi,S., 'Biometric Authenrication for e commerce Transaction', published in the proceeding of international workshop on Imaging Systems and Techniques(IEEE IST),2004

[2] Daugman JG (1993) High confidence visual recognition of persons by a test of statistical independence. IEEE- PAMI, 15: 1148-1161.

[3] Daugman JG (2002) How Iris recognition works. The Computer Laboratory, Cambridge, Iridian Technologies, U.K.

[4] Daugman J (2003) Demodulation by complex-valued wavelets for stochastic pattern recognition. International Journal of Wavelets, Multiresolution and Information Processing, 1: 1-17.

[5] Daugman J (2004) How Iris recognition works. IEEE Trans. Circuits and Systems for Video Technology, 14: 21-30.

[6] Rajendra Reddy, Vangala Sreela Sasi, "Biometric Authentication for E-Commerce Transaction", IEEE IST 2004, International Workshop on Imaging Systems and Techniques, Stresa Italy, 14 May *2004*

[7] Wildes RP (1997) Iris recognition: an emerging biometric technology. IEEE Proceeding, 85: 1348-1363.

[8] Monro DM, Zhang D (2007) DCT-Based Iris Recognition. IEEE PAMI 29: 586-595.

[9] Khan,M.K, Zhang,J.,Tian,L."Chaotic secure content-based hidden transmission of biometric templates", journal of Cahos,Solitions and Fractals, vol. 32, pp.1749-1759,2007

[10] Ljupco Kocarev, "Chaos-Based Cryptography: A Brief Overview", IEEE CAS Newsletter, 2001, pp. 18-19

[11] Khan, M.K, Zhang,J., Tian,L., "Protecting Data for Personal Identifiaction ",Sinobiometrics,pp. 629-638,2004

[12] Randy C. Marchany, Joseph G. Tront, "E-Commerce security issues", Proceedings Of the 35th Hawaii Intemational Conference on System Sciences, January 7-10, 2002.