Efficient Iris Biometrics Technique for Secure Distributed Systems

Ameer A. Mohammed Baqer[1†] and Suhas H. Patil [2††],

[1,2]Department of Computer Engineering, College of Engineering,
Bharati Vidyapeeth Deemed University, Katraj, Pune, INDIA

Summary
In recent years the need has grown for the use of distributed systems for use in different applications and this applications become used in many areas and as an example for the applications of distributed systems is the E-commerce transactions, E-commerce is a set of e-business such as sales, purchase or exchange of goods and this business is done through large computer networks (such as the 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 Efficient and fast Iris recognition method as an authentication technique is proposed for protecting identity theft in e-commerce transactions because Iris patterns are unique to an individual. 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.

Key words:

iris recognition; biometric authentication; distributed system.

1. Introduction

In reality, the Web represents a huge distributed system that appears as a single resource to the user available at the click of a button. There are several definitions and view points on what distributed systems are. Coulouris defines a distributed system as "a system in which hardware or software components located at networked computers communicate and coordinate their actions only by message passing" [1]; and Tanenbaum defines it as "A collection of independent computers that appear to the users of the system as a single computer" [2]. Leslie Lamport – a famous researcher on timing, message ordering, and clock synchronization in distributed systems once said that "A distributed system is one on which I cannot get any work done because some machine I have never heard of has crashed" reflecting on the huge number of challenges faced by distributed system designers. Despite these challenges, the benefits of distributed systems and applications are many, making it worthwhile to pursue.

Various types of distributed systems and applications have been developed and are being used extensively in the real world. In this article, we present one of the main Application of distributed systems that is e-commerce transactions where in this paper we propose 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 templates transmission and a high performance algorithm for Iris recognition as human identification.

2. Biometric Authentication

Biometric authentication virtually eliminates the risk of anonymity in a two-factor security scenario by using a physical attribute of the person to authenticate a token. The process is similar to biometric identification. First, the requestor presents a token to assert identity. For example, an ATM or credit card is inserted into a reader. (A number encoded on the card is actually the token; the card is more like a container for the token, but treating the card as a token is appropriate.) As with identification, the system must acquire an image of the personal attribute. Second, the attribute must be localized, minutiae extracted, and a matching template created. Finally, the value of the token is used to look up the template previously stored for this individual. If it matches the template presented on this occasion, the requestor is authenticated, all the above stages explained in the Figure (1)[3].

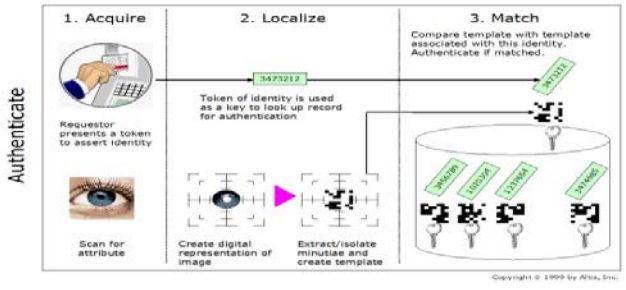

Figure 1: Biometric Authentication Process.

Manuscript received March 5, 2013
Manuscript revised March 20, 2013

3. Biometric Iris-Based Authentication

Having an iris-based authentication system can bring us a list of benefits, for instance [4], [5], [7]:

- Resistance to false matching and exceptionally high levels of accuracy, due to the unique textures of the iris.
- Stability of characteristic over lifetime, since the iris is an internal organ that is well protected against damage and wear.
- Suitability for both physical and logical access (in both verification and identification cases).
- Externally visible and noninvasive to the user, unlike the retina scan.
- Efficient encoding and search speed (Of course, it depends on the algorithm).

On the other hand, this technology also has its deficiencies, including [5], [6]:

- Difficulty of usage, since acquisition of the image requires moderate training and attentiveness in the non-automatic systems.
- False non-matching and failure to enroll, due to poor image quality of a small moving target, sometimes obscured by eyelashes, lenses, and/or reflections.
- User discomfort with eye-based technology.
- Need for a proprietary acquisition device for deployment.

4. Proposed web-based system using Biometric Authentication

In this section we explain the proposed architecture for our system, that system contains two subsections: Image processing and secure template transmission scheme. Also in this paper, we are going to explain the content of the biometric authentication packet in our proposed system that is used that is explained in Figure. (2).

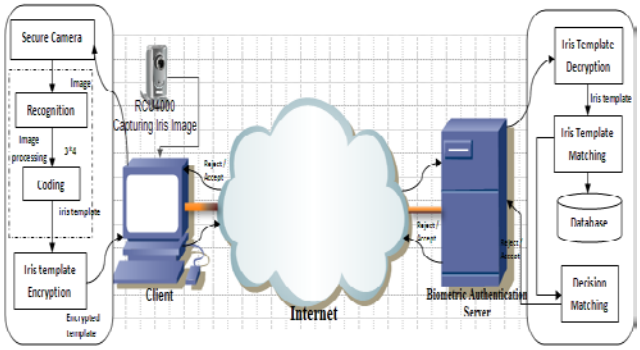

Figure 2: Proposed Web-based system for e-commerce transaction.

In this research, the proposed system used 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, iris recognition algorithm is used to extract key characteristic features of Iris pattern of an individual. These features are encrypted using chaotic maps . 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 this operation is called Enrollment. 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, Figure(2).

A biometric Authentication packet contain two parts:

- Iris template that is encrypted by chaotic maps.
- The encryption key that is sent to the server Issuer side to decrypt the iris template.

The steps for processing the biometric authentication packets is explained in Figure (1).

5. 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 [8], [9], [10], [11]. In the previous papers, the extensive amount of research has been done on Daugman's algorithm [12], the Boles's algorithm[13]and the Arian's algorithm[7]. In this paper we are going to introduce an algorithm to improve the Daugman's algorithm and another algorithms 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

Daugman[8,10]presented an algorithm that needs to process the two dimensional information of the texture, and increases feature extraction time; Wildes[14,15] used the Gauss-Laplace filter to decompose the iris image under the different resolution, and carried on the correlation comparison for the corresponding images, the computation is huge; Boles and Boashash[13] proposed a novel iris recognition algorithm based on zero crossing detection of the wavelet transform, this method has only obtained the limited results in the small samples, and this algorithm is sensitive to the grey value changes, thus recognition rate is lower.

This paper presents a Efficient iris recognition method based on the natural-open eyes. Firstly, it makes preprocess to iris image, ensures the effective iris area adaptively. Secondly, it finds all iris feature points by directional information, length information, width information of texture, the neighboring gray information and relativity in the effective iris area. Thirdly, it makes codes to feature points and figures the iris pattern by iris codes. Finally, it sorts the different iris patterns by auto accommodated pattern matching method and gives the recognition results.

Usually an iris image impossibly contains the iris merely, there are also other parts of the eye such as the eyelid, the eyelash. This point may be seen clearly from Figure 3. The interior boundary of iris can change, and make the texture of iris distort. In order to realize exactly matching, it must eliminate these factors through the image preprocessing. Iris image preprocessing includes iris localization, eyelid fitting, eyelash detection and normalization [16].

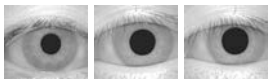

Figure 3: Iris Images.

A. Iris localization: Firstly, it finds the sketchy pupil center through the gray projection and the pupil center detection operator; Secondly, finds four iris inner boundary points by the direction edge detection operator and the voting mechanism beginning from the sketchy pupil center, and locates the iris inner boundary according to these four points; Finally finds four iris outer boundary points by the direction edge detection operator and the voting mechanism beginning from the center of pupil, and locates the iris outer boundary according to these four points. Localization accuracy rate of this method is high, the speed is quick.

B. Fitting lower lid: Firstly it uses Canny operator to extraction edge information of iris image, then uses the parabolic equation as formula (1) to fit the lower eyelid:

$$y = a (x - b)^2 + c \qquad (1)$$

a is the parabola curvature; **b**, **c** are the horizontal and vertical coordinates of parabola apex respectively. Through establishing different a, b, and c it may fit the lower eyelid well, thus it can eliminates influence of the lower eyelid for the effective iris region. It finds the parabola apex. The resultant images of Figure 3 are shown in Figure 4.

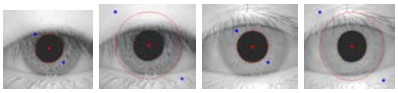

Figure 4: The resultant images of iris location and fitting the contour of the lower eyelid.

C. Eyelash detection: Firstly, it makes sure the search area. The parameters of inner boundary and outer boundary are (x_p , y_p , r_p) and (x_i , y_i , r_i) respectively. It chooses two rectangles of the left and right sides of the pupil as the possible area covered by the eyelash. The four vertexes of right area are $(x_p , y_i - r_i)$, $(lWidth - 1 , y_i - r_i)$, $(x_p, y_i + r_i)$, $(lWidth - 1 , y_i + r_i)$.The lWidth is the width of the image. The four vertexes of left area are $(0 , y_i - r_i)$, $(x_p , y_i - r_i)$, $(0 , y_i + r_i)$, $(x_p , y_i + r_i)$.

Because the gray of eyelash is low, so a template of detection eyelash is designed, its shape is shown in Figure 5.Each sub-template X1 , X , X2 may compose by single pixel or multiple pixels. If a sub-template is composed by a single pixel, this pixel corresponds the center of the sub-template; if a sub-template is composed by N(N>=2) pixels $\{a_1,a_2,\ldots,a_N\}$,the center pixel locates at n=ceil(N/2) and a_n is the center pixel of the corresponding sub-template. It looks the center of X as the current point and sums the gray difference with X1,X2 respectively, if two difference is less than 0, the current point is taken as the candidate eyelash point.

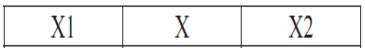

Figure 5: Eyelash detection template

D. Iris normalization: After locating the iris, it cannot carry on the code for the locating iris image immediately, and should carry on the calibration firstly. Therefore it should adjust each primitive image to the same size and corresponding position through normalization. This article used the polar coordinate transform to carry on the normalization, because the inner and outer circles are not concentric, this kind of transform is not concentric. During the experiments, beginning from the upper vertical radius of pupil center it unwrapped the ring like iris to rectangular iris of 512×64 according to the counter clockwise. In the normalized image, the row direction coordinate of point D which confirmed in section B is rD. In Figure 3 four image's normalized result as shown in Figure 6. The white rectangular area is the

effective iris area. The width along vertical direction of the rectangle is rD, the vertical line of the left part of rectangle corresponds the connecting line locating at the left of the center of pupil with the minimum slope confirmed in section C and the horizontal coordinate of each
point in the line is X_1, the vertical line of the right part of rectangle corresponds the connecting line locating at the right of the center of pupil with the maximum slope confirmed in section C and the horizontal coordinate of each point in the line is X_r.

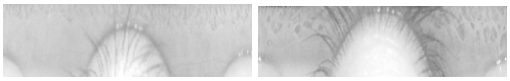

Figure 6: The processing image of pre-processing

5.1 Feature Extraction and Code

An iris image contains much detail texture, the texture is composed by many shape blocks such as strip and speckle, the gray differences are big and distribute unevenly, these blocks with irregular shape can be as distinguish characteristics for iris recognition[16].

Firstly we need to determine the collective and effective coding region of the entering iris and the registering iris, this region does not contain noise such as eyelash, eyelid and facula. We suppose vertical coordinates of D point of the entering iris and the registering iris in the normalized image are r_D *Enroll* , r_D *Register* respectively, and determine the smaller value as r_D *Match* between two values x_1,x_r, of the entering iris and the registering iris in the normalized image are x_1*Enroll* , x_r*Enroll* and x_1*Register* , x_r*Register* respectively, determine the bigger value as x_1*Match* , x_1*Enroll* between and x_1*Register*, and determine the smaller value as between x_r*Match* , x_r*Enroll* between and x_r*Register* . So we determine collective and effective texture region of the entering iris and the registering iris.

Considering the block characteristics of iris texture, it first makes sub-block for the image, the size of the block is M*N(M and N are integers) and ensures not overlap between each block. The number of block is (ceil((xrMatch - x1Match)/N))*(ceil(xDMatch /M)) in the collective and effective area of entering iris and registering iris, the horizontal number of block is Hnum= ceil((xrMatch - x1Match)/N) , the vertical number of block is Vnum=(ceil(xDMatch /M)).

In order to realize the compression code, it accumulates all the gray values in each block, the average of this accumulation is the gray value of the center point. During the feature extraction, it makes code by taking the center point of each block image as the basic feature point. This code method plays well in the compression, what is more, this can not lose feature points.

In the collective and effective area of iris image, considering the texture characteristics which are the strength of the edge and direction information of texture it takes the basic feature point as the center point and considers the eight neighborhood of each center point, these eight points correspond to the four directional texture of the center point such as 45° , 90° , 135° and 180°. Each direction corresponds to two adjacent points, the neighborhood relationship is shown in TABLE 1. In each direction it calculates the gray differences between two adjacent points and the center point respectively, if two gray differences are bigger than zero, the corresponding code bit $procode_k(i , j)$ of the center point in this direction sets "1", otherwise sets "0". K(45,90,135,180) corresponds the direction respectively.

Table 1: The Relational Of Adjacent Points

Texture of 45 degree	Texture of 180 degree	Texture of 135 degree
Texture of 90 degree	Current center point	Texture of 90 degree
Texture of 135 degree	Texture of 180 degree	Texture of 45 degree

Then according to the formula (2) it calculates four directional output values of each basic feature point[16]:

$$\left.\begin{aligned} Direction_{180}(i,j)&=(I(i,j-1)+I(i,j+1)-2*I(i,j))/2\\ Direction_{135}(i,j)&=(I(i+1,j-1)+I(i-1,j+1)-2*I(i,j))/2\\ Direction_{45}(i,j)&=(I(i-1,j-1)+I(i+1,j+1)-2*I(i,j))/2\\ Direction_{90}(i,j)&=(I(i-1,j)+I(i+1,j)-2*I(i,j))/2 \end{aligned}\right\} \quad (2)$$

Among them , i=0,1,…., ceil((x_rMatch – x_1Match)/N)-1, j=0,1,…, (ceil(r_DMatch /M))-1, I(i,j) expresses the corresponding gray value of each basic feature point.

Finally, it eliminates the false feature points, the detail method is as follows: it records the directional number K(45,90,135,180) with the maximal directional out value of each basic feature point According to formula (3) it makes binary code for each basic feature point, if a directional code of each basic feature point is “1” and this directional out value is bigger than three other directional out values, this directional code is still “1”, three other directional codes are set “0”; otherwise this directional

code is set "0". It makes similar operation for four directional codes of each basic feature point[16]:

$$code_a(i,j)=\begin{cases} b & a=K, procode_a(i,j)=b \\ 0 & a\neq K \end{cases} \quad a=45,90,135,180, b=0,1 \qquad (3)$$

Among them, a expresses the corresponding directional code bit, so it gets:
(ceil((x_rMatch – x_1Match)/N))* (ceil(r_DMatch /M))*4 bits code.

5.2 Iris Match

In the collective and effective area, we make match to the entering iris and registering iris. The corresponding codes of the entering iris and registering iris are $Registercode_i$, $Enrollcode_i$ which correspond to the code of each directional output value $Direction_a$ respectively. i=1,2,3,4; a=45,90,135,180; i=1 corresponds to the directional code of 45 degree, i=2 corresponds to the directional code of 90 degree, i=3 corresponds to the directional code of 135 degree, i=4 corresponds to the directional code of 180 degree[16].

When we compare with two iris codes, because the anterior normalized operation can not solve the revolving invariable problem, we need to carry on certain revolving match for registering iris and entering iris. The revolving can be compensated even the corresponding code of the registering iris and the entering iris can not correspond completely. This article solves the revolving invariable problem in the normalized image, this may transform the revolving operation in the annular iris to the translation operation in the rectangular iris. The concrete method is as follows: when it compares with two iris codes, maintains the code of the registering iris motionless, and the code of the entering iris is translated several pixels to left or right along horizontal direction (because the angles of rotation of image is not big, translation pixels are small), it calculates a match value with the registering iris code after translating one pixel, after the translation ends, we keep the maximum of all the match values as the final match value of the registering iris and the entering iris. We sum the match distance by formula (4) as follows:

$$Md_{3\times 3}=\max_{\substack{(p=-2,-1,0,1,2)\\(q=-2,-1,0,1,2)}}\left\{\sum_{K=1}^{K=4}\sum_{m=0}^{m=ceil((x_r Match-x_l Match)/N)-1}\sum_{n=0}^{n=ceil(r_D Match/M)-1}\left[Registercode_K(m,n)\,\&\,Enrollcode_K(m+p,n+q)\right]\right\} \qquad (4)$$

The final match distance Md is as following:

$$Md=Md_{3\times 3}/\left(ceil\left(\frac{x_r Match-x_l Match}{N}\right)\times ceil\left(\frac{r_D Match}{M}\right)\right) \qquad (5)$$

5.3 Experimental Results

When we carry on the recognition experiment, we weigh the algorithm with false acceptance rate (FAR), false rejection rate(FRR), equal error rate(EER), and correct recognition rate(CRR). Simultaneously we inspect the algorithm with the execution time, including feature extraction time, match time. We use the CASIA in the iris database [9] 567 images, including 81 different irises of eyes, each eye had 7 8-bit images, the resolution is 320×280. We carry on the recognition experiments 160461 times, the inter-class experiments was 158760, the intra-class experiments was 1701.

When the size of block is 3*4, the experimental result is best. The threshold of match distance is 0.22922, CRR=99.685%, FAR=0.313051%, FRR=0.293945%, namely the correct recognition results are 159959 times, the false rejection results are 5 times, the false acceptance results are 497 times. We carry on the duplicated experiments for two previous mentioned methods in the same image samples, the experimental results are listed in Table (2).

Table 2: The Accurate Recognition Rate Of Different Algorithm

Method	CRR(%)	EER (%)	Feature extraction time(ms)	Match time (ms)	Total time (ms)
Daugman	100	0.05	443.0	4.0	448.000
Boles	67.5	7.1	86.0	9.0	95.746
Arian	99.684	0.273	87.0	5.0	92.999
Proposed	99.685	0.281	6.0	5.0	11.999

The CRR of this article under the threshold value is slightly lower than the Daugman's algorithm, but is higher than Boles's algorithm and Arian's algorithm.

6. Secure Template Transmission Schema

6.1 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 [17]. 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 [17].

6.2 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 data technique 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. To transmit securely of Iris codes in e-commerce transactions, we have used cryptography to achieve highly secure Iris code transmission [18], In the Figure(7) we can see the Iris code before and after we applying the encryption.

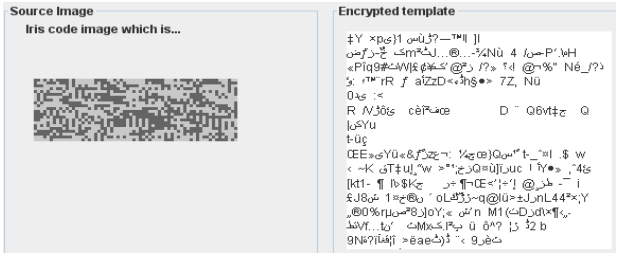

Figure 7: a) Iris code Before Encryption. b) Iris code After Encryption

6.3 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 Encrypted. 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 [19].

To perform verification of a person's claimed identity, the Encrypted Iris codes is sent to the authentication server over network. At the server end, the Encrypted Iris codes is received. After receiving the Encrypted 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(2)[18].

7. Conclusion

This paper has proposed a new secure model of architecture for online credit card transactions as example for using the distributed systems in the applications. 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, in this paper we introduced high performance of Iris recognition algorithm in compare with Daugman’s algorithm and the other algorithms is created. The new Iris recognition method based on the natural-open eyes. This method can find the iris characteristic point in a short time, the recognition rate is high, the recognition speed is guaranteed. And also we displayed in our paper how can provide securely transmission of iris templates over Internet, it has been recognized that the chaos theory as appropriate security technique that can used in our system, that is used to provide authentication and identification to the customers , they used the credit card.

References

[1] G. Couloris, J. Dollimore, T. Kinberg,2001, Distributed Systems-Concepts and Design, 4th Edition, Addison-Wesley, Pearson Education, UK.

[2] A. Tanenbaum and M. Van Steen,2002, Distributed Systems: Principles and Paradigms, Prentice Hall, Pearson Education, USA.

[3] Ganorkar, S. R., & Ghatol, A. A., 2007. Iris Recognition: An Emerging Biometric Technology. International Conference on Signal Processing, Robotics and Automation, Corfu Island, Greece, pp. 91-96.

[4] Iridian Technologies. Iris Recognition Basics, science behind the technology, http://www.iriscan.com.

[5] Ratha, N. K., Connell, J. H., & Bolle, R. M., 2003. Biometrics break-ins and band-aids. Pattern Recognition Letters, Vol. 24, pp. 2105-2113.

[6] International Biometric Group, 2006. Biometric market by technology, http://www.biometricgroup.com.

[7] Arain R., Sharhriar M., Rozita R.,2010.A New Web-based Architecture Based on Iris Biometrics Technique to Decrease Credit Cards Frauds over Internet. International Journal of Digital Society (IJDS), Vol. 1, pp. 86-93.

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

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

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

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

[12] Rajendra Reddy, Vangala Sreela Sasi,2004,“Biometric Authentication for E-Commerce Transaction”, IEEE IST 2004, International Workshop on Imaging Systems and Techniques, Stresa Italy.

[13] W. Boles, B. Boashash,1998,“A human identification technique using images of the iris and wavelet transform, ” IEEE Transaction on Signal Processing, 46(4): 1185–1188.

[14] R. Wilde, J. Asmuth, G. Green,1996, “A machine-vision system for iris recognition, ” Mach. Vis. Applic, 9: 1–8.

[15] R. Wildes,1997, “Iris recognition: an emerging biometric technology, ” Proc. IEEE, 85(9): 1348–1363.

[16] Zhonghua Lin,2010, "A Novel Iris Recognition Method Based on the Natural-Open Eyes", ICSP – IEEE, pp. 1090-1093.

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

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

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

Ameer A. Mohammed Baqer received BE. In Computer Engineering from Department of Computer Engineering and Information Technology, University of Technology , Baghdad, Iraq in 2006, and Know M-Tech. (Research Scholar) in Department of Computer Engineering , College of Engineering , Bharati Vidyapeeth Deemed University, Pune, India. His current area of research includes Computer Engineering, including Embedded Systems (esp. VHDL implementation of DSP Systems), Biometrics , Security. He is a member of the International Association of Engineers (IAENG), and member of the International Association of Computer Science and Information Technology (IACSIT).

Dr. Suhas H. Patil is a Professor and Head, Department of Computer Engineering and Information Technology, College of Engineering, Bharati Vidyapeeth University, Pune, India. His current area of research includes Operating System, Computer Network, Expert System, Distributed System. He has also presented more than one hundred research articles in national and international conferences. He has written nine books related to his research work.