Color Based Segmentation Iris image for Secure Distributed Systems

Ameer A. Mohammed Baqer, Hind Rostom Mohammed

Abstract— 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 authentication technique is proposed for protecting identity theft in e-commerce transactions. 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.

Iris image detection method based on color based segmentation and morphological operation is proposed. The color based segmentation takes in only two color spaces HSI and YCrCb, instead of three color spaces, followed by the morphological operations and a template matching. For each stage a novel algorithm which combines pixel and region based color segmentation techniques is used. The experimental results confirm the effectiveness of the proposed algorithm.

Index Terms— Secure Distributed Systems, Iris mage detection, Image Color, Morphology Operations, HSI color space, YCbCr color space, Components, Template matching.

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 viewpoints on what distributed systems are. Color is 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.

The paper is organized as follows; Section 2 deals with the Physiological Biometrics, Section 3 deals with Proposed web-based architecture using biometric authentication, Section 4 deals with the color based segmentation where different color spaces, HSI and YCrCb , Section 5 deals with the Iris Feature Extraction , Coding and Match, Section 6 deals with the Experimental Results, section 7 deals with the design Secure Template Transmission Schema 7.1. Cryptography Algorithm based on Chaos Theory, last section 8 ends the paper with conclusion.

2 PHYSIOLOGICAL BIOMETRICS

Physiological biometrics depends upon the physical appearance of the human body or shape of the human like nose, chin, eyes, face and lips etc. Face recognition, finger print, iris technology, retina technology, hand geometry, odour or DNA deoxyribonucleic acid etc. are the examples of physiological biometrics as shown in fig1.

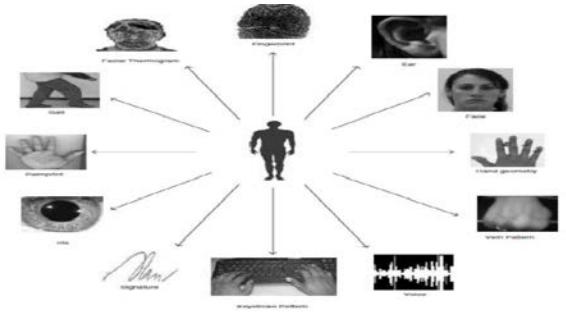


Fig.1. Biometric traits

The human iris is an annular part between pupil (black portion) and cornea shown in. Iris is an inner organ part of hu-

- *Ameer A. Mohammed Baqer is currently Assistant Lecturer and Director of Training Department at IT-RDC at the University of Kufa, Iraq,. E-mail: ameer.alshammaa@uokufa.edu.iq*

- *Hind Rostom Mohammed is currentlyAssistant Professor and Head of computer science department in Faculty of Mathematical and Computer Sciences at the University of kufa, Iraq. E-mail: hindrustum.shaaban @uokufa.edu.iq* man body. The structure of human Iris contains five layers of fiber like tissues. These tissues are very complex and reveal in various forms. The surface of iris also contains a complex structure such as crystals, thin threads, spot con caves, radials, furrows, stripes etc. Iris is a place where our nerve systems are situated and it gives information about human body [10].

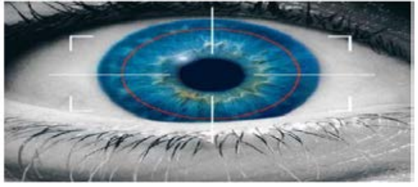


Fig.2. Iris Recognition Biometric

3 Proposed Web-Based Architecture 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. In this paper, we are going to introduce good technique to choose shortest reliable path to sending Biometric Authentication packet to decrease the forgetting of this packets and the time that is require to arriving the packet from the source to destination, also we explain the content of the biometric authentication packet in our proposed system that is used fig2.

In this research, a technical solutions is proposed to prevent the losing biometric authentication packet and decrease the time that is require to sending the packet to destination, also this 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. 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, fig3.

A biometric Authentication packet contains 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 are explained in fig4.

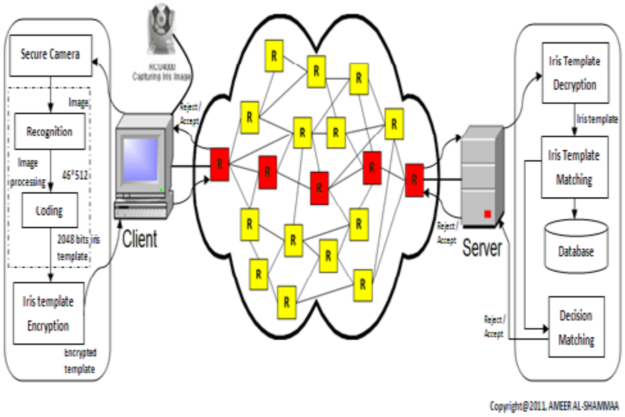


Fig.3 Proposed Web-based system for e-commerce transaction

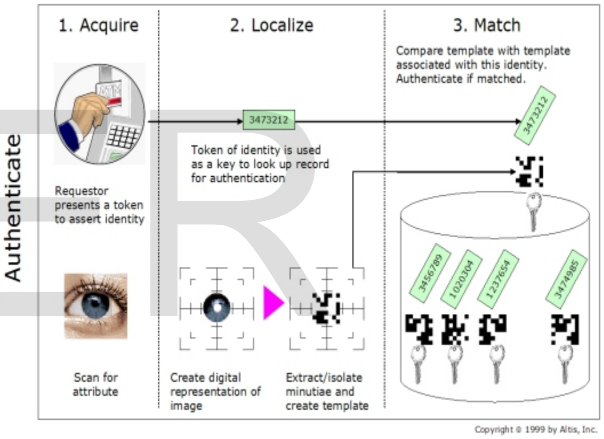

1. Acquire
2. Localize
3. Match
Authenticate
Compare template with template associated with this identity. Authenticate if matched.
3473212
Token of identity is used as a key to look up record for authentication
Requestor presents a token to assert identity
3456789
1020304
1237654
3474985
Scan for attribute
Create digital representation of image
Extract/isolate minutiae and create template
Copyright © 1999 by Altis, Inc.

Fig.4 Biometric Authentication Process

4 Color Based Segmentation

Iris recognition has recently emerged as one of the top biometric authentication methods due to its accuracy and outstanding identification efficacy. It is also commonly believed that the pattern of iris tissue is highly stable throughout the human live, although recent scientific notifications start to surprisingly suggest the opposite hypothesis [11].

Segmentation is subdividing an image into its constituent regions or object. The level up to which the subdivision is carried out depends on the problem being solved. A human Iris color model is used to decide either a pixel is Iris color or non-Iris-color [5]. This model is characterized by a classification algorithm and color space used to represent pixel color. Color spaces used in Iris color segmentation include YCbCr, HSV and RGB [6]. A wide variety of them have been applied to the problem of Iris color modeling (Iridian Technologies). Because color is a powerful fundamental feature and because it is, under constant illumination, almost invariant to scale, orientation and partial occlusion, we propose a method using color information to extract efficiently human Iris in images captured in complex environmental conditions. Iris-color image segmentation is computationally inexpensive and is robust to cluttered background [7]. In this research, we use the HSV (hue, saturation, value) color representation because it is compatible with the human color perception and because previous work has shown that this color space is one of the most adapted for Iris-color detection [12]. The HSV color space is obtained by a non-linear transformation of the fundamental RGB color space. We use the cone representation of the HSV color space, where H, S and V are all normalized in the range [0,1]. The H and S components represent the chromatic information, while V represents the luminance information [6]. In the literature [13],[14], there are many color based face detection algorithm, but the proposed algorithm uses the two color spaces only namely, HSI and YCbCr. The bounding ranges calculated for the values of H, Y, Cb and Cr were used to generate the binary images.

Hue-saturation based color spaces were introduced when there was a need for the user to specify color properties numerically. Describe color with intuitive values, based on the artist's idea of tint, saturation and tone. Hue defines the dominant color (such as red, green, purple and yellow) of an area; saturation measures the colorfulness of an area in proportion to its brightness. Many applications use the HSI color model.

Machine vision uses HSI color space in identifying the color of different objects. Image processing applications such as histogram operations, intensity transformations and convolutions operate only on an intensity image. These operations are performed with much ease on an image in the HIS color space. For the HSI being modeled with cylindrical coordinates.

Iris color classification in HSI color space is the same as YCbCr color space but here the responsible values are hue (H) and saturation (S) [12]. YCrCb is an encoded nonlinear RGB signal, commonly used by European television studios and for image compression work. Color is represented by luma (which is luminance, computed from nonlinear RGB. RGB components convert to YCbCr components by Equation:

$$Y=0.299R+0.587G+0.114B$$
$$Cb=-0.169R-0.332G+0.500B$$
$$Cr=0.500R-0.419G-0.081B \quad (1)$$

Different plots for Y, Cb and Cr values for face and non-Iris pixels were plotted and studied to find the range of Y, Cb and Cr values for face pixels. After experimenting with various thresholds the best result were found by using the following rule for detecting the Iris pixel:

$$135<Y<145$$
$$100<Cb<110$$
$$140<Cr<150 \quad (2)$$

The results are shown in Fig .5 (A): Original Iris Image, (B) YCbCr Iris Image and results are shown in Fig.6 (A): Original Iris Image with Y Plane, Cb Plane and Cr Plane. The transformation simplicity and explicit separation of luminance and chrominance components makes this color space attractive for Iris color modeling. In pursuing this goal, we looked at three color spaces that have been reported to be useful in the literature, HSV and YCrCb spaces, as well as the more commonly seen RGB space. Below we will briefly describe what we found and how that knowledge was used in our system [9].

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 [14] and the Arian's and Wilds algorithm [15]. 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.

5 Iris Feature Extraction, Coding and Match

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, and 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 rD Enroll , rD Register respectively, and determine the smaller value as rD Match between two values x1,xr, of the entering iris and the registering iris in the normalized image are x1Enroll , xrEnroll and x1Register , xrRegister respectively, determine the bigger value as x1Match , x1Enroll between and x1Register, and determine the smaller value as between xrMatch , xrEnroll between and xrRegister . 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 cannot 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 procodek(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°	**Texture of 180°**	**Texture of 135°**
Texture of 90°	Current center point	Texture of 90°
Texture of 135°	Texture of 180°	Texture of 45°

Then according to the formula (3) it calculates four directional output values of each basic feature point[16]:

$$\left.\begin{array}{l} \text{Direction}_{180}(i,j)=(I(i,j-1)+I(i,j+1)-2*I(i,j))/2 \\ \text{Direction}_{135}(i,j)=(I(i+1,j-1)+I(i-1,j+1)-2*I(i,j))/2 \\ \text{Direction}_{45}(i,j)=(I(i-1,j-1)+I(i+1,j+1)-2*I(i,j))/2 \\ \text{Direction}_{90}(i,j)=(I(i-1,j)+I(i+1,j)-2*I(i,j))/2 \end{array}\right\} \quad (3)$$

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 (4) 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]:

$$code_a(i,j)=\begin{cases} b & a=K, procode_a(i,j)=b \\ 0 & a\neq K \end{cases} \quad a=45,90,135,180, b=0,1 \qquad (4)$$

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.

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 Registercodei , Enrollcodei which correspond to the code of each directional output value Directiona 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.

When we compare with two iris codes, because the anterior normalized operation cannot 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 cannot 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.
The final match distance Md is as following:

$$\mathbf{Md} = \mathbf{Md}_{3\times3}/(\mathbf{ceil}\left(\frac{\mathbf{x_rMatch - x_1Match}}{\mathbf{N}}\right)\times \mathbf{ceil}\left(\frac{\mathbf{r_DMatch}}{\mathbf{M}}\right)) \qquad (5)$$

6 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, and 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.

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.

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	448.00
Boles	67.5	7.1	86.0	9.0	95.746
Arian	99.68	0.27	87.0	5.0	92.999
Proposed	99.68	0.28	6.0	5.0	11.999

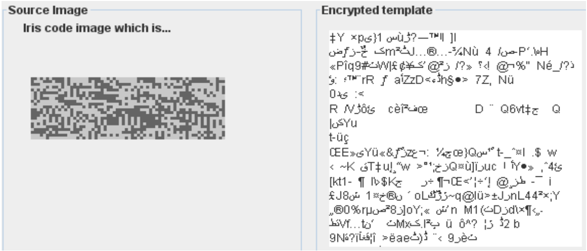
7 SECURE TEMPLATE TRANSMISSION SCHEMA

7.1 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].

7.2 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 is 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 [15], In the Fig. 5; we can see the Iris code before and after we applying the encryption.



```
‡Y ×pى}1 سûژ?—™‖ ]I
ضرƒز-ځ کسm²ڷJ...®...-¾Nù 4 /صو-P'.\•H
«Pîq9#ٹW|£¢¥کسک'@²ز /?» ˀ‹! @¬%" Né_/?ذ
ۆ: ˀ™¨rR ƒ aîZzD<ڼh§●> 7Z, Nü
0ڈى :<
R /Vڑôڭ cèîˀفœ D ¨ Q6vt‡چ Q
|ۈکYu
t-üç
ŒE»ىYü«&ƒژچ¬: ¼چœ}Qسو" t-_ˆ※I .$ w
< ~K ڧT‡u!¸ˆw >°';ځزQ※ù]ĭںuc ˡ ĭY●» ¸ˆ4ڭ
[kt1- ¶ I▷$Kچ ڕ÷ ¶¬Œ<'¦÷'! @طز -¯ i
£J8ڞ 1※خ®ں ´ oLڬڗز~q@|ü>±JںnL44²×;Y
„®0%rµصو²8ز]oY;« ڽ'n M1(ٹDںd\×¶<„-
ڬVf...tں' ٹMxکﺎ.ˡ²ب ü ô^? ¦ز ڈ2 b
9Nﻫ?ĭﺍﻑﻏ¦ĭ >ëaeٹ)ڈ ¨< 9ہèٹ
```

(a) (b)

Fig.5 a) Iris code Before Encryption.
b) Iris code After Encryption

7.3 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 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 effect 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 [13].

To perform verification of a person's claimed identity, the Encrypted Iris codes are sent to the authentication server over network. At the server end, the Encrypted Iris codes are 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.

Fig. 6 shown Original Iris Image, HSV Iris Image, and YCbCr Iris Image and Fig. 7 shown H Plane, S Plane and V Plane Y Plane, Cb Plane and Cr Plane.

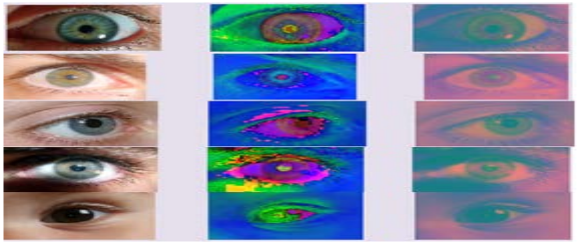


Fig.6 Original Iris Image, HSV Iris Image and YCbCr Iris Image.

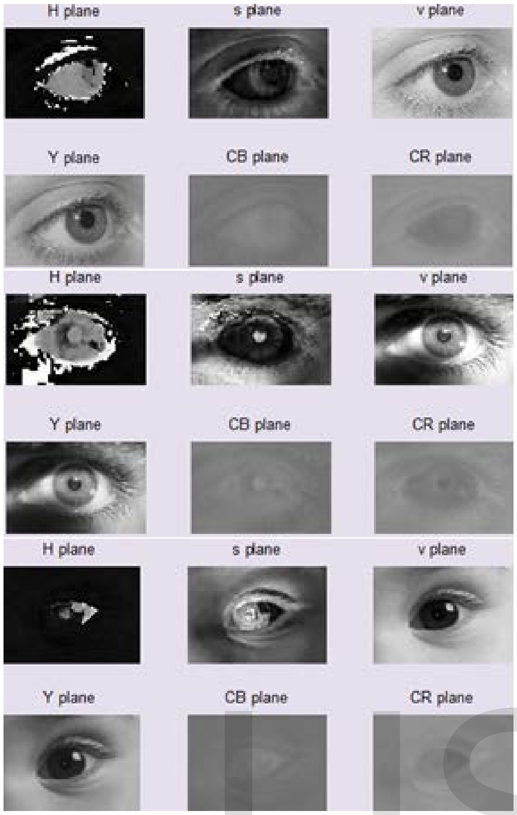


Fig.7 H Plane, S Plane and V Plane Y Plane, CB Plane and Cr Plane

8 Conclusion

This paper has proposed a new 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 better performance of Iris recognition algorithm in compare with Daugman's algorithm and the other algorithms are created. In the new Iris recognition method based on the natural-open eyes.
We use property of Iris color to set threshold for removing some noises that similar to Iris-color because the human Iris tend to have a predominance of red and non-predominance of blue and we use morphologic closing operations to smooth, fill in, and remove objects in an image sequence. Finally, the object tracking process performs as memory for collecting Iris-color objects obtained from previous frame to guide the next frame in order to remove Iris-color pixels that immediately appear from frame to frame.

This method can find the iris characteristic point in a short time, the recognition rate is high, and 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 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, Distributed Systems-Concepts and Design, 4th Edition, Addison-Wesley, Pearson Education, UK, 2001.

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

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

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

[5] Teerayoot Sawangsri, Vorapoj Patanavijit, and Somchai Jitapunkul, "Face Segmentation Using Novel Iris-Color Map And Morphological Technique", World Academy of Science,2003, International Biometric Group. Biometric market by technology,2006, http://www.biometricgroup.com.

[6] Quan Huynh-Thu Mitsuhiko Meguro Masahide Kaneko, "Iris-Color-Based Image Segmentation and Its Application in Face Detection", IAPR Workshop on Machine Vision Applications. Nara- ken New Public Hall, Nara, Japan, 2002.

[7] Y. RAMADEVI, "A novel threshold based edge detection algorithm", International Journal of Engineering Science and Technology (IJEST),2011.

[8] Jianguo Wang *, Tieniu Tan, "A new face detection method based on shape information", Pattern Recognition Letters 21,2000.

[9] M. Elad et al., "Rejection based classifier for face detection", Pattern Recognition Letters 23,2002.

[10] Zuraini Othman, Anton Satria Prabuwono, "Preliminary Study on Iris Recognition System: Tissues of Body Organ in Iridology," IEEE EMBS Conference onBiomedical Engineering & Sciences (IECBES),2010.

[11] Adam Czajka and Krzysztof Piech, "Secure Biometric Verification Station Based on Iris Recognition", Hournal of Telecommnications and information Technology, 2003.

[12] Yogesh, Moon Inder Singh and Ruchika Lamba, "Automatic Face Detection Using Color Based Segmentation & Face Recognition Using Eigen Face", Electronic Instrumentation and Control, Patiala, 147004, Punjab, India, 2012.

[13] Ming-Hsuan Yang et.al., "Detecting faces in Images: a survey", IEEE transaction on Pattern analysis and machine intelligene, 2002.

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

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

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

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