An Adaptive Effectiveness of Iris Recognition to E-Security Based on Wavelet Theory

Dennis Nestory Mwighusa[1], Prof. Pei Zhijun[2]

[1, 2]Tianjin University of Technology and Education, Tianjin, China, P.R

Abstract: **A poor E-Security can result in the corruption of files and can enable criminals and others to access personal and financial information; the loss of trust, confidence and respect exact a far higher financial toll. In this paper the Iris recognition techniques is applied to access control and provide strong e-security. The iris is a portion of the inner eye of an individual and contains an abstract and randomly generated texture pattern arising from orientation of complex tissues within the region. The complexity and randomness of the iris also its genetic properties - no two eyes are the same, the characteristic that is dependent on genetics is the pigmentation of the iris, which determines its color and determines the gross anatomy. Details of development, that are unique to each case, determine the detailed morphology amongst various other factors, ensure that this biometric system is inarguably an exact and reliable method of identification. We shall focus on an efficient methodology of which wavelet transform is the algorithm responsible for image extraction.**

Keywords: **Biometrics, E-Security, Iris Recognition, Wavelet Transform, Hamming Distance**.

1. INTRODUCTION

Today's E-security are in critical need of finding accurate, secure and cost-effective alternatives to passwords and personal identification numbers (PIN) as financial losses increase dramatically year over year from computer-based fraud such as computer hacking and identity theft. Biometric solutions address these fundamental problems, because an individual's biometric data is unique and cannot be transferred.

Biometrics is defined as the science of measuring an individual's physiological or behavioral characteristics for automatic identification. It has capability to distinguish between authorized user and an imposter. An advantage of using biometric authentication is that it cannot be lost or forgotten, as the person has to be physically present during at the point of identification process. Biometrics is inherently more reliable and capable than traditional knowledge based and token based techniques. The commonly used biometric features include speech, fingerprint, face, Iris, voice, DNA, hand geometry, retinal identification, and body odor identification. There are seven basic criteria for biometric security system; uniqueness, universality, permanence, collectability, performance, acceptability and circumvention. As mentioned above, uniqueness is considered as the priority one requirement for biometric data. It will indicate how differently and uniquely the biometric system will be able to recognize each user among groups of users.

2. E-SECURITY

E-security can be described on the one hand as those policies, guidelines, processes, and actions needed to enable electronic transactions to be carried out with a minimum risk of breach, intrusion, or theft. On the other hand, e-security is any tool, technique, or process used to protect a system’s information assets. E-security enhances or adds value to a naked network and is composed of both a “soft” and a “hard” infrastructure.

3. HUMAN IRIS

The iris is the colored part of the eye behind the eyelids, and in front of the lens.

It is the only internal organ of the body, which is normally externally visible. These visible patterns are unique to all individuals and it has been found that the probability of finding two individuals with identical iris patterns is almost zero.

The iris controls the amount of light that reaches the retina. Due to heavy pigmentation, light pass only through the iris via pupil, which contracts and dilates according to the amount of available light. Iris dimensions vary slightly between the individuals. Its shape is conical with the papillary margin located more interiorly than the root. A thickened region called the collarete divides the anterior surface into the ciliary and pupil zones.

The original eye image is shown on fig. 1

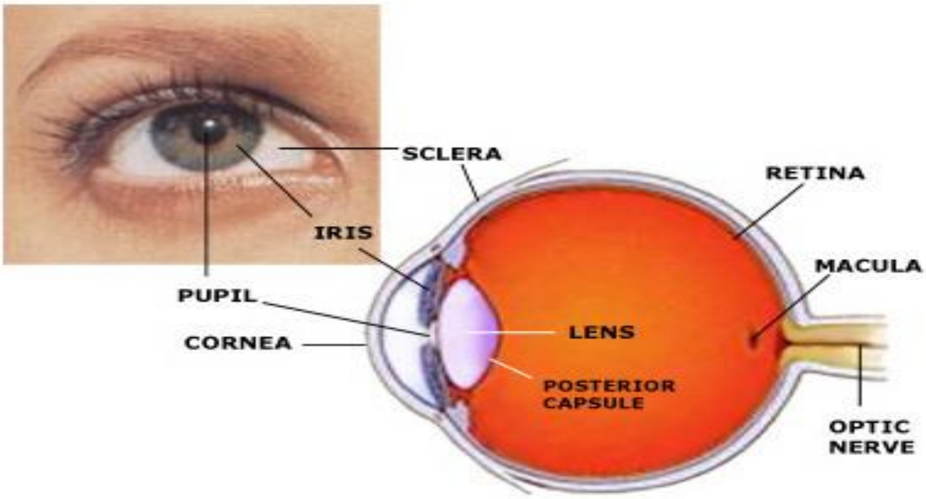


Fig:1. Human Iris

4. IRIS RECOGNITION

Iris recognition is a method of biometric authentication that uses pattern-recognition techniques based on high-resolution images of the irises of an individual's eyes. This operation can be done by means of comparisons between the unknown iris and iris images stored in the database.

The iris pattern is taken by a special gray scale camera in the distance of 10- 40 cm of camera. Once the gray scale image of the eye is obtained then the software tries to locate the iris within the image. If an iris is found then the software creates a net of curves covering the iris. Based on the darkness of the points along the lines the software creates the iris code.

A discrete wavelet transform is used in order to extract the spatial frequency range that contains a good best signal-to-noise ratio considering the focus quality of available cameras. The result is a set of complex numbers that carry local amplitude and phase information for the iris image.

Indicated below is the Iris recognition system.

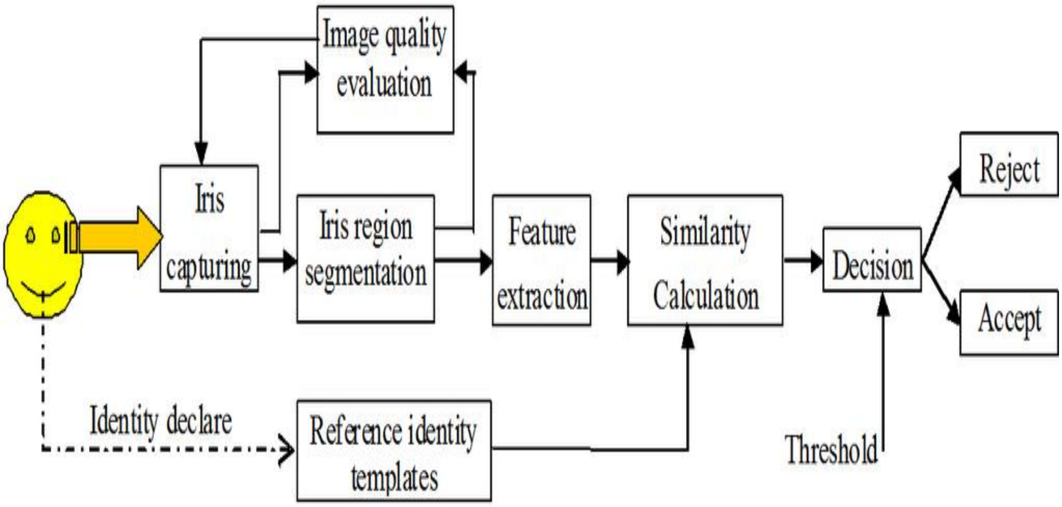


Fig: 2. Iris Recognition System

4.1 IMAGE ACQUISITION:

One of the major challenges of automated iris recognition system is to capture a high quality image of the iris while remaining noninvasive to the human operator. Given that the iris is a relatively small (1 cm in diameter), dark object and that human operators are very sensitive about their eyes, this matter required careful engineering. The following points should be of concern:

- Desirable to acquire images of the iris with sufficient resolution and sharpness to support recognition
- It is important to have good contrast in the interior iris pattern without resorting to a level of illumination that annoys the operator
- The images should be well framed (i.e. centered)
- Noises in the acquired images should be eliminated as much as possible.

The human eye should be 9 cm far away from the camera as shown above. The halogen lamp is in a fixed position to get the same illumination effect over all the images, thus excluding the illuminated part from the Iris while getting the Iris Code is easier, to acquire a more clear images through a CCD camera and minimize the effect of the reflected lights caused by the surrounding illumination, we arrange two halogen lamps as the surrounding lights and the two halogen lamp should be in front of the eye. Fig. 3 shows the device configuration for acquiring human eye images.

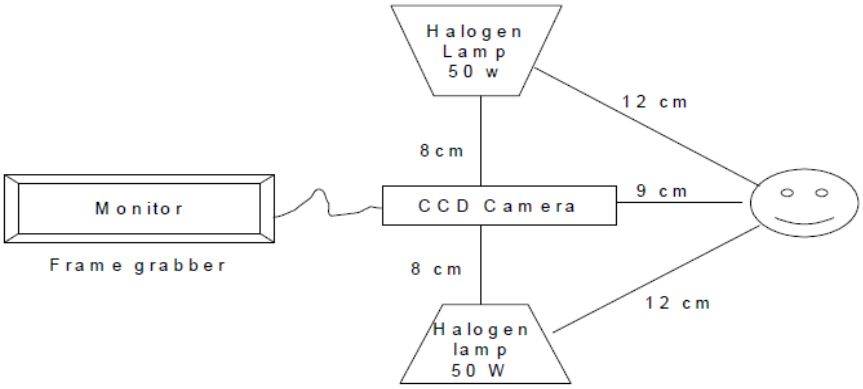


Fig. 3. Configuration of the proposed image acquisition device

4.2 PREPROCESSING:

4.2.1 Algorithm for Detection and Segmentation:

4.2.1.1 Iris Detection:

Irises are detected even when the images have obstructions, visual noise and different levels of illumination. Lighting reflections, eyelids and eyelashes obstructions are eliminated. Images with narrowed eyelids or eyes that are gazing away are also accepted using wavelet algorithm.

Automatic interlacing detection and correction: The correction results in maximum quality of iris features templates from moving iris images.

*Gazing-away eyes****:*** A gazing-away iris image is correctly detected, segmented and transformed as if it were looking directly into the camera.

4.2.1.2 Correct Iris Segmentation*:* is achieved under these conditions:

Perfect circles fail. VeriEye uses active shape models that more precisely model the contours of the eye, as perfect circles do not model iris boundaries.

The centers of the iris inner and outer boundaries are different Fig. 6. The iris inner boundary and its center are marked in red; the iris outer boundary and its center are marked in green.

Iris boundaries are definitely not circles and even not ellipses Fig. 7, and especially in gazing-away iris images.

Iris boundaries seem to be perfect circles **.** The recognition quality can still be improved if boundaries are found more precisely Fig. 8, Compared to perfect circular white contours.

4.2.1.3 Locating Iris:

The first processing step consists in locating the inner and outer boundaries of the iris and second step to normalize iris and third step to enhance the original image as in (see Fig. 4). The Daugman's system, Integro differential operators as in (1) is used to detect the center and diameter of iris and pupil respectively.

$$\max(r, x0, y0) = \left\{ \frac{\partial}{\partial r} \int_0^{2\pi} I(r * \cos\theta + x0, r * \sin\theta + y0) \right\} \quad \_\_(1)$$

Where (x0, y0) denotes the potential center of the searched circular boundary, and r its radius.

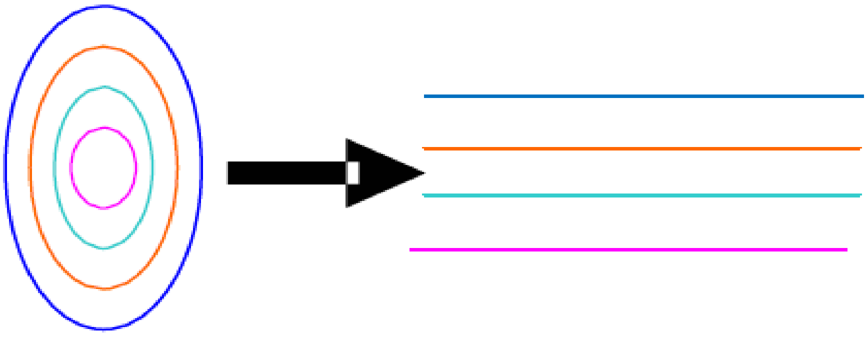


Fig. 4. Polar transformation

4.2.2 Cartesian to polar reference transform:

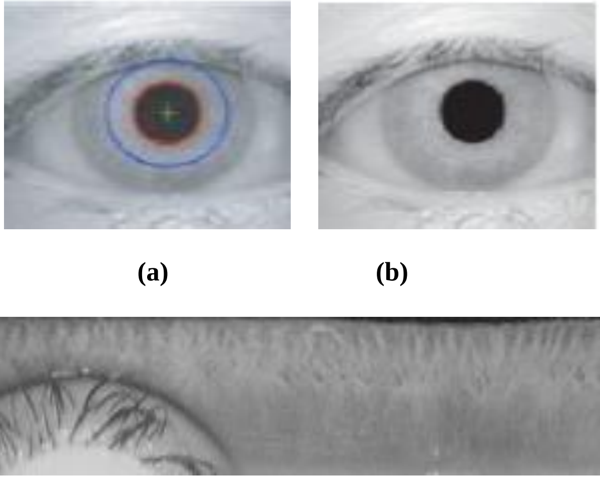
Cartesian to polar reference transform suggested by J. Daugman authorizes equivalent rectangular representation of the zone of interest as in Fig. 4,5 remaps each pixel in the pair of polar co-ordinates(r, θ) where r and θ are on interval [0,1] and [0,π] respectively. The unwrapping in formulated as in (2).

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \quad \_\_\_\_(2)$$

Such that

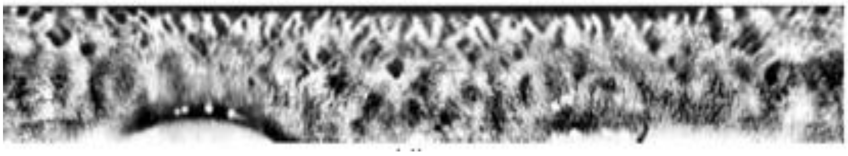
$$\left. \begin{aligned} x(r,\theta) &= (1-r)x_p(\theta) + rx_i(\theta), \\ y(r,\theta) &= (1-r)y_p(\theta) + ry_i(\theta) \end{aligned} \right\} \quad \_\_\_(3)$$

Where $I(x, y)$, (x, y), (r, θ), (xp, yp), (xi, yi) are the iris region, Cartesian coordinates, corresponding polar coordinates, coordinates of the pupil, and iris boundaries along the θ direction, respectively. (See Fig. 4) shows polar transformation.



(a) **(b)**

(c)



(d)

Fig. 5. (a) Original image; (b) localized iris; (c)normalized iris and (d) enhanced iris.

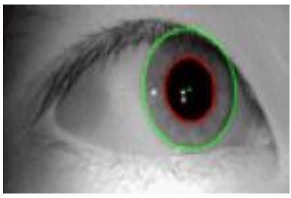


fig. 6

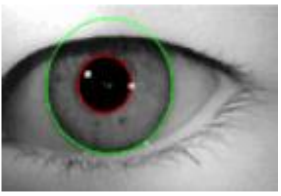


fig. 7

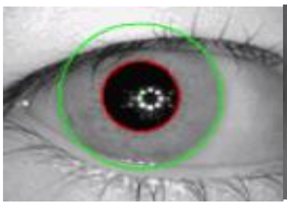


fig. 8

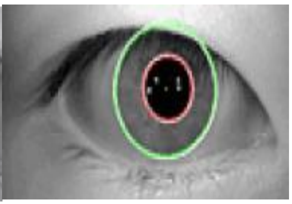


fig. 9

4.3 FEATURE EXTRACTION: **Iris Code:**

This section illustrates the technique of how to get the feature vector (iris code) to able to compare the similarities of the human eyes and to identify the person. Gabor transform and wavelet transform are typically used for analyzing the human iris patterns and extracting feature points from them. In this paper, a **wavelet transform** is used to extract features from iris images. Among the mother wavelets, we use Haar wavelet. The wavelet transform breaks an image down into four sub-sampled, or images. The results consist of one image that has been high pass in the horizontal and vertical directions, one that has been low passed in the vertical and high passed in the horizontal, and one that has been low pass filtered in both directions. This transform is typically implemented in the spatial domain by using 1-D convolution filters *g*.

Fig. 10 shows the result of Harr transform. Where, H and L mean the high pass and low pass filter, respectively. While HH means that the high pass filter is applied to signals of both directions. The results of Haar transform in four types of coefficients: (a) coefficients that result from a convolution with g in both directions (HH) represent diagonal features of the image. (b) coefficients that result from a convolution with g on the columns after a convolution with h on the rows (HL) correspond to horizontal structures. (c) Coefficients from high pass filtering on the rows, followed by low pass filtering of the columns (LH) reflect vertical information. (d) The coefficients from low pass filtering in both directions are further processed in the next step.

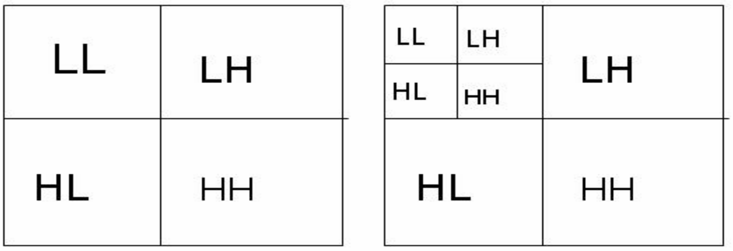


Fig. 10. Harr transform

The following MATLAB code illustrates the Haar decomposition process:

Step-1 Initiations:

function [s,d]= dwthaar(Signal);

```
N = length(Signal); s = zeros(1, N/2); d = s;
```

Step-2 The actual transform:

```
for n=1:N/2
s(n) = 1/2*(Signal(2*n-1) + Signal(2*n));
d(n) = Signal(2*n-1) - s(n);
```

Step-3 Wavelet decomposition using the Haar transform:

```
function T = wavelet-decomp(Signal)
N = size(Signal,2); J = log2(N);
if rem(J,1) error('Signal must be of length 2^N.');
T = zeros(J, N); T(1,:) = Signal;
for j=1:J
Length = 2^(J+1-j);
T(j+1, 1:Length) = dwthaar( T(j, 1:Length) );
T(j+1, Length+1:N) = T(j, Length+1:N);
```

For the 450x60 iris image in polar coordinates, we apply wavelet transform 4- times in order to get the 28x3 sub-images (i.e. 84 features). By combining these 84 features in the HH sub-image of the high-pass filter of the fourth transform (HH4) and each average value for the three remaining high-pass filters areas (HH1,HH2,HH3), the dimension of the resulting feature vector is 87. Each value of 87 dimensions has a real value between -1.0 and 1.0. By quantizing each real value into binary form by convert the positive value into 1 and the negative value into 0. Therefore, we can represent an iris image with only 87 bits.

4.4 PATTERN MATCHING:

4.4.1 Matching process: Hamming Distance Calculation:

Comparison of Iris Code records includes calculation of a Hamming Distance (HD), as a measure of variation between the Iris Coe recorded from the presented iris and each Iris Code recorded in the databases. Let *Aj* and *Bj* be two iris codes to be compared, the Hamming distance function can be calculated as:

$$HD = \frac{1}{87}\sum_{j}^{87} A_j \oplus B_j \quad \_\_\_\_ (4)$$

$\oplus$ denoting exclusive-OR operator. (The exclusive-OR is a Boolean operator that equals one if and only if the two bits *Aj* and *Bj* are different).

4.4.2 Matching Algorithm:

Let *Aj* and *Bj* be two iris codes to be compared and to test if *Aj* in the database or not.

The following steps describe the process:

- For j = 1 to 87 do
- Comparing bit-by-bit code *Aj* with the first code *Bj* in the database.
- If the result of the XOR is (0), this mean the 2 bits are the same, so count the number of zero’s
- Else don’t count it and continue to the next bit
- Next *j* until reaching the final code in the database.
- Calculating the similarities (matching) ration by the following formula:

$$MR = \frac{N_z * 100}{T_n} \qquad \_\_\_\_ (5)$$

Where Nz and Tn are the number of zero's and total number of bits in each code, respectively. MR is a matching ratio.

4.5 IDENTIFICATION AND VERIFICATION:

Identification and verification modes are two main goals of every security system based on the needs of the environment. In the verification stage, the system checks if the user data that was entered is correct or not (e.g., username and password) but in the identification stage, the system tries to discover who the subject is without any input information. Hence, verification is a one-to one search but identification is a one-to-many comparison.

5. CONCLUSION

Considering the financial risk of on-line banking, payment or of the like is important and strongly increases. The user authentication scheme is usable for users as they do not have to remember different passwords. The protocol demonstrates very good performances and good properties considering security and privacy issues. Wavelets iris recognition algorithm is suitable for reliable, fast and secure person identification. It has proven to be a very useful and versatile security measure. It is a quick and accurate way of identifying an individual with no room for human error.

Its use has been successful with little to no exception, and iris recognition will prove to be a widely used security measure in the future. The system find out the recognition rate is about 97.3%. Future perspectives of this study are numerous. We plan to use multiple biometric data in order to increase more security if not at all clearing any possibility to intrude into the system.

REFERENCES

[1] Shimaa M. Elsherief, Mhamoud E. Allam and Mohamed W. Fakhr, Biometric Personal Identification based on Iris Recognition, IEEE, 2006.

[2] John Daugman, - Recognizing persons by their iris patterns - Cambridge University, Cambridge, UK.

[3] John Daugman How Iris works‖ IEEE Transaction on circuit and systems for Video Technology, VOL.14, No.1, January 2004.

[4] Arian Rahimi, Sharhriar Mohammadi and Rozita Rahimi, A New Web-based Architecture Based on Iris Biometrics Technique to

[5] Decrease Credit Cards Frauds over Internet, International Journal of Digital Society (IJDS), Volume 1, Issue 2, June 2010.

[6] Kalyan Chatterjee , Nilotpal Mrinal, Prasannjit. An Efficient Implementation of Iris Recognition and Cryptography in Internet Security System, IJCA Special Issue on "Recent Trends in Pattern Recognition and Image Analysis" RTPRIA 2013.

[7] W.W. Boles and B. Boashash "A Human Identification Technique Using Images off the Iris and Wavelet Transform" IEEE TRANSACTIONS ON SIGNAL PROCESING,VOL. 46, NO.4, APRIL 1998.

[8] .A. Basit, M. Y. Javed, M. A. Anjum "Efficient Iris Recognition Method for Human Identification" World Academy of Science, Engineering and Technology 4 2007.

[9] V K NARENDIRA KUMAR, B.SHRINIVASAN, P.NARENDRAN "Efficient Implementation of Electronic Passport Scheme Using Cryptographic Security Along With Multiple Biometrics" I.J. Information Engineering and Electronic Business, 2012, 1, 18-24.

[10] Jafar M. H. Ali Aboul Ella Hassanien, An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, AMO - Advanced Modeling and Optimization, Volume 5, Number 2, 2003.

[11] Aude Plateaux, Patrick Lacharme, Christophe Rosenberger, Audun J_sang, One-Time Biometrics for Online Banking and Electronic Payment Authentication. International Conference on Availability, Reliability and Security

(ARES), workshop on Security and Cognitive Informatics for Homeland Defense, Sep 2014, Fribourg, Switzerland. pp.179 - 193,

[12] S. Drimer, S. Murdoch, and R. Anderson R. Optimised to fail: Card readers for online banking, Financial Cryptography and Data Security, pages 184–200, 2009.

[13] Vanaja Roselin.E.Chirchi, Dr.L.M.Waghmare, E.R.Chirchi, Iris Biometric Recognition for Person Identification in Security Systems.

[14] Dr. H.B. Kekre, Sudeep D. Thepade, Juhi Jain , Naman Agrawal, IRIS Recognition using Texture Features Extracted from Haarlet Pyramid, International Journal of Computer Applications (0975 – 8887) Volume 11– No.12, December 2010.

[15] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A, and Minkyu Choi, Biometric Authentication, A Review, International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009.

[16] Leila Fallah Araghi, Hamed Shahhosseini, Farbod Setoudeh, IRIS Recognition Using Neural Network, Proceedings of International MultiConference of Engineers and Computer Scientists 2010 Vol I, IMECS 2010, March 17-19 2010, Hong Kong.

[17] 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.

[18] F. Kagan Gürkaynak, Y. Leblebici and D. Mlynek "A Compact High-Speed Hamming Distance Comparator for Pattern Matching Applications" http://turquoise.wpi.edu, 1998.

[19] .A. Julian, "Biometrics: Advanced Identity Verification" The Complete Guide, Springer- Verlag publishers, 2000.

[20] Centre for Biometrics and Security Research page, http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp.