An Efficient Implementation of Iris Recognition and Cryptography in Internet Security System

Kalyan Chatterjee
Computer Science & Engg Dept.
Bengal College of Engineering & Technology
Durgapur

Nilotpal Mrinal
Information Technology Dept.
Bengal College of Engineering & Technology
Durgapur

Prasannjit
Information Technology Dept.
Bengal College of Engineering & Technology
Durgapur

ABSTRACT
Internet is one of the most popular communication channels but it is insecure. Since it is an open and insecure medium, malicious medium can intercept the program or data. In the present scenario, fast growth in online application results in data security problem. In order to get secure internet, users need secure communication method for sending secret messages and data through internet. In this paper, we have developed an efficient way to provide a secure internet using Iris Recognition and Cryptography. The Iris Recognition system consists of an automatic segmentation that is based on Hough Transform. The Hamming Distance is employed for classification of Iris template. Thus this paper can be implemented in any real time application.

General Terms
Iris recognition, Cryptography, Internet Security

Keywords
Biometric authentication,Internet Security, Iris, Cryptography, Segmentation, Hamming Distance.

1. INTRODUCTION
The objective is to implement iris recognition in Internet for security of Data or secrets. Cryptography is used for multiple secrets to hide in one image. Encryption is a well-known method for data security. It transforms secret information into an encrypted form, which looks like a random message. This transformation procedure is called encryption process and the result is called cipher text. A computational device is required

to perform decryption of the cipher text. Therefore, the cost or efficiency of the hardware, complex algorithms and mathematical computations increase to encrypt and decrypt the data. Thus, it can be said that the cost increases and the efficiency reduces. Also, mathematical computations increase to encrypt and decrypt the data. This paper uses the concept of cryptography and biometric authentication. The main objective of this paper is:-

- To provide security in any real time application.
- To provide more than one secret at a time.
- To provide more security by adding Iris Recognition.

2. INTERNET SECURITY
Internet Security is a subset of actions aimed at securing information based on computers and in transit between them. Security of internet has been a major issue from last few years.

3. BIOMETRIC TECHNOLOGY
A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometric systems have been developed based on fingerprints, facial features, voice, hand geometry, handwriting, the retina and the iris. Biometric systems work by first capturing a sample of the feature, such as recording a digital sound signal for voice recognition, or taking a digital color image for face recognition. The sample is then transformed using some sort of mathematical function into a biometric template. The biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be objectively compared with other templates in order to determine identity. Most biometric systems allow two modes of operation. An enrolment mode for adding templates to a database, and an identification mode, where a template is created for an individual and then a match is searched for in the database of pre-enrolled templates. The Best biometric is characterized by use of a feature that is; highly unique – so that the chance of any two people having the same characteristic will be minimal, stable – so that the feature does not change over time, and be easily captured – in order to provide convenience to the user, and prevent misrepresentation of the feature.

3.1 The Human Iris
The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. A front-on view of the iris is shown in Figure 1. The iris is perforated close to its centre by a circular aperture known as the pupil. The function of the iris is to control the amount of light entering through the pupil, and this is done by the sphincter and the dilator muscles, which adjust the size of the pupil. The average diameter of the iris is 12 mm, and the pupil size can vary from 10% to 80% of the iris diameter. The iris consists of a number of layers, the lowest is the epithelium layer, which contains dense pigmentation cells. The stromal layer lies above the epithelium layer, and contains blood vessels, pigment cells and the two iris muscles. The density of stromal pigmentation determines the color of the iris. The externally visible surface of the multi-layered iris contains two zones, which often differ in color. An outer ciliary zone and an inner papillary zone, and these two zones are divided by the collarette – which appears as a zigzag pattern.

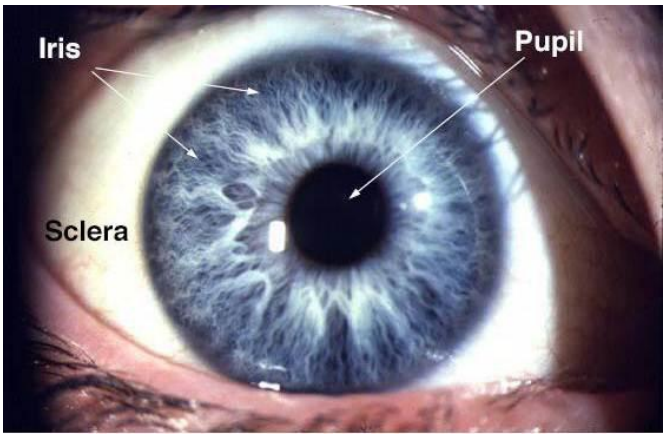

Figure 1: Front view of Human Eye

The iris consists of a number of layers, the lowest is the epithelium layer, which contains dense pigmentation cells. The stromal layer lies above the epithelium layer, and contains blood vessels, pigment cells and the two iris muscles. The density of stromal pigmentation determines the color of the iris.

3.2 Iris Recognition

An iris-recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images. To authenticate via identification or verification, a template created by imaging the iris is compared to a stored value template in a database. If the Hamming Distance is below the decision threshold, a positive identification has effectively been made (HD<=0.32). An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person to be identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye can be brought very close to a lens (like looking into a microscope lens).The originally commercially deployed iris-recognition algorithm, John Daugman's Iris Code, has an unprecedented false match rate.

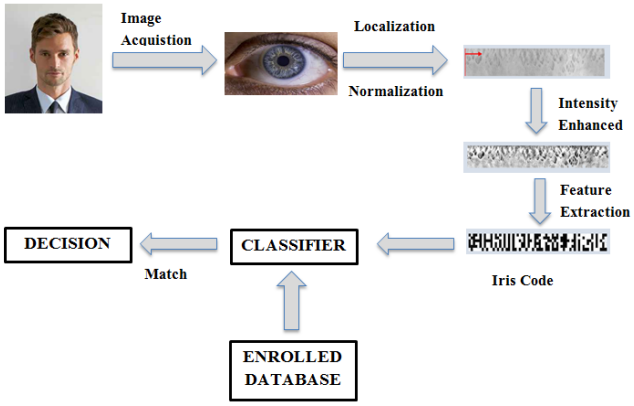

Figure 2: Iris Recognition System.

3.2.1 *Segmentation*

The part of the eye carrying information is only the iris part. It lies between the sclera and the pupil. Hence the next step after acquiring the image is to separate the iris part from the eye image. The image was filtered using Gaussian filter, which blurs the image and reduces effects due to noise. The iris inner and outer boundaries are located by finding the edge image using the canny edge detector, then using the Hough transform to find the circles in the edge image. For every edge pixel, the points on the circles surrounding it at different radius are taken, and their weights are increased if they are edge points too, and these weights are added to the accumulator array.

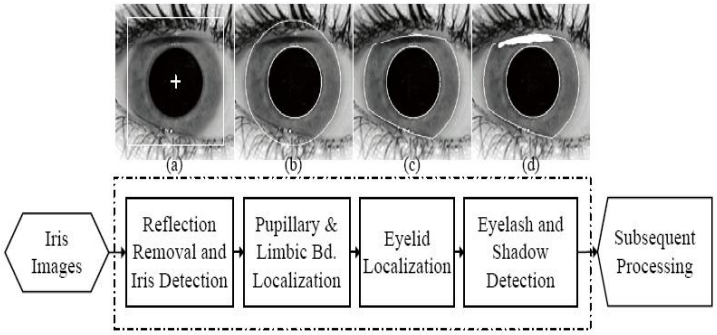

Figure 3: Segmentation Algorithm.

3.2.2 *Normalization*

Once the iris region is segmented, the next stage is to normalize this part, to enable generation of the "iris code" and their comparisons. Since variations in the eye, like optical size of the iris, position of pupil in the iris, and the iris orientation change person to person, it is required to normalize the iris image so that the representation is common to all with similar dimensions. Normalization process involves unwrap the iris and converting it into its polar equivalent.

3.2.3 *Feature Extraction*

The Wavelet transform is used to extract features from the enhanced iris images. Haar wavelet is used as the mother wavelet. The Wavelet transform breaks an image down into four sub-sampled images. The results consist of one image that has been high-pass filtered in the horizontal and vertical directions (*HH* or diagonal coefficients), one that has been low-pass filtered in the vertical and high-pass filtered in the horizontal (*LH* or horizontal coefficients), one that has been low pass filtered in the horizontal and high-pass filtered in the vertical (*HL* or vertical coefficients), and one that has been low-pass filtered in both directions (*LL* or details coefficient). In order to generate the binary data, feature vector is encoded by using two and four level quantization as shown in Fig. 7, which shows the process used for obtaining the feature vectors with the optimized dimension. Here, *H* and *L* refer to the high-pass and the low-pass filter, respectively, and *HH* indicates that the high-pass filter is applied to the signals of both axes.

3.2.4 *Identification*

The last module of an iris recognition system is used for matching two iris templates. Its purpose is to measure how similar or different the templates are and to decide whether they belong to the same individual or not. An appropriate match metric can be based on direct point-wise comparisons between the phase codes [8]. The test of matching is

implemented by the XOR operator that is applied to the encoded feature vector of any two iris patterns. The XOR operator detects disagreement between any corresponding pair of bits. The system quantifies this matter by computing the percentage of mismatched bits between a pair of iris representations, *i.e.*, the normalized Hamming distance. Let *X* and *Y* be two iris templates to be compared and *N* be the total number of bits so, *HD* is equal to the number of disagreed bits divided by *N*.

3.2.4.1 Hamming Distance

The Hamming distance gives a measure of how many bits are the same between two bit patterns. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one.

In comparing the bit patterns *X* and *Y*, the Hamming distance, *HD*, is defined as the sum of disagreeing bits (sum of the exclusive-OR between *X* and *Y*) over *N*, the total number of bits in the bit pattern.

$$\mathrm{HD} = \frac{1}{N}\sum_{j=1}^{N} \mathrm{X_J}(\mathrm{XOR})\mathrm{Y_J}$$

Since an individual iris region contains features with high degrees of freedom, each iris region will produce a bit-pattern which is independent to that produced by another iris, on the other hand, two iris codes produced from the same iris will be highly correlated.

If two bits patterns are completely independent, such as iris templates generated from different irises, the Hamming distance between the two patterns should equal 0.5. This occurs because independence implies the two bit patterns will be totally random, so there is

0.5 chance of setting any bit to 1, and vice versa. Therefore, half of the bits will agree and half will disagree between the two patterns. If two patterns are derived from the same iris, the Hamming distance between them will be close to 0.0, since they are highly correlated and the bits should agree between the two iris codes.

4. CRYPTOGRAPHY

Cryptography is the Study and practice and study of techniques for the secure communication in the presence of adversaries. It is one of the best methods to secure the data.

4.1 Encryption

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text . This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

4.2 Decryption

Decryption is the process of retrieving the original data from The Encrypted data. After the biometric authentication is completed the customer will give his share. The two shares from the application side and the client side would be superimposed and if they match the secret would be

Revealed. This would be done for each level and the embedded secrets at each level will also be revealed.

5. TEST RESULT

It was not possible to use all of the eye images from each database, since perfect segmentation success rates were not attained. Instead a sub-set of each database was selected, which contained only those images that were segmented successfully. The details of each sub-set are outlined in Table 1.

Set name	Superset	Number of Eye images	Possible Intra class comparisons	Possible inter class comparisons.
Cbsr-n	CBSR	75	131	2646

Table 1: Table Represents Eye image sets for testing the system.

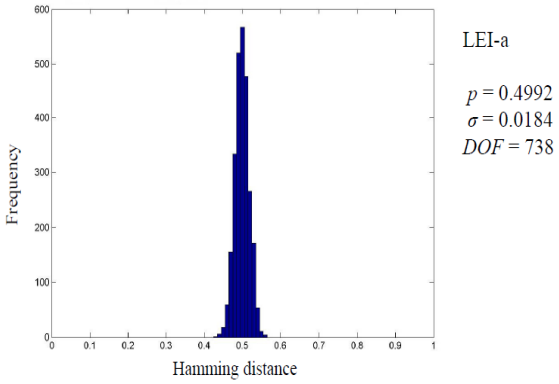

Figure 4: Inter class Hamming Distance with no shifts.

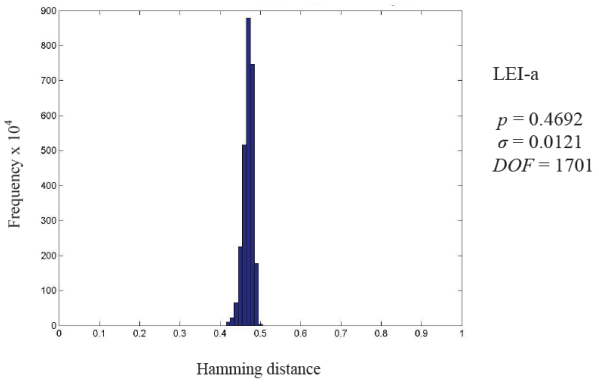

Figure 5: Inter class hamming distance with 10 shifts left and right when comparing templates.

Threshold	FAR (%)	FRR (%)
0.20	0.00	73.04
0.25	0.00	46.08
0.30	0.00	23.28
0.35	0.00	3.88
0.40	0.00	0.00
0.45	2.51	0.00
0.50	92.68	0.00

Table 2: False Accept and False Reject Sets of Datasets

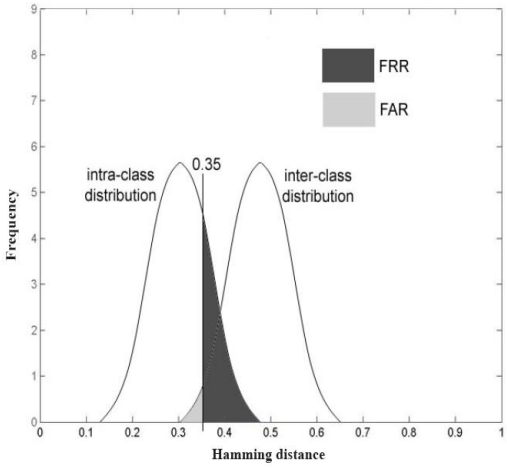

Figure 6: False Accept and False Reject Ratio for two distribution with Hamming Distance of 0.35.

For the data set, perfect recognition is possible by selecting a separation Hamming distance of 0.40, which gives false accept rate and false reject rate both as 0.000% which allows accurate recognition.

6. CONCLUSION

Our existing security systems involve a lot of complexities for authorization of a particular system, which results in greater time consumption. In order to consume less time to show the result of authorization, we have taken iris image of the person.

At last, we came up with the result that perfect recognition is Possible, when we select a separation Hamming distance of 0.40, which gives the false accept rate as well as the false reject rate as 0.000%. Thus, it can be very well concluded that perfect and accurate recognition is possible with the help of the algorithm implied in our paper.

ACKNOWLEDGMENT

We would like to acknowledge "International Journal of Computer Application" society for giving us an opportunity to present our research paper.

7. REFERENCES

[1] 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.

[2] Mohammad Ramli, Nurul Akmar, Kamarudin, Muhammad Saufi and JORET Ariffuddin "**Iris** Recognition for Personal Identification" The International Conference on Electrical Engineering 2008July 6-10, 2008, OKINAWA, JAPAN No. O-099.

[3] Ashish Kumar Dewangan, Majid Ahmed Siddhiqui "Iris Recognition - An Efficient Biometric for Human Identification and Verification" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-3, February 2012.

[4] A.Porusaberi and B.N.Arabbi "Iris Recognition for Partially Occluded Images: Methodology and Sensitivity Analysis" EURASIP Journal on Advances in Signal Processing, Volume 2007, Article ID 36751, doi:10.1155/2007/36751.

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

[6] Makram Nabti, Lahouari Ghouti and Ahmed Bouridane "An effective and fast iris recognition system based on a combined multiscale feature extraction technique" Pattern Recognition 41(2008) 868-879.

[7] W.K.KONG,D.ZHANG "Accurate Iris segmentation based on novel reflection and eyelash detection model" proceeding of 2001 International Symposium on Intelligent multimedia, video and speech processing May 2-4 2001 Hong Kong

[8] C. R. Prashanth, Shashikumar D.R., K. B. Raja, K. R. Venugopal, L. M. Patnaik "High Security Human Recognition System using Iris Images" International journal of Recent Trends In Engineering,Vol. 1,No. 1,May 2009.

[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] Anni U. Gupta, Prof. Dr. Alice N. Cheeran, Mangesh D. Nikose "IMAGE RESTORATION USING WAVELET BASED IMAGE FUSION" International Journal of Engineering Science and Technology (IJEST) ISSN: 0975-5462 vol. 3 no.2 2 Feb 2011.

[11] V.B.Gopala Krishna and ,S. Chandra Sekhar, M.Venkateswarlu "RFID card with iris recognition for high security access environment" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622

[12] P.S.Revenkar , Anisa Anjum , W .Z.Gandhare "Secure Iris Authentication Using Visual Cryptography" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No.3, 2010

[13] Y.V. Subba Rao, Yulia Sukonkina, Chakravarthy Bhagwati, Umesh Kumar Singh , "Fingerprint based

authentication application using visual cryptography methods(Improved ID card)" Tencon 2008,IEEE Region 10th conference 2008

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

[15] J. Daugman, "High confidence recognition of persons by test of statistical independence". IEEE Trans. on PAMI, vol. 15, 1148-1160, 1993.

[16] Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang , "Visual cryptography for general access structure by multi-pixel encoding with variable block size". In Proceedings of the International Symposium on Knowledge Acquisition and Modeling, 340-344, 2008

[17] Xiao-Qing Tan, "Two kinds of ideal contrast visual cryptography schemes". In Proceedings of the International Conference on Signal Processing Systems, 450-453, 2009

[18] Wen-pinn Fang "Non-expansion visual secret sharing in reversible style" International Journal Of Computer Science and Network Security(IJCSNS),9(2),February 2009

[19] Lin Kezheng,Fan Bo, Zhao Hong, "visual cryptographic scheme with high image quality" In proceedings of the International conference on Computational Intelligence and Security, 366-370,IEEE ,2008

[20] Tuyls, P., Akkermans, A. H. M., Kevenaar, T. A. M., Schrijen, G-J Bazen, A. M., and Veldhuis, R. N. J., "Practical biometric authentication with template protection" In Proceedings of the 5th International conference on Audio and video based personal authentication.436-41,2005.

[21] A.K.Jain and U.Uludag "Hiding biometric data" In proceedings of the IEEE, 25(11), Nov. 2004.

[22] Jing Dong, Tieniu Tan, "Effects of watermarking on its recognition performance". 978–1–4244–2287–6, IEEE, 2008.

[23] Shenglin Yang, Ingrid Verbauwhede "Secure iris verification". In Proceedings of the ICASSP, 133-136, 2007

[24] Nick Bartlow, Nathan Kalka, Bojan Cukic, and Arun Ross, "Protecting iris images through asymmetric digital watermarking".1-4244-1300-1, IEEE 2007.

[25] P. Kovesi. MATLAB Functions for Computer Vision and Image Analysis. Available at: http://www.cs.uwa.edu.au/~pk/Research/MatlabFns/index.html.