IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. III (May – Jun. 2015), PP 54-57
www.iosrjournals.org

"Enhancing Iris Scanning Using Visual Cryptography"

Anuja Pawar, Trupti Kumbhare, Pradnya Murkute, Prof. Sneha kallapur
Trupti kumbhare
Sneha Kallapur

Abstract**:** *Biometric technique consists of uniquely identifying person based on their physical characteristic or behavioral characteristic. It is mainly used for authentication. Iris sacnning is one of the most secure techniques among all biometrics because of its uniqueness and stability i.e. no two persons in the world can have same iris. For authentication, the feature template in the database and the user template should be the same. Storing the template in the database securely is not a secure approach, because it can be stolen. To deal with this security issue, in our paper a new method for securely storing the template in the database is proposed.*

Visual Cryptography (VC) concept is used in our proposed system. Using Visual Cryptography concept scanned image is divided into different parts i.e. called as shares; these shares are stored in the database. The proposed Visual Cryptography will generate meaningful shares which overcomes the problem in traditional methods. In our proposed system, we present a powerful approach of iris recognition. It uses an improved circular Hough transform to detect the inner boundary.

Keywords: *Biometric Iris,Visual Cryptography,Hough Transform*

I. Introduction

Now a days, providing security for accessing some secure resources is becoming a crucial process. Technology has introduced a much smarter solution to us which is known as Biometrics. Biometric is a Greek Word Bio means ―Life‖ and metrics means ―Measurement‖. Biometrics deal with automated methods of identifying a person or verifying the identity of person based on physiological or behavioral (signature, gait, etc.) characteristics.

Applications such as ATM ,Bank,International identity card, aviation security, Reseach Lab require identication of people. Recognition systems which use iris biometric are believed to be very accurate, and hence efforts are being put to improve their accuracy and reliability.Iris biometric is the one which can be easily available, less expensive, accurate.It is the most powerful and secure technique when compared to other methods. Iris is a thin circular structure in the human eye. Powerful feature of the iris is used for identification purpose. Iris is a very unique feature.

Identification of a person is done using following steps. Human eye is acquired and the iris preprocessing steps are carried out. preprocessing consists of segmentation, normalization and feature extraction. Iris template is got after iris preprocessing. Then iris template is stored in the database and then the user authentication is verified using the comparison between the iris template.

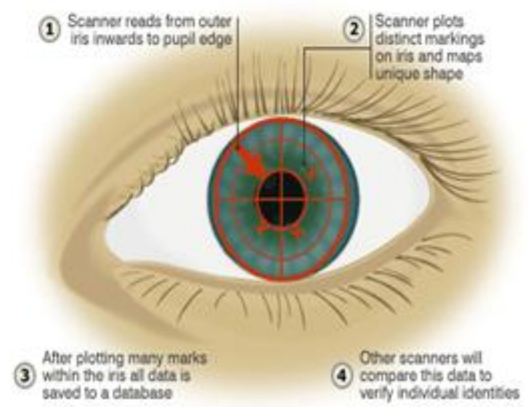
HOW IRIS SCANNERS RECORD IDENTITIES
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

Fig1. Iris scan method

The template is stored in database, hence security of stored templates get affected, the attacker can easily get unauthorized access. The hacked templates can be misused. e.g. Bank transactions. Hence, fool-proof methodologies are essential to securely store the templates.

In this paper a system is proposed by visual cryptography technique to protect the iris template to make it secure from attack in system database as well as dual layer of authentication to the users.

The proposed model is a literature survey on "Enhancing Iris Recognition" based on Visual Cryptography".

II. Motivation And Related Work

Security of data is very important issue because many a times security lacks in encryption and decryption that way we use a powerful technique of Visual cryptography and provide a biometric authentication. Biometric is a method of identifying the identity of person based on physiological or behavioral characteristics. Many biometric technique are available such as Facial , iris, hand, palm print, voice and signature among those iris recognition is one of the most powerful and unique.

Applications such as Bank and ATM require efficient security. Biometric identification methods that identify individual person are based on physiological and behavioral characteristics. Currently, fingerprint, face and iris are the most widely used recognition systems. Recognition systems which use iris biometric are believed to be very accurate, and hence efforts are being put to improve their accuracy and reliability.

Iris recognition is define in three steps they are iris segmentation, normalization, feature extraction Segmentation is done in order to detect the inner and the outer boundaries of the iris that forms a circle. It is used for finding the center and the diameter of the iris. Normalization is done for mapping the iris from polar to Cartesian coordinates. It converts the iris ring into rectangular form. It will make all the iris patters to same size. For extracting the specific features from the iris, feature extraction method is used.The motivational theme behind this proposed literature survey is to built meaningful shares which overcome the problem of security crucial. The key source of inspiration is an opportunity to know which researches has been done on visual cryptography.

III. Literature Review

Authentication can be implemented in different ways, such as password based authentication, device based authentication and biometric authentication .Password based authentication is one of the best ways to provide security but it can be hacked easily. Device based authentication includes the methods for providing the security by means of hardware token,software tokens ,smart card and USB tokens but these methods are very expensive. Biometric authentication provide different types for recognizing human based on their physical and behavioral characteristics.Biometrics makes use of physical characteristics such as Iris, Finger Print, , Palm Prints, Retinal, Ear, Hand Geometry, DNA, and Face where as behavioral characteristics such as Handwriting, Signature, Gait, Body Odor, and Thermal Emission of Human Body. Iris authentication is one of the most powerful and secure technique. Iris is one of the most unique features in the human body and it can be used for rmost secured identification purpose.

Biometric templates should not be stored securely in plain text form different methods are needed to securely stored the templates in database. Biometric data and templates can be protected using cryptography, stenography and watermarking. In this paper, the proposed method visual cryptography is used for securely storing templates in database system. Visual cryptography concept is used for generating the meaningful shares so that quality of image will not be reduced.

IV. System Architecture

Visual Cryptography technique is used for protecting the iris template from attackers and to avoid an unauthorized access

The proposed system consist of two modules Enrollment module and Authentication module. Enrollment module is classified into two sub modules : SNF module and VC module. An authorized person will have to pass through these phases as explained below.

3.1 Enrollment : During enrollment phase, all biometric information from an authorized person is captured.

3.1.1 SNF Module: The system administrator will collect the eye image of person for authentication purpose. This image will be passed to the SNF module which consists of three steps : Segmentation, Normalization and Feature extraction. The extracted iris image is created and stored in the database and it is named as any system generated random number. Then, png image of this number will be sent to the VC module.

In Segmentation, main objective is to extract the iris template from the eye image. The Hough Transform algorithm is used in this step.

In Normalization, the iris region is transformed to the fixed dimensions in order to allow comparisons.

In Feature extraction, accurate recognition of individuals is obtained.The most essential information of an iris must be extracted. Only the desired features of the iris must be encoded so that templates can be compared.

3.1.2 VC Module: Using Random number generator algorithm the extracted iris template is stored in database. This number is given as input to the VC module and then two shares are generated. out of which one share is stored in the database and the other is kept with employee.

3.2 Authntication phase: In this phase, eye image of the user will passed through the SNF process. Then this extracted image and iris template will be compared. If both the templates match then that the user is a registered employee.

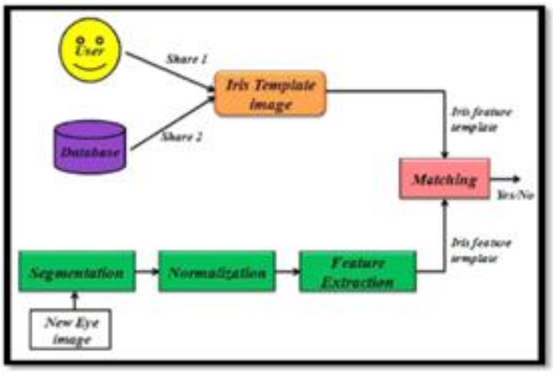

Fig2. Future Request System Architecture

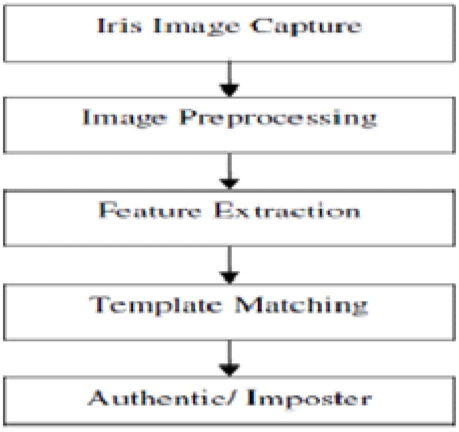

Fig3. Stages of iris recognition

V. Future Scope

The proposed method will work for monochrome images. The future work is to be on the colored eye image.The shared should be generated using color visual cryptography.

VI. Conclusion

There are various techniques adopted by researchers to secure raw biometric template but in this paper a new approach for authenticating the person by securely the iris template by generating the shares. The visual cryptography proposed in this paper will generates the meaningful shares which reduces the problem of existing method. In existing method, meaningless shares generates the poor quality compared to original image. The new method invented in this paper will be more secure and efficient .Hence iris system will be more secured and reliable in security critical applications.

References

[1]. PDont Blink:Iris Recognition for Biometric Identication", SANS Institute InfoSec Reading Room

[2]. L.Masek, P Kovesi, "Recognition of human iris patterns for biometric identification". Tech. Rep., The School of Computer Science and Software Engineering, The University of Western Australia.

[3]. Libor Masek ,"Recognition of Human Iris Patterns for Biometric Identication", The University of Western Australia, 2003.

[4]. Moni Nair and Adi Shamir, "Visual cryptography" .In Proceedings of the advances in cryptology- Eurocrypt, 1- 12,1995.

[5]. S. Lim K. Lee O. Byeon and T. Kim, "Ecient Iris Recognition through Improvement of Feature Vector and Classier." ETRI J., vol. 23, no. 2,pp. 61-70, 200l

[6]. "Biometric Template Protection With Robust Semi Blind Watermarking Using Image Intrinsic Local Property", International Journal of Biometrics and Bio-informatics (I1BB), Volume (5) : Issue (2) : 2011

[7]. Chander Kant, Ranjender Nath & Sheetal Chaudhary,"Biometrics Security using Steganography", International Journal of Security, Volume (2) : Issue (1).

[8]. Zhifang Wang, Qi Han and Xiamu Niu, Christoph

[9]. Busch," A Novel Template Protection Algorithm For Iris Recognition", Eighth International Conference on Intelligent Systems Design and Applications.

[10]. "Iris matching using multi-dimensional artificial neural network" R.M. Faroukl R. Kumar2 K.A. Riad, The Institution of Engineering and Technology 2011, lET Com put. Vis., 2011, Vol. 5, Iss. 3, pp. 178-184

[11]. Wen-Pinn Fang "Non-expansion visual secret sharing in reversible style". I1CSNS International Journal of Computer Science and Network Security, 9(2), February 2009. ISBN: 978-