International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.2., 2016
(Mar-Apr)

RESEARCH ARTICLE

ISSN: 2321-7758

ENHANCING SECURITY AND PRIVACY IN IRIS AUTHENTICATION SYSTEM

TUMTO BAGRA, AMIT SINGH RAJPUT, SUYAKANT MANE' SHANTANU UNDE,

Prof. MRS NEHA HAJARE

Computer Engineering, Savitribai Phule Pune University
MIT-AOE, Alandi(D), Pune, India

ABSTRACT

Biometrics refers to physiological and behavioural characteristics. Biometric features include fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent etc. Biometric authentication systems are being used to verify identity and grant access control to an individual. Of all the biometrics being used Iris yields very high performance and also provides considerably highly uniqueness so we have opted Iris. Visual Cryptography is the technique of secretly encrypting image so that the image can only be decrypted by the intended individual. Using this concept of visual cryptography the image is split into numbers of smaller images called as shares. These shares are safely stored in the database. This Visual Cryptography overcomes the problem of security and privacy.

Keywords: Biometric, Authentication, Security, visual cryptography.

I. INTRODUCTION

With the use of advancement in information technology, security issue of crucial data and information are ever growing.. Biometrics deal with verifying the authenticity of a person or verifying the identity of person based on physiological or behavioural characteristics. As biometric traits are distinctive and it neither can be forgotten nor has the chance of getting lost biometric Technology can provide a smart solution to this issue. One major drawback of biometric is that if it is once compromised it is compromised forever and cannot be replaced.

The human iris has a plenty of distinguishable features like collageneous fibre, colour, coronas, contraction furrows, freckles, rifts, and pits etc which differ highly from eye to eye. The pattern of these features and their spatial relationship to each other provides a means of parameter used in identification process. Possible method of attack like Spoofing can be ruled out in case of iris patterns in comparison with other biometrics as it is highly difficult. One important advantage of iris is that ageing has no effect on theiris pattern. An iris remains the same since the early age of an individual till the death. Moreover, wearing glasses and contact lenses have no considerable effect on the iris and hence, it remains constant during the lifetime of an individual. Image of an iris is shown in fig 1

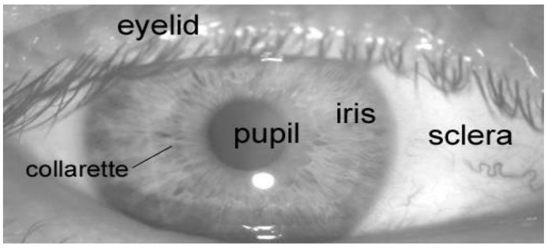

Fig1.Iris image

II. LITERATURE REVIEW

There are several ways that can be used in authentication systems. These includes traditional password based authentication, hardware or software device based authentication and biometric based authentication. Traditional password based authentication is the oldest and the most used authentication system .However, the security level it provide is of low quality and it can be easily hacked. Device based authentication system employs the used of hardware token, software token, smart card and USB tokens. The drawback of these systems is they are very expensive. Biometrics authentication is based on identifying a human on the basis of his/her physical and behavioural characteristics. Biometric physical characteristics are Iris, Finger print, Palm prints ,Retina ,Hand geometry ,DNA ,Face and many more while behavioural characteristics include Handwriting , Signature ,Gait ,Body odour etc. Iris authentication system is considered as one of the most powerful and secures technique that is being used these days. Biometric feature in human are unique in every individual and hence iris is unique. Its use in authentication system provides secured identification process. Considering few but important aspects of biometric features comparisons among nine biometric is listed in Table 1.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance
Face	High	Low	Medium	High	Low
Fingerprint	Medium	High	High	Medium	High
Iris	High	High	High	Medium	High
Signature	Low	Low	Low	High	Low
Voice	Medium	Low	Low	Medium	Low

Table1.Comparisons of biometrics

III. PROPOSED SYSTEM

In this Biometric based authentication system first, the eye is scanned to obtain the digitised image of the eye, and then by employing Image processing techniques the unique iris pattern is extracted. The steps involved in the processing is shown in figure2

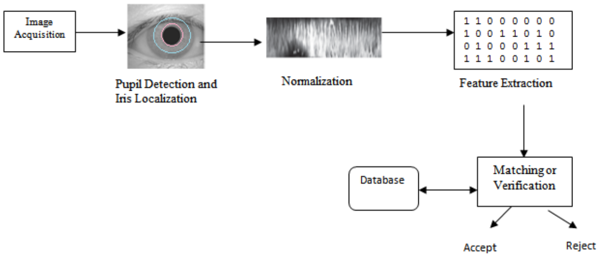

Fig2.Authentication process

A. *Localisation*

The inner boundary and outer boundary of iris is determined in these steps which are usually circles and may not be con-centric. The basic objective of this process is to isolate the actual iris region. Circular Hough Transform is used for detecting the iris and pupil boundaries and linear Hough Transform is used to isolate eyelids

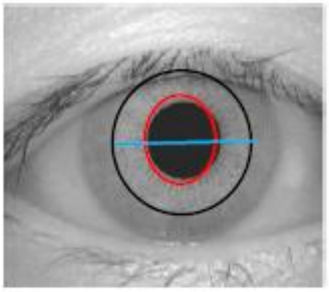

Fig3.Localised Iris

B. *Normalisation*

After the iris region is successfully isolated from a digitised image of the eye, normalisation is the subsequent step. In normalisation the iris region is mapped to rectangular block so that it has fixed dimensions in order to allow comparisons. The normalisation process produces iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location.

Fig4.Normalised Iris

A. *Image Enhancement*

Due to the low contrast and non-uniform illumination nature of the image, it is required to be enhanced because it may impair the result of texture analysis.

Fig5.Enhanced Iris

IV. CONCLUSIONS

There are numerous techniques that could be employed to secure the biometric templates. This paper use visual cryptography to secure the template in the database where the iris image is stored. This technique is robust and reliable that enables good matching accuracy. However, there is scope for improvement in effectiveness in terms of computational cost time. Encryption does not include any NP-Hard problem dependency. Thus, this project is NP-complete. This paper propose a visual cryptography which will generate meaning full share and thus reduce the earlier method of meaningless share generation which results in poor quality image. Hence, this system provides greater level of security and thus, privacy in authentication system.

REFERENCES

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

[2] Arun Ross, "IRIS RECOGNITION: THE PATH FORWARD". Published by the IEEE Computer Society, February2010, 0018-9162/10.pp 30-35

[3] Bharanivendhan N and Amitha T, "Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm". *International Journal of Computer Applications (0975 – 8887) Volume 92 – No.8, April 2014*

[4] Vanaja Roselin.E.C and Dr.L.M.Waghmare, "Pupil detection and feature extraction algorithm for Iris recognition". *AMO-Advanced Modeling and Optimization, Volume 15, Number 2, 2013*

[5] BojanCukic, and Arun Ross, "Protecting iris images through asymmetric digital watermarking". 1-4244-1300-1, IEEE, 2007

[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] BRIAN A.WANDELL, ABBAS EL GAMAL, BERND GIROD, "Common Principles of Image Acquisition Systems and Biological Vision'',Proceedings of IEEE VOL. 90, No. 1, January 2002