International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 6 (July 2014) http://ijirae.com

Iris Encryption using (2, 2) Visual cryptography & Average Orientation Circularity Algorithm

Priti.P.Dafale
PG Scholar-Tech
Dept. of Computer Science & Engineering
B.D. College of Engineering Wardha

Prof.P.V.Chavan
Asst.Prof (Sr.Gr)
Dept. of Computer Engineering
B.D. College of Engineering Wardha,

Abstract: Biometric authentication scheme used for person identification. Biometric authentication scheme consists of uniqueness for identifying human using physiological and behavioral characteristics. So this technique is used for criminal identification and this technique is used in civil service areas. In order to provide security to the data (2, 2) secret sharing scheme. Basically iris recognition is the most secured scheme. Visual cryptography is the techniques that divide the secret into shares.

Keywords: Secret sharing, Visual cryptography, Iris, Biometrics, Image processing.

I.INTRODUCTION

In the internet era, it is a trend that data has been transmitted, published and shared on the internet. Through internet lot of user problems solved in spite of that internet is the convenient platform there still problems may exist. Hackers may misuse the internet to commit the computer crime, resulting secret data may be forged, and stolen etc.The best way to provide security security to data is to encrypt the secret information before sharing them. Authentication is of different types such as physiological, behavioural and biometric authentication. The basic idea behind visual cryptography is to divide the secret into two shares. To decrypt the secret, shares are super imposed (logical X-OR operation is performed).There are different types of visual cryptography schemes such as (2,2),(K,N) & (N,N)etc.Basic scheme (2,2) is also called secret sharing scheme. To reveal secret all shares are to be gathered[11].

Biometric authentication consists of some characteristics such as

- Universality means that every person using a system should possess the quality, characteristics.
- Uniqueness means the trait should be sufficiently different for individuals such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait.
- Acceptability relates to individuals in the relevant population accept the how the manner in which a trait varies over time.[10]

As biometric authentication include iris recognition, facial recognition. hand recognition, gait recognition, fingerprint recognition etc. The performance of perfect biometric scheme includes uniqueness, universality, permanence, user friendliness.

1.1IRIS

Iris is the thin circular structure of human eye. While comparing each and every authentication scheme it is found that iris is unique.Texture of iris start at the third months of born baby and this structure is unique throughout the life of that person.The most important feature of iris that it is used for identification purpose.

1.2 FINGERPRINT

Fingerprint are graphical flow like ridges present on the human fingers.Its formations depend on the initial conditions of the embryonic mesoderm from which they develop. Lot of research has been done later it is used for criminal identification purpose.Nowadays this system are used in multiple civil areas.

1.3 HAND GEOMETRY

Hand geometry based biometric system has proven to be the most suitable and acceptable biometric trait for medium and low security application. Geometric measurements of the human hand have been used for identity authentication in commercial system [17].

1.4. FACIAL EXPRESSION

Emotion is a state of feeling like thoughts, psychological changes and expressions. Emotions positively affect intelligent functions such as decision making, perception and empathic understanding. The approach on Facial Action Coding System (FACS) which separates the expression into upper and lower face action[18]

II. SHARE GENERATION SCHEME

The theoretical foundation of key generation rule are stated below.
Input: original image I of size 512 X 512 pixels
output: shares S 1 and S2.
for(i=0;i<512;i++)
for(j=0;j<512;j++)
Random assign s1[i][j] as white or black
If I[i][j] is white then
S2[i][j]=S1[i][j]
else
S2[i][j]=complement of S1[i][j];
else
End if
End for

By using traditional methods original secret image can be reveal by using OR operation which has low contrast and quality.Inorder to improve the we will replace this methods by using binary XOR operation .By using XOR operation it will give original image without noise.

III. LITERATURE SURVEY

Desmedt,Y.Hou,S.Quisquata in 1998 proposed(2,n) audio secret sharing scheme. In this scheme shares are the audio files but the secret is the bit string which is constructed without any computation. The ASSS is a secret sharing scheme in which shares & or the secret are audio files. It is mainly used in audio application. This scheme achieve shares in random[1] Yong Zhu,Tieniu Tan and Yunhong Wang in 2000 proposed a new system based on personal identification based on iris patterns[2]. Thien and Lin in 2002 proposed (k,n) threshold secret sharing scheme using shamir secret sharing scheme to generate the image shares[3]. Milos Stojmenovic,Amiya Nayak in 2007 proposed the circularity measures.There are two ways of determining the center of shape.The algo work on open and closed algo.The measures were compared with human measurements of circularity of the same set[4]. A. Ektesabi,A. Kapoor in 2011 proposed techniques to determine the exact iris,pupil boundaries with high speed processing without losing the accuracy. The software filters is applied to reduce the disturbance .To improve the computational time , it is more accurate,simpler and faster with shorter detection[5]. Pallavi V Chavan, Dr. Mohammad Atique, and Dr. Anjali R Mahajan proposed the concept of an intelligent hierarchical visual cryptography. Visual cryptography is the art of encryption such that decryption can be perform by mathematical operation. The secret image consists of collection of black and white pixels. The major disadvantages of this scheme is that visually blind people cannot used this scheme[6].

Young-Chang Hou and Zen-Yu Quan proposed the techniques of progressive visual cryptography with unexpanded shares.The contrast of this scheme is better than conventional VC.The share size is same as that of secret.PVSS differs from the conventional VSS in the way that when more than one share is stacked together,the hidden information will appear little by little.The current researches on PVSS are based on pixel expansion which resulted in the waste of the transmission time and storage space[7]. R.M. Farouk, R. Kumar, K.A. Riad in 2011 proposed this method is found to give results that are with the other pattern recognition techniques.It is capable of excellent pattern recognition.The conventional matching techniques with regard to time and effectiveness of results[8]. A visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into *n* shares distributed to *n* participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS[9]. R.Sinduja,R.D.Sathiya and Dr.V.Vaithiyanatham in 2012 proposed the feature template databases and the user template should be same. For authentication, storing authentication, storing the template in the database. Main issue with generating the shares is the degradation on the image quality found[10]. Ferhat-taleb Alim,K .Messaoudi, S.Seddiki and O.Kerdjiji in 2012 proposed FPGA an architecture method used to detect circles from edge images based on Hough transform algorithm. Hough transform is the broad application ,it robust techniques for finding curves that increases the complexity of hardware parameter. Hough transform algo. is applied on binary images ,first we have to convert binary images into color images[11]. Leandro Schwarz,Fabio Cabral Pacheco in 2012 proposed to describe a computer system to detect and measure the pupil and iris size. Open CV is defined as open computer vision library. The system was written in real time video processing. The frames are captured in gray scale images and proceed using normalization and threshold techniques. The pupillometry is the measurement in the dilation of pupils. Increase in the amount of light enters in eye,the activity of sphincter muscle of the iris is inhibit and the activity of dilator muscle is stimulated,causing the pupils dilate. Due to the arrangement of camera and the mask used to support the face the image

filtering operation is not to be performed. In this it is possible to select an area of image that contains eye and perform operation to save processing time and memory. The library is written in C/C++ language,but also supports java, Python and visual basics .It is used to perform the main filtering,feature extraction such as Active Contour and Hough transformation[13]. T.Kathikeyan ,B.Sabarigiri in 2012 proposed IRIS and EEG. Used multi-modality human identification system. Multi-modality human identification makes it difficult to achieve spoofing in biometric sensors [15]. Milos Stojmenovic, Aleksander Jevremovic, Amiya Nayak in 2013 proposed shape based circularity.The algorithmn isolates the pupil boundary byextracting image edges,then find the largest contiguous set of points.If human irises are sometimes not perfect circles ,nor do the iris and pupil necessarily form concentric circle[16]. Hui Zhang, Xiangfeng Guan in 2012 proposed new iris recognition system to improve accuracy and to reduce the recognition time. Most of the human eyes iris boundary is not round by shape,it may certainly cause pupil legacy,reducing iris identification. As for the operation time compared with neural network,combination of KNN algo. Ensure the accuracy,average,reduce the operation time more than 20 times. It can improved the running speed of recognition [17].

1V.IMPLEMENTED WORK

By using (2,2) secret sharing scheme we will generate shares and reveal the secret and also used the average orientation circularity algorithm.Circulariy value is in the range of 0 and 1.If the circularity value is 1 then shapr is circle Otherwise shape is line. To select the center of the shape is the important factor while measuring the circularity.Center of gravity of shape corresponds to per-coordinate average value of each pixel in the shape.The cartesian pixel array was transformed into the array of polar co-ordinates pixels.Points are transformed from polar coordinate to cartesian coordinates. The points (x,y) in the cartesian form ($\sqrt{x^2+y^2}$,arctan(y/x)).

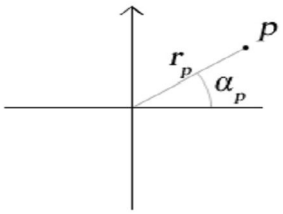

Fig2.Polar co-ordinate representation

There are two phases of IRIS detection algorithm such as

- Registration phase
- Authentication phase

In Registration phase: In the Registration phase administrative has to collect all the user iris image. We processed the iris image apply edge detection & generate meaningful shares of all the iris image stored in the database. There are two shares first shares stored in the database called as database share & second share are stored in the user shares.

In the Authentication phase :

When the user share match with the database share by using unique identification id then it is authenticated one. Otherwise it is not a authenticated one. At the same time it will open the person person with its information. Graph is also calculated.Time complexity for generating shares and to reveal the secret is also calculated. We will also count the total number of black and white pixels

COMPARATIVE STUDY

PARAMETERS	NO. OF SHARE	PIXEL EXPANSION	TYPE OF SECRET	CONTRAST	TYPE OF IMAGES
Halftone cryptography color images	N	No	Random	Better	Color images
(K,N) for color images Extended VCS	N	No	Meaningful shares	Poor	Color images
(K,N) Visual cryptography scheme	K	No	Random	Better	Gray images
Progressive Visual cryptography	2	No	Random	50%	Gray Images
(2,n)Visual Threshold scheme	N	Minimal Expansion	Random	optimality	Gray images
(2,2)Secret sharing scheme	2	Yes	Random	Better	Gray Images

V.CONCLUSION

Iris is more secure, reliable .To provide security to iris we used (2,2) secret sharing scheme .It is used for authentication purpose. So,it come into conclude that conventional ID are one that we carry but biometric system are those that we are!.In future we will try to work on realtime images.

VI.REFERENCES

[1] Desmedt, Y.Hou, S.Quisquater, J,,"Audio and optical cryptography",*in Advances in Cryptology-Asia crypt'98,Springer-Verlag LNCS* vol.1514, pp,392-404,1998.
[2] Yong Zhu,Tieniu Tan and Yunhong Wang,"Biometric Personal identification based on iris patterns",IEEE pp,801-804,2000.
[3] C.C.Thien and J.C.Lin,"Secret image sharing",*Computers & Graphics*, vol.26, no.5,pp.765-770,2002.
[4] "Shape based circularity measures of planar point set "Milos Stojmenovic, Amiya Nayak in IEEE 2007 page no-1279-1282.
[5] A. Ektesabi, A. Kapoor," Exact pupil and iris boundary detection", *IInd International conference on control, Instrumentation and Automation* ,IEEE,PP.1217-1221,2011.
[6] P.V.Chavan, Dr. M.Atique, Dr.A.R.Mahajan," An intelligent System for secured Authentication using Hierarchical Visual cryptography-review", *ACEEE International Journal on Network Security*, Vol 02,No.04,Oct 2011.
[7] "Young-Chang Hou and Zen-Yu Quan",Progressive visual cryptography with unexpanded shares,*IEEE Transactions on circuits and system for video technology* ,Vol 21,Nov 2011.
[8] R.M. Farouk, R. Kumar, K.A. Riad ,"Iris matching using multi-dimensional artificial neural network" , *The Institution of Engineering and Technology 2011, lET Comput*. Vis., 2011, Vol. 5, Iss. 3, pp. 178-1.
[9] Feng Liu,Chauanku Wu,"Embedded Extended VC scheme",Volume:6,2011,IEEE
[10] Dr.V.Vaithiyanathan,R.Sinduja,R.D.Sathiya "Sheltered Iris Attestation by means of Visual Cryptography (SIA-VC)", *IEEE International conference on advances in Engineering Science and Management* 2012.page no.650-655.
[11] "Modified Circular Hough Transform using FPGA" F. Ferhat-taleb Alim, K. Messaoudi, S. Seddiki an O.Kerdjidj,*International conference on Microelectronics*, IEEE, 2012.
[12] "Pupil & iris detection in dynamic pupillometry using OpenCV Library","Leandro Schwarz,Fabio Cabral Pachew,Miguel Autonio Sovierzoski",CISP,IEEE,PP,211-215,2012
[13] "Halftone VC with color share",*Granular Computing IEEE 2012,International Conference,Liu,Yuangfeng,Wang,Zhongmi*
[14] T. Kathikeyan, B.Sabagiri", Countermeasures against IRIS Spoofing and Liveness Detection using Electroencephalogram", IEEE ,2012.
[15] Hui Zhang,Xiangfeng Guan,"Iris Recognition Based on Grouping KNN and Rrectangle conversion ",IEEE 2012.
[16] Milos Stojmenovic, Aleksander Jevremovic, Amiya Nayak,"Fast iris detection via shape based circularity",*8th Conference on Industrial Electronics & Applications*, pp.747-753,IEEE,2013
[17] Poonam Rathi, Dr. Sipi Dubey, ", *(IJARCET) Volume 2, Issue 6, June 2013*, "Hand Geometry Recognition System Using Feature Extraction"
[18] G.Hemalatha1, C.P. Sumathi, (IJCSES) Vol.5, April 2014,"A Study of Techniques for Facial Detection and Expression Classification"

