Secure of Face Authentication using Visual Cryptography

Atul Sureshpant Akotkar, Chaitali Choudhary

Abstract: Visual Cryptography is a process of creating shares from an Image so that it would becomes unreadable for intruder or unauthenticated person. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret image. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image.This paper implements visual cryptography for color images in a biometric application. The project modules have a strong authentication and robustness scheme. In this project, face authentication scheme helps in achieving robustness by locating an image face from n input image.

Keywords: Face Detection, Color Recovery, Visual Cryptography, Image Authentication, Pixel by Pixel Matching.

I. INTRODUCTION

Biometrics is the technology that uses physiological or behavioral characteristics to authenticate identity of persons. For automated personal identification biometric authentication is getting more attention. There are various application where personal identification is required such as computer login control, secure electronic banking, premises access control, border crossing, airport, mobile phones etc. many biometric techniques are available such as fingerprint, face, iris, retina, palm print, ear, hand vein, facial thermogram, gait, keystroke, odor, voice, hand geometry and signature. Among those face recognition is one of the most promising approach because of stability, uniqueness and noninvasiveness. **Suppose** 4 intelligent thieves have deposited their loot in a Swiss bank account 1. These thieves obviously do not trust each other. In particular, they do not want a single member of themselves to withdraw the money and °ed. However, they assume that withdrawing money by two members of the group is not considered a conspiracy; rather it is considered to have received "authorizations". Therefore, they decided to encode the bank code (with a trusted computer) into 4 partitions so that any two or more partitions can be used to reconstruct the code. Since the thieves's representatives will not have a computer with them to decode the bank code when they come to withdraw the money, they want to be able to decode visually: each thief gets a transparency. The transparency should yield no information about the bank code (even implicitly). However, by taking any two transparencies, stacking them together and aligning them, the secret number should "pop out". How can this be done? The solution is proposed in 1994 by Naor and Shamir [1] who introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS).

Manuscript received April, 2014.

Mr. Atul Sureshpant Akotkar M. Tech (CSE) scholar Deptt. Of Computer science & Engineering RCET, Bhilai, Chhattisgarh,Bhilai- India.

Chaitali Choudhary M. Tech (CSE) Assistant professor in Deptt. Of Computer science & Engineering RCET, Bhilai, Chhattisgarh,Bhilai- India.

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want .To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography is introduced by first in 1994 Noar and Shamir [1]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

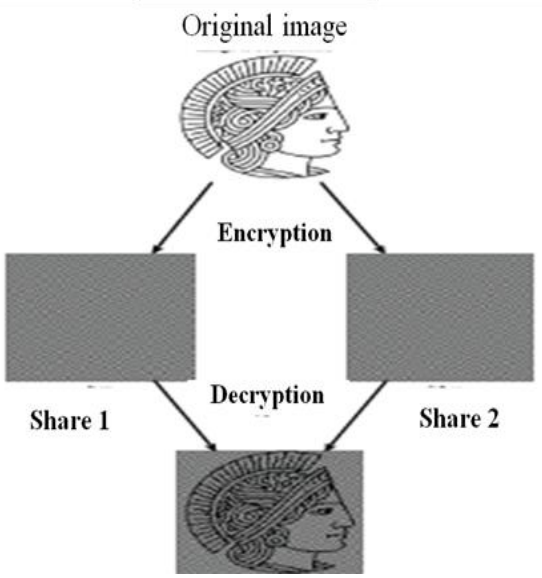

Fig:1 Encryption & decryption in visual cryptography

Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. This paper provides overview of various visual cryptography schemes. Taking limited bandwidth and storage into consideration two criteria pixel expansion and number of shares encoded is of significance. Smaller pixel expansion results in smaller size of the share. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. To meet the demand of today's multimedia information gray and color image format should be encoded by the schemes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

II. PROBLEM IDENTIFICATION

Biometric template is stored in centralized database, due to security threats biometric template may be modified by attacker. Biometric templates are vulnerable to eavesdropping and attacks. If biometric template is altered by attacker then authorized user will not be allowed to access the resource. So visual cryptography technique has been applied on to the biometrics template to make it secure from attack in centralized database. Visual cryptography will provide extra layer of authentication to the users. Eight types of attacks on biometrics system :

1. Involves presenting fake biometric.
2. Replay attack.
3. Feature extractor module is replaced with a Trojan horse program.
4. Genuine feature values are replaced with values selected by attacker.
5. The matcher is replaced with Trojan horse.
6. Template database attack.
7. Templates are replaced or altered in transition medium between template and database.
8. The matcher result can be overridden by attacker.

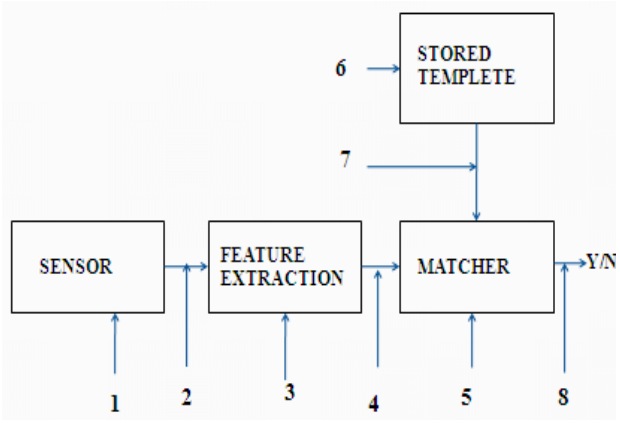

Fig:2 Possible attack points in generic biometric system..

III. PROPOSED METHODE

This project consist of following phases

- Face Detection based on skin color
- RGB Share generation.
- Share authentication
- Image Retrieval from RGB Shares

A. Face Detection Based on Skin Color:

Skin color plays a vital role in differentiating human and non-human faces. From the study it is observe that skin color pixels have a decimal value in the range of 120 to 140. In this project, we used a trial and error method to locate skin color and non skin color pixels. But many of the times, system fails to detect whether an image contains human face or not (i.e. for those images where there is a skin color background).an image is segmented into skin color and non-skin color pixels with the equations

$140 \leq |Pxy| \leq 120$----------eq. 3.1.1

$where\ Pxy = pixel\ at\ position\ xy$

The skin pixels values are set to 1(i.e. #FFFF) and non skin pixels are set to 0(i.e. 0000). The pixels are collected and set as per equation

If

$\lim_{i \to 1} n\ (\int_1^3 140 \leq |Pxy| \leq 120) = 1$--------

eq3.1.2

Else

$\lim_{i \to 1} n\ (\int_1^3 140 \leq |Pxy| \leq 120) = 0$-------eq 3.1.3

$where\ n\ =$

$total\ number\ of\ pixels\ of\ input\ image$

The resultant image becomes as

Original Image

Skin and non-skin pixels

Fig. 3.1 (Phase I)

B. RGB Share Generation

An image consists of Red, Blue & Green colors of 8 bit each.

Sr.No	Red(R)	Green(G)	Blue(B)
1	10000111	10011110	00110101

Each pixel is divided in to three equivalent blocks R, G, B respectively. In visual cryptography, we separate out these blocks to get shares.An Image Pixels can be represented as

$$Pi = \sum (Pr + Pg + Pb)$$ eq-------2.1

While forming sharing, we are considering an individual color components and shares can be formed with equations

$S_r = \int_1^n \lim_{n \to 1\ to\ n} (Pxyr)$ eq-------2.2

$Sg = \int_1^n \lim_{n \to 1\ to\ n} (Pxyg)$ eq-------2.3

$S_b = \int_1^n \lim_{n \to 1\ to\ n} (Pxyb)$ eq-------2.4

Where

S_r, Sg, S_b=Red, Green and blue Shares Respectively

P_{xyr}=P_{xyg}=P_{xyb}=Red, Green and Blue components of an image pixel.

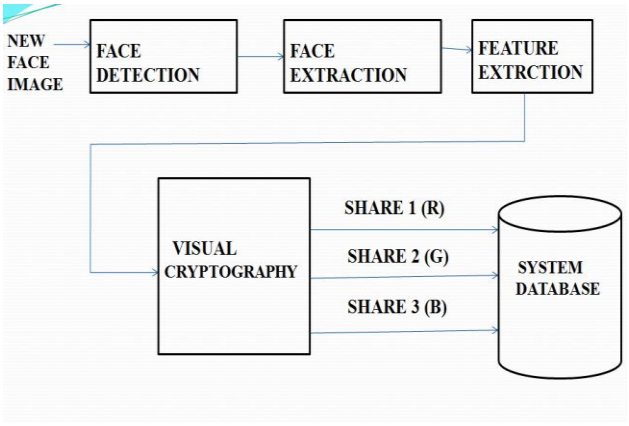

Fig: 3.2 User Enrollment

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

C. Share Authentication

Once shares of an test image are formed, these shares are matched with training shares .An overall sheme for share authentication can be presented as follows

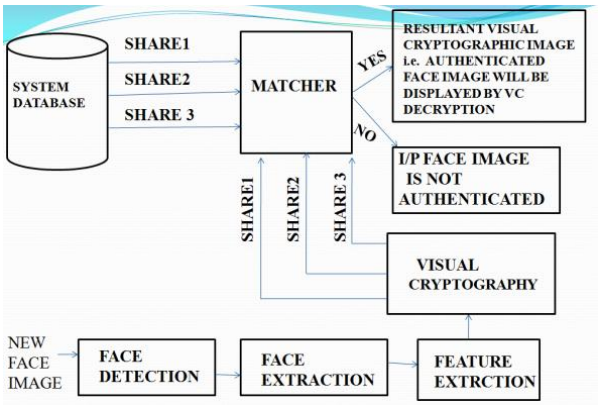

Fig: 3.3 User Authentication

System database maintains shares for various training images of which one of the shares can be matched with test image share. Matching can be done aas per the equation

$$D_f=\left|\lim_{n\to 1\ to\ n}\left(\lim_{x,y\to 1\ to\ n}(Pxym-Pxyt)\right)\right| \quad \text{Eq 3.1}$$

Where

D_f=Deviation Factor

P_{xym}=Input Image Pixels

P_{xyt}=Training Image Pixel.

From deviation factor , Matching percentage calculated as

$$P_r=|100-D_f| \qquad \text{E.q-------3.2}$$

Where P_r=Matching Percentage

Image authentication can be done based on matching percentage

$$If \quad \begin{matrix} Pr\geq 95 & authenticate \\ Pr<95 & Not\ authenticate \end{matrix}$$

D. Image Retrieval

Once share is authenticate, image retrieval can be done From three shares that are stored in training images set.

$$Ri=\int_1^n \lim_{x,y\to 1\ to\ n}(Concat|Srxy,Sgxy,Sbxy|)^n$$

E.q----------4.1

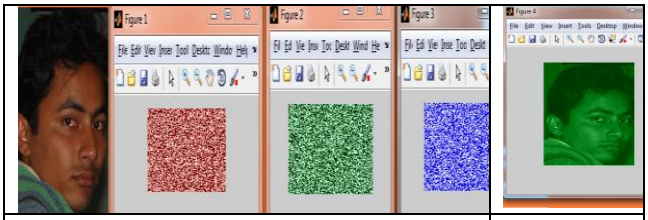

Fig:3.4 Input Image and its shares | *Retrieved Image*

IV. CONCLUSION

There are various measures on which performance of visual cryptography scheme depends, such as contrast, security, accuracy, computational complexity, share generated ,type of secret image.In the proposed system visual cryptography techniques is applied to protect face template in the database as well as providing extra layer of authentication to the existing face based authentication system.

In order to hide the secrecy we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in visual cryptography is towards maintaining the contrast at the same time maintaining the security. In this project we use visual cryptography for securing face authentication, here during encryption part actual image is decompose in to three shares i.e. red share, green share and blue share. Here we get R,G,B share as a result of encryption so it may be done for C, M, Y shares i.e. cyan, magenta, yellow shares.

In this project we use visual cryptography, here during encryption part actual image is decompose in to three shares this can be done for more number of share generation in future so that security will enhance.

REFERENCES

[1] Arun Ross, Asem Othman, "Visual Cryptography for Biometric Privacy ",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY , VOL.6 No.1, MARCH 2011.

[2] P. S. Revenkar, W. Z. Gandhare, "Secure iris authentication using visual cryptography", IJCSIS,1947-5500,2010.

[3] P. S. Revenkar, Anisa Anjum, W. Z. Gandhare, "Survey of Visual Cryptography Schemes", International Journal of Security and its Applictions, Vol.4, No.2, April 2010.

[4] Wen-Pinn Fang, "Non-Expansion Visual Secret Sharing In Reversible Style", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009.

[5] Daoshun Wang, FengYi, XiaoboLi, "On General Construction For Extended Visual Cryptography Schemes", Pattern Recognition 42 (2009),pp 3071 – 3082, 2009.

[6] Jung-San Lee, T. Hoang Ngan Le, "Hybrid (2, N) Visual Secret Sharing Scheme For Color Images", 978-1- 4244-4568-4/09, IEEE, 2009.

[7] Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang , "Visual Cryptography For General Access Structure By Multi-Pixel Encoding With Variable Block Size", International Symposium on Knowledge Acquisition and Modeling, pp. 340-344, 2008.

[8] F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.

[9] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen,"Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

[10] A. Jain and A. Ross, Handbook of Biometrics, Springer, 2007.

Mr. Atul Sureshpant Akotkar M. Tech (CSE) scholar Deptt. Of Computer science & Engineering RCET, Bhilai, Chhattisgarh,Bhilai-India. Publication: "A Comprehensive Approach Of Visual Cryptography For Color Images" IJTS International journal of Technology & Science Volume 1, issue 1, January 2o12.

Chaitali Choudhary M. Tech (CSE) Assistant professor in Deptt. Of Computer science & Engineering RCET, Bhilai, Chhattisgarh,Bhilai-India.
Publication: "A Comprehensive Approach Of Visual Cryptography For Color Images" IJTS International journal of Technology & Science Volume 1, issue 1, January 2o12.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.