Visual Cryptography Authentication for Locker Systems using Biometric Input

Siddhesh Urkude
Department of Computer Engineering,
Fr.Conceicaio Rodrigues Institute of Technology,
Vashi, Navi Mumbai

Pranjali Vaidya
Department of Computer Engineering,
Fr.Conceicaio Rodrigues Institute of Technology,
Vashi, Navi Mumbai

Shagufta Rajguru
Department of Computer Engineering,
Fr.Conceicaio Rodrigues Institute of Technology,
Vashi, Navi Mumbai

ABSTRACT
Visual Cryptography is an encryption technique that hides information in the images such that it can be decrypted by the human vision if the correct key image is used. This technique divides a secret image into various parts called shares depending on the variation of pixels. Biometrics deals with the automated methods of verifying the identity of a person based on physiological or behavioral characteristics.

This project aims to implement visual cryptography and biometric authentication to build a secure locker system. The fingerprint image of a user is considered as a secret image to generate shares that will be distributed among admin database and user. Authentication will take place by comparing the real time fingerprint image of the user and the image generated from the combination of the shares.

Keywords
Visual Cryptography, Shares, Biometrics, Authentication, Fingerprint, (2, 2) VC

1. INTRODUCTION

1.1 Visual Cryptography
Visual Cryptography is a process of creating shares or parts from an image so that it becomes unreadable for an 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.

Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. This can be achieved by one of the following access structure schemes:

1.1.1 (2, 2) Threshold VCS scheme
This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

1.1.2 (2, n) Threshold VCS scheme
This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed.

1.1.3 (n, n) Threshold VCS scheme
This scheme encrypts the secret image into n shares such that when all n of the shares are combined the secret image will be revealed.

1.1.4 (k, n) Threshold VCS scheme
This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

1.2 Biometric Authentication
Biometric Authentication uses the unique biological characteristics of an individual to verify identity for secure logins into electronic systems. The biometric technologies involved are based on the ways in which individuals can be uniquely identified through one or more distinguishing biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures. Biometric authentication is the application of that proof of identity as part of a process validating a user for access to a system. The system compares the current biometric captured data to the stored data in a database. If both samples of the biometric data match, authentication is confirmed and access is granted.

Types of biometric authentication technologies:-

- Retina scan produces an image of the blood vessel pattern in the light-sensitive surface lining the individual's inner eye.
- Iris recognition is used to identify individuals based on unique patterns within the ring-shaped region surrounding the pupil of the eye.
- Finger scanning, the digital version of the ink-and-paper fingerprinting process, and works with details in the pattern of raised areas and branches in a human finger image.
- Finger vein ID is based on the unique vascular pattern in an individual's finger.
- Facial recognition systems work with numeric codes called face prints, which identify 80 nodal points on a human face.
- Voice identification systems rely on characteristics created by the shape of the speaker's mouth and throat, rather than more variable conditions.

2. LITERATURE SURVEY

2.1 How Visual Cryptography Works

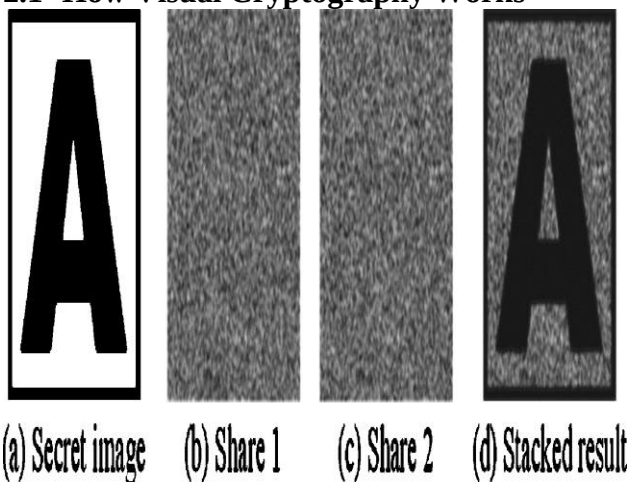

Figure 1: Visual Cryptography Working

Every secret image is divided into shares on the basis of the VC scheme chosen. The shares appear random and contain no decipherable information about the underlying secret image, however the stacking of the shares on top of one another makes the secret image decipherable by the human eye.

2.2 Various Visual Cryptography Schemes

Various schemes proposed for implementing Visual Cryptography in images are as follows:

2.2.1 Visual Secret Sharing Scheme (VSSS)

In 1994 Naor and Shamir[4] proposed this scheme. This is a *k* out of *n* VSSS or (k,n) scheme in which a binary image(picture or text) is transformed into *n* sheets of transparencies of random images. The original image becomes visible when any *k* sheets of the *n* transparencies are put together, but any combination of less than *k* sheets cannot reveal the original binary image.

2.2.2 2-out-of-2 VC scheme

Rijimen presented a 2-out-of-2 VC scheme. This applies the idea of colour mixture. The stacking of two transparencies with different colours leads to a third mixed colour.

2.2.3 Extended Visual Cryptography

Nakajima[5] proposed a VC scheme for natural images. It is used to produce meaningful binary shares. It presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together.

2.2.4 Binary Visual cryptography scheme

Hou[6] proposed the binary visual cryptography scheme which is applied to gray level images. According to this first the gray level image is transformed into a halftone image and then two transparencies of visual cryptography are generated. These shares are generated by applying halftone methods and colour decomposition. He decomposed the colour image into three (yellow, magenta and cyan) halftone images and then improvised three coloured 2-out-of-2 VC schemes which follow the subtractive model.

2.2.5 Halftone visual cryptography

In 2006 the Zhi Zhou, Gonzalo, R.Arce and Giovanni Dicrescenzo[7] have proposed halftone visual cryptography which produces good high quality and meaningful halftone shares, the generated halftone shares contain the visual information. In halftone visual cryptography a secret binary pixel "P" is encoded into an array of Q1 x Q2 ("m" in basic model) sub pixels, referred to as halftone cell in each of the "n" shares.

2.3 Comparison of Visual Cryptography Schemes

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

Figure2: Various Visual Cryptography Schemes

3. 2-OUT-OF-2 SECRET IMAGE SHARING SCHEME

In the 2-out-of-2 scheme, every secret pixel of the image is converted into two shares and recovered by simply stacking of the two shares together. This is equivalent to using the OR or XOR operation between the shares.

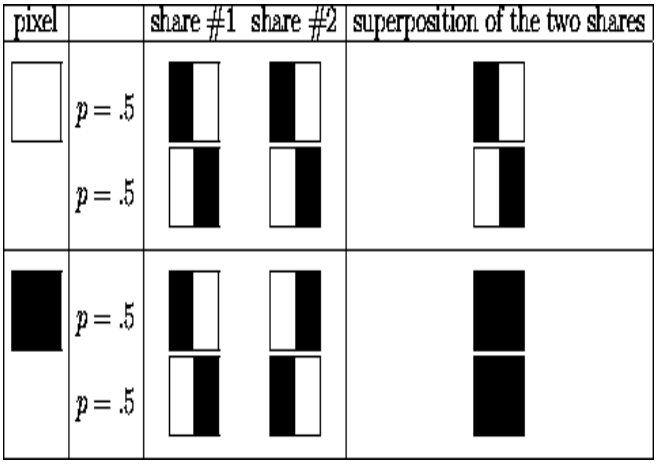

Figure 3: 2-out-of-2 secret sharing scheme

3.1 Algorithm (2-out-of-2 VC Share Generation Algorithm)

Input: A 2-d secret image img

Output: 2 meaningless shares S1 and S2

1. Find width and height of secret image
2. width=IMG WIDTH;
3. height=IMG HEIGHT;
4. Get the first share S1 of size width*height as binary random matrix,

   S1=Random_matrix
5. Generate second share S2 of size width*height by bitwise XORing the first share with secret image,

   S2=S1 XOR IMG
6. Return S1, S2
7. Exit.

4. EXISTING SYSTEM

4.1 Key Based Locker Systems

Most of the home and bank locker systems involve manual locks. For accessing the locker an individual requires a manual key. These are relatively easy to either access or duplicate. Any individual can easily access the locker because there is no other verification or authentication involved.

4.2 Digital Locker Systems

In a digital locker system each locker is provided with a low cost digital system that controls the lock to the locker instead of a key. This digital system comprises of a small display mounted on the locker itself. For home and hotel room lockers, the digital system is connected to an embedded controller that will manage the locking and unlocking of the locker through the verification of the password that is set by the user.

4.3 GSM Based Locker Systems

Each locker is provided with a digital system that is connected to a computer that has the database of the users. The digital system uses various personal details of the user like the date of birth and their ATM pin and the date of the particular day to generate a random number that is unique to the user. This random number is display on the display on the locker. When a individual wants to access the locker they have to see the random number and send this number from their registered mobile number to admin computer. Message transfer involves use of GSM technology.

4.4 RFID Based Locker System

This system consists of microcontroller, RFID reader, GSM modem, keyboard, and LCD. The RFID reader reads the id number from passive tag and sends to the microcontroller. If the id number is valid then microcontroller sends the SMS request to the authenticated person's mobile number, for the original password to open the locker. The person sends the password to the microcontroller, which will verify the password entered by the key board and the one received from the authenticated mobile phone. If these two passwords are matched the locker will open.

4.5 Biometric Authentication Locker Systems

These locker systems implement the locking and unlocking of the lockers with the technique of fingerprint recognition or other biometric parameters like retina scan as the way to open and close the lock. The system captures the fingerprint of the locker user and requires a fingerprint match to reopen the locker door, ensuring that only the authorized user can open the locker door to remove its contents. This system not only reduces the trouble for customers to bring the key, but also increases the trust and security for customer.

4.6 DigiLocker

A DigiLocker is used to securely store e-documents as well as store Uniform Resource Identifier (URI) link of e-documents issued by various issuer departments. The e-Sign facility provided as a part of the DigiLocker system can be used to digitally sign e-documents.

5. PROPOSED SYSTEM

The working of the proposed locker authentication system is divided into two phases:

- Registration
- Login

5.1 Registration

An authorized user's fingerprint is scanned by the system The fingerprint image is divided into shares using the visual cryptography algorithms. One share is stored in the system database and the second share is provided to the user. The share stored in the database is linked with the user id so that in the database a proper table is created. In this table user id will act as an index for each particular share related with that user id.

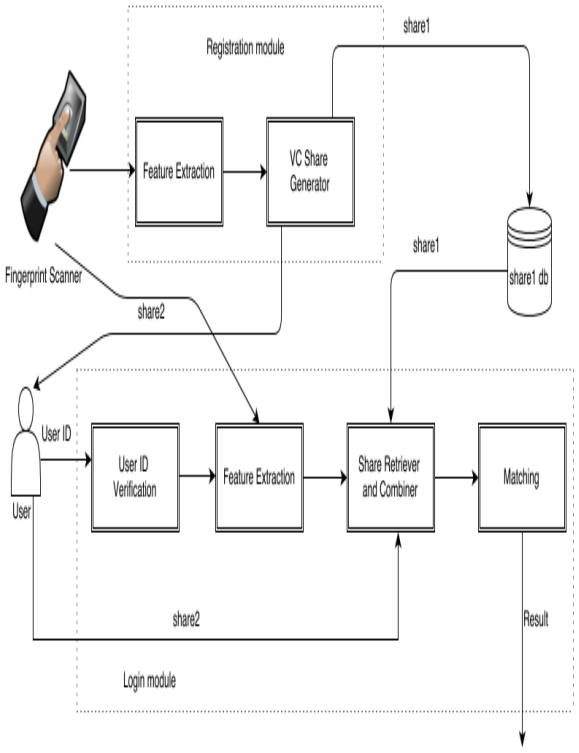

Figure 4: Block Diagram

5.2 Login

In order to access the locker the registered user should provide the share stored with the user and his/her user id. This user id will be matched with the one in the system database. Once it is matched, share obtained from the user is combined with the corresponding half share stored in the database to form a complete fingerprint image. The fingerprint of the user wanting to access the locker will also be scanned at the real

time and compared with the generated fingerprint image from the shares of that registered user. If the two fingerprint images match in the real time, then the user is authenticated and the locker access is provided, else the locker access is denied. This system provides a two-way security mechanism for the lockers. The uniqueness of fingerprints to every individual human being and the visual cryptography sharing technique ensures that no unauthorized user can be provided an access to the locker and there are no threats of duplication or hacking.

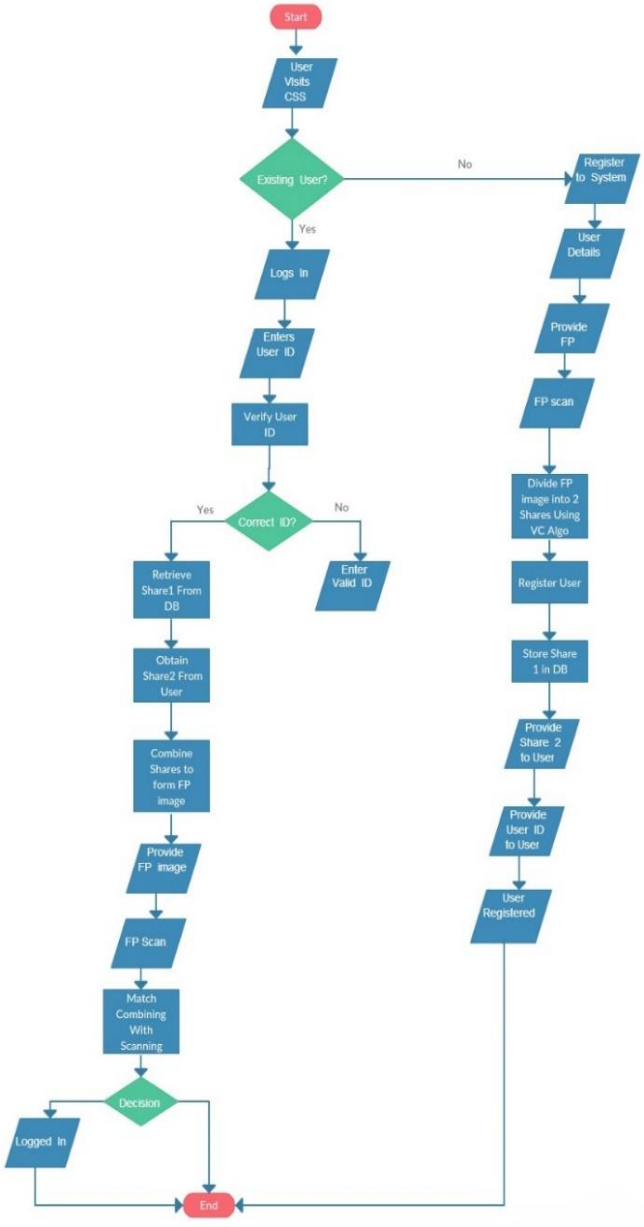

Figure 5: Flowchart

6. APPLICATIONS

6.1 Military ammunition box

The proposed system can be used for military ammunition boxes used to store the weapons and ammunition which are to be delivered or are stored at a particular place such that any outside intruders do not access the box. The proposed two level security system will make it difficult for any intruder to hack the system.

6.2 Online data storage

The system can also be used for the online storage of docs, pdfs, files, images etc. In this way any soft copy can be kept more secured with hassle free authentication technique.

6.3 Bank and jewelry lockers

Bank lockers contain huge amount of money in the form of cash stores and jewelry. The proposed system can be used to store the jewelry and cash securely such that the transactions can be handled only by authenticated bank employees and customers.

6.4 Home and hotel lockers

Home lockers are used for storing jewelry, important confidential papers, cash, and other valuables. Such important amenities can be kept safely and secured using this system.

7. CONCLUSION

Visual cryptography is a current area of research where a lot of scope exists. Various innovative ideas and extensions exist for the basic visual cryptographic model. In the existing Locker Systems the system database contains the password of the user. Whereas in this proposed scheme, the user will provide the password at real time and till then the database will have just the half of the shares which are useless alone. Thus the proposed system provides two levels of security through encryption and sharing of fingerprint image and biometric fingerprint authentication to validate the unique identity of every person.

8. FUTURE SCOPE

Secure e-lockers for storing the confidential e-documents can be developed using the proposed authentication system. Other biometric properties like retina and iris pattern, voice structure, hand geometry, earlobe geometry, etc. can be incorporated in the project for further enhancements. Two or more biometric properties can be combined and implemented for the authentication process.

9. REFERENCES

[1] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm

[2] https://en.wikipedia.org/wiki/Visual_cryptography

[3] http://www.datagenetics.com/blog/november32013/

[4] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology - EUROCRYPT'94, pp. 1-12, 1995.

[5] Mizuho Nakajima and Yasushi Yamaguchi, “Extended Visual Cryptography for Natural Images”

[6] Young-Chang Hou, "Visual cryptography for color images," Pattern Recognition, Vol. 36, No. 7, pp. 1619-1629, 2003.

[7] Z. Zhou, G.R. Arce and G. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, Vol. 15, No. 8, pp. 2441-2453, 2006.

[8] Nazanin Askari, Cecilia Moloney, Howard M. Heys, “Application of Visual Cryptography to Biometric Authentication”, Electrical and Computer Engineering, Memorial University of Newfoundland St. John’s, Canada, October 19, 2011.

[9] P.S.Revenkar Faculty of Department of Computer Science and Engineering Government College of Engineering, Aurangabad, Maharashtra, India,

AnisaAnjum, Department of Computer Science and Engineering Government College of Engineering, Aurangabad, Maharashtra, India, W.Z.Gandhare, Principal of Government College of Engineering, Aurangabad, Maharashtra, India. "Secure Iris Authentication Using Visual Cryptography". (IJCIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, 2010.

[10] Mr. Rohith S, Mr. Vinay G, Department of E&C,NCET, Bangalore, Karnataka, India. "A Novel Two Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme", International Journal Of Computational Engineering Research / ISSN: 2250–3005 IJCER | May-June 2012 | Vol. 2 | Issue No.3 |642-646 Page 642

[11] Rajeswari Mukeshi, Department of Computer Science and Engineering, Meenakshi College of Engineering, Chennai, India, V.J.Subashini, Department of Computer Applications, Jerusalem College of Engineering, Chennai, India. "Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique". IEEE- International Conference on Advances in Engineering, Science and Management(ICAESM-2012), March 30,31, 2012.