Visual Cryptographic Applications

Anushree Suklabaidya
Department of Computer Science
Birla Institute of Technology, Mesra
Ranchi, India
anushree.suklabaidya@gmail.com

G. Sahoo
Department of Information Technology
Birla Institute of Technology, Mesra
Ranchi, India
gsahoo@bitmesra.ac.in

***Abstract*—Visual Cryptography is a special kind of cryptographic scheme where the decryption of the encrypted secret is done by the human vision and not by complex mathematical calculations. Visual Cryptography deals with any secrets such as printed or pictures, etc. These secrets are fed into the system in a digital (image) form. The digital form of the secrets is then divided into different parts based on the pixel of the digital secret. These parts are called shares. The shares are then overlapped correctly to visualize the secret. This paper shows the different applicable areas of Visual Cryptography.**

Keywords- Authentication, Overlap, Secret, Shares, Subpixels, Visual Cryptography.

I. INTRODUCTION

Naor and Shamir [1] introduced Visual Cryptography in 1994. The basic model of Visual Cryptography assumes that the secret message consists of black and white pixels. Each secret pixel is either divided into two subpixels or four subpixels. These subpixels form the shares for the secret message. There are different or similar subpixel pattern based on the secret pixel according to Figure 1.

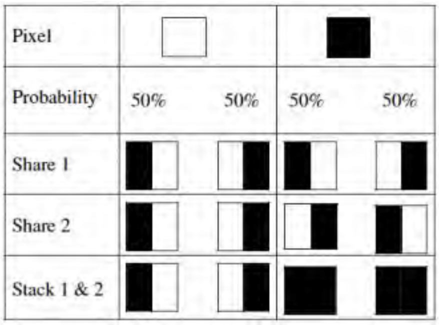


Figure 1: 2 out of 2 using 2 subpixels per original pixel.

The inferred structure can be described in the form of m×n Boolean matrix S = [s_{ij}] where s_{ij}=1 iff the jth subpixel of the ith share is black. These subpixels are then printed on transparent sheets so that overlapping the transparent sheets reveals the secret message. The graylevel value of this combination of shares is equal to the Hamming Weight H(V) of the "or" ed m-vector V. The graylevel is visualized as black if H(V) ≥ d and white if H(V)≤ d-α.m for some fixed threshold 1≤d≤m and relative difference . .

Different kinds of Visual Secret Sharing Schemes existing are:

- (n, n) Visual Secret Sharing Scheme
- (k, n) Visual Secret Sharing Scheme

(n, n) Visual Secret Sharing Scheme is where the secret is divided into a total of n shares and all the n shares are overlapped to get visually read the secret message.

(k, n) Visual Secret Sharing Scheme is where the secret is divided into n shares and any k or more of these shares when overlapped reveals the secret.

(k, n) Visual Secret Sharing Scheme consists of two collections of n×m Boolean matrices C_0 and C_1. When a white pixel is shared, any one of the matrices out of the collection in C_0 is chosen. And when a black pixel is desired to be shared, anyone matrix out of all in the collection in C_1 is considered. The following conditions are to be satisfied to reveal the secret in a (k, n) Visual Scheme using the above matrices.

- For ant S in C_0, the "or" V of any k of the n rows satisfies H(V)≥ d.

- For any subset $\{i_1, i_2, \ldots\ldots, i_q\}$ of $\{1, 2, \ldots.., n\}$ with $q < k$, the two collections of $q \times m$ matrices D_t for $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrix in C_t (where $t=\{0, 1\}$) to rows $i_1, i_2, \ldots\ldots, i_r$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The third condition means that if less than k shares are inspected, it is almost impossible to gain any knowledge about the secret pixel shared being black or white. The first two conditions are to ensure the contrast and the third condition ensures security.

The parameters,

m = the number of pixels in a share. Also known as the pixel expansion should be as small as possible to retain the resolution of the original image in a decrypted image.

α = the relative difference. This represents the loss in contrast and hence it must be as large as possible.

r = the size of the collections C_0 and C_1.

The advantages of Visual Cryptography are:

- Secure transmission of secret.
- Visual decryption without the help of complex mathematics.

The disadvantages of Visual Cryptography are:

- The decrypted image displays loss of resolution.
- The overlapping had to be done correctly to reveal the secret.

II. APPLICABLE AREAS OF VISUAL CRYPTOGRAPHY

A. Print and Scan Applications

Yan et al. [2] proposed a scheme in which they found a way of properly aligning the shares. The proper alignments of the shares are very important since only then the secret will be revealed. They came up with two methods:

Firstly, they put a mark beside the shares as shown in Figure 2 I and then the shares are overlapped according to the mark.

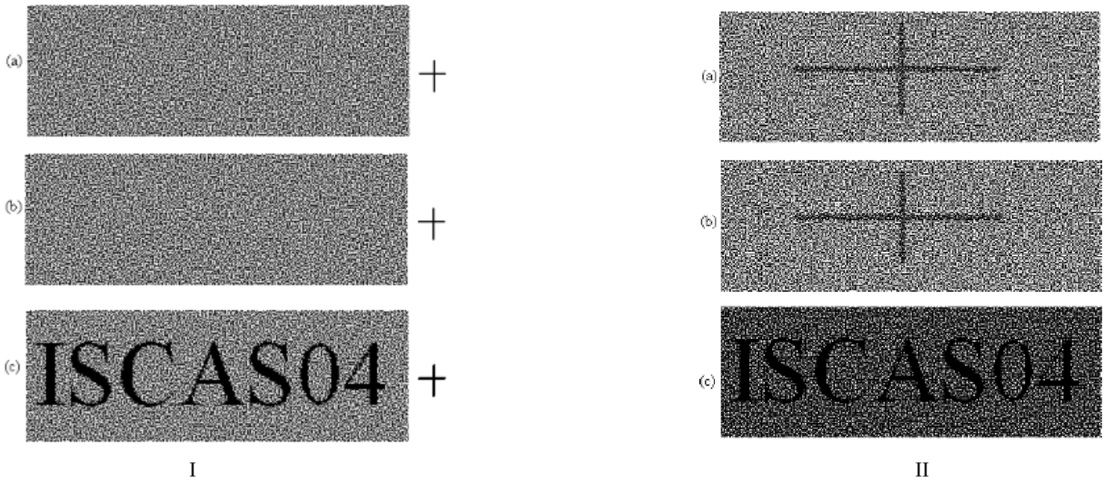


Figure 2: I. Shares and reconstructed image using the first technique. II. Shares and reconstructed image using the second technique.

Secondly, they put the mark in the shares using extended Visual Cryptography scheme. The example of this method is shown in Figure 2 II.

The above two techniques work in the spatial domain. The drawback of these methods is that the alignment marks are visible to the unauthorized persons and can be thus easily removed by cropping (for the first method) and by localized image alteration (for the second method).

Thus, to overcome the drawback they came up with another idea of marking the shares in the frequency domain. They used discrete Walsh Transform to do the same. The basic idea was that during encryption marks are embedded in the shares in the high frequency coefficients of the Walsh Transform. Then the inverse transform is used to make the new shares without any mark. These shares are then printed on transparent papers and distributed among the recipients.

During decryption, the papers, on which the new shares are printed, are scanned. The marks are then extracted using Walsh transform so that the shares are properly aligned to reveal the secret.

B. Human machine identification using Visual Cryptography

Kim et al. [3] proposed a scheme for the identification of human and terminal. They further extended Katoh and Imai's [4] scheme into a more generalized form, in which their extended form concealed several query images in a single display image. They then extended Droste's [5] scheme into a generalized scheme such that the combination of the transparent shares concealed independent secret images.

The steps for the human-machine identification are as follows:

- The user and the terminal both are associated with an identity (ID) and they both share a secret. A slide is distributed to the user which is generated by a (2, 2) Visual Secret Sharing Scheme.
- The user provides his ID to the terminal so as to acquire access to the service.
- The display image is then displayed on the screen on which the user overlaps his initially acquired share to get the secret message.
- A simple operation is then carried out by the user in which he uses the message and the share secret (which was shared initially). The inference of this operation is then provided to the terminal.

The generalized construction method of Katoh and Imai [4] is cited below with the aid of Figure 3.

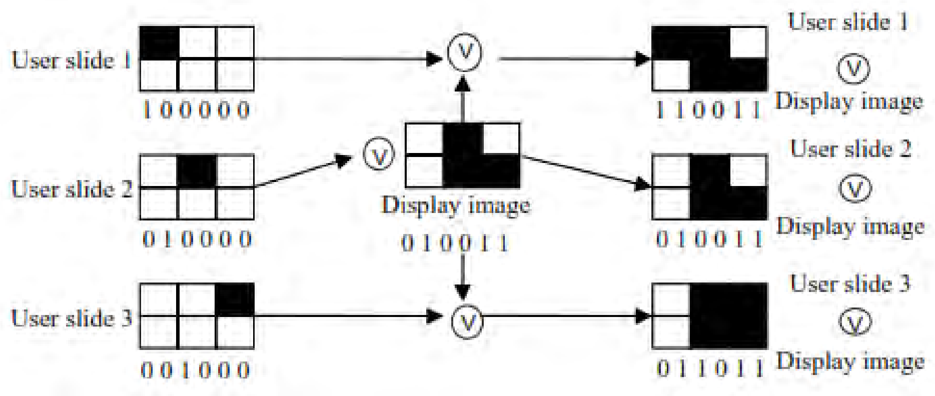


Figure 3: Generalized scheme of Katoh and Imai by Kin et al.

According to Figure 3, three query images can be concealed in one display image. Three different slides are distributed among three different users. The terminal generates only one display image. When these three user slides are overlapped with the display image, three different secrets are revealed.

The generalized construction of Droste's [5] scheme is cited below with the help of Figure 4.

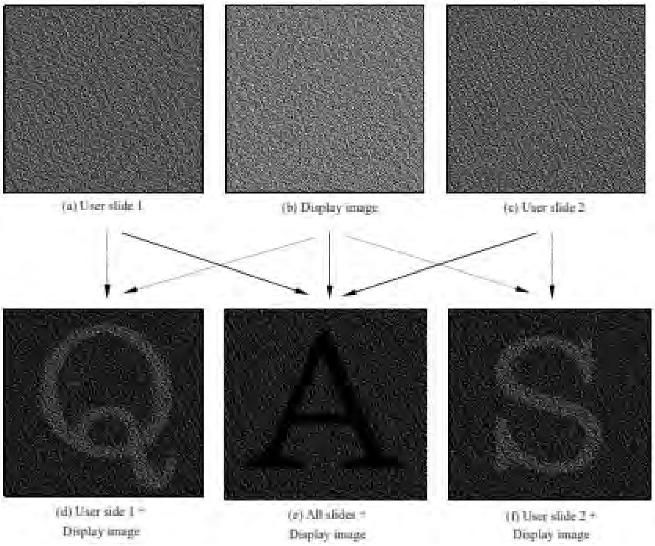

(a) User slide 1
(b) Display image
(c) User slide 2
(d) User side 1 + Display image
(e) All slides + Display image
(f) User slide 2 + Display image

Figure 4: Generalized scheme of Droste by Kim et al.

According to Figure 4, the different users are provided with the different user slides and a display image is generated at the terminal. Now, overlapping the user slides separately with the display image reveals different secrets. And when both the user slides are overlapped with the display image together, then a different secret is revealed.

C. Visual Cryptography Authentication for Data Matrix Code

Sharma and Rao [6] used Visual Cryptography authentication for Data Matrix Code in Identity cards. They proposed two levels of security of the Identity Card.

- The authentication of the Identity Card.

- The identity of the Identity Card owner.

Data Matrix Code is used to address the authenticity and security of the vital information of the owner such as credit card number, contact number, address or even photograph. Data Matrix Code is an optical, machine readable representation of data which uses the vertical dimension to store and retrieve information. Two 2D Data Matrix Codes are used in an Identity Card for storing private and public data. The first Data Matrix Code stores information that helps in digital logging and recording of information from the Identity Card. The second Data Matrix Code contains private information in the encrypted form. The first Data Matrix Code is known as the “Public Data Matrix Code” and the second Data Matrix Code is known as the “Private Data Matrix Code”.

The authentication process contains two levels. In the first level the Public Data Matrix Code and a master seed is used both of which is unknown to the owner of the Identity Card. The master seed contains the key for authentication of the Identity Card.

The second level authenticates the owner of the Identity Card. This level uses both the Data Matrix Codes as its shares and reveals the facial image of the owner hence authenticating the owner of the Identity Card.

The encoding and decoding process is shown in Figure 5 and Figure 6.

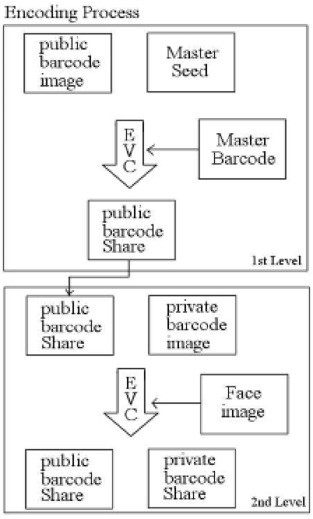


Figure 5: The encoding process.

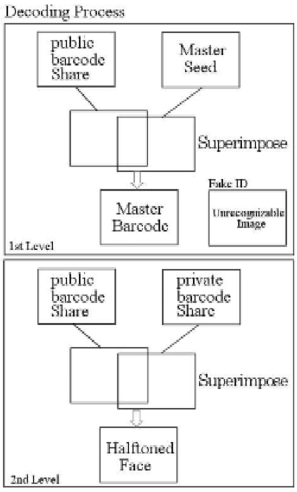


Figure 6: The decoding process.

D. Offline QR Code Authorization

Fang [7] proposed an algorithm for the authentication of offline QR (Quick Response**)** code. He used Visual Secret Sharing Scheme for the authentication. A QR code is matrix barcode which is readable by specific readers dedicated to QR code. The code consists of a white background on which black modules are arranged in a square pattern. The information that is encoded in a QR code can be any text or URL or any other data. There are six important features of a QR code:

- High capacity encoding of data.
- Small printout size.
- Chinese/Japanese (Kanji and Kana) capability.
- Dirt and damage resistance.
- Readable from any direction in 360^0.
- A structure append feature.

A QR code can append 7089 numeric characters for numeric data. A QR code must contain an encoding region and a function pattern viz., finder, separator, timing patterns and alignment pattern. Function pattern should not be used for encoding data. The code is surrounded by a quiet zone on all the four sides. An example of QR code is shown in Figure 7. Fang [7] used geometric calibration to use Visual Cryptography by print and scan.

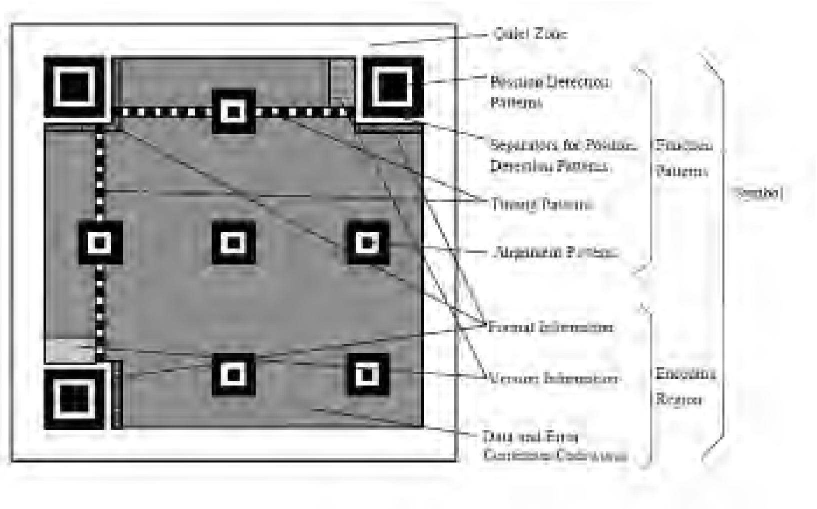


Figure 7: Structure of QR Code.

E. CAPTCHA

Vinodhini and Ambarasi [8] proposed a method for authentication based on Visual Cryptography using CAPTCHA. CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. Their method consists of three processes:

- Share Creation Process

User registers by furnishing their credentials such as name, date of birth, address, PIN, etc. These credentials are stored in the database. The secret PIN number provided by the user will act as a basis for the creation of the CAPTCHA image unique in nature. The CAPTCHA is then divided into two shares. One share is stored in the database and the other is given to the customer.

- Hash Code Generation

MD5 is used for the hash code generation. MD5 transforms a variable length message into a fixed length output of 128 bit. The input message is divided into blocks of 512 bits. The message is padded in such a way that its length becomes completely divisible by 512.

- Authentication Process

The customer needs to provide his share for any transaction. A hash code is generated for the share and the value is compared with the value already stored in the database. If a match occurs, the customer share is stacked with the share present in the database server. The stacked image is then processed to remove any noises. Then the authentication testing is done to accept or reject the user.

F. Fingerprint based Authentication

Rao et al. [9] worked with fingerprint which is one of the most reliable biometric features. Biometrics is the detailed measurements of human body. It deals with the automated methods of identifying on individual and verifying his identity. The scheme proposed by them consists of two processes:

- Registration process

In the registration process they considered the fingerprint as the secret image and made two shares out of it. One share is stored in the database. The other share is embedded into the photo identity card of the user. The share stored in the database is known as the “dummy share” and the share that is passed on to the user is known as the “participant share”.

- Authentication process

In the authentication process the photo identity card of the user is produced. The participant share is extracted from the identity card and is overlapped with the dummy share. This gives the fingerprint of the user which authenticates his identity.

The registration process and the authentication process are shown in Figure 8 and Figure 9.

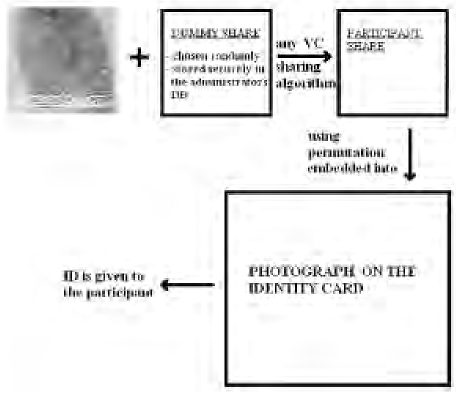

DUMMY SHARE
- chosen randomly
- stored securely in the administrator's DB
any VC sharing algorithm
PARTICIPANT SHARE
using permutation embedded into
PHOTOGRAPH ON THE IDENTITY CARD
ID is given to the participant

Figure 8: Registration process.

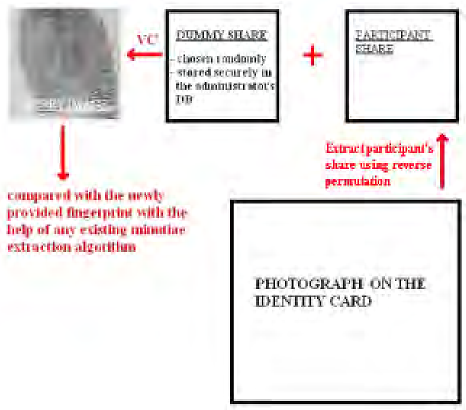

VC'
DUMMY SHARE
- chosen randomly
- stored securely in the administrator's DB
PARTICIPANT SHARE
Extract participant's share using reverse permutation
compared with the newly provided fingerprint with the help of any existing minutiae extraction algorithm
PHOTOGRAPH ON THE IDENTITY CARD

Figure 9: Authentication process.

G. *Signature based Authentication*

Hegde et al. [10] proposed a technique for the secure authentication for banking application based on signature. Their method consists of the steps as shown in Figure 10.

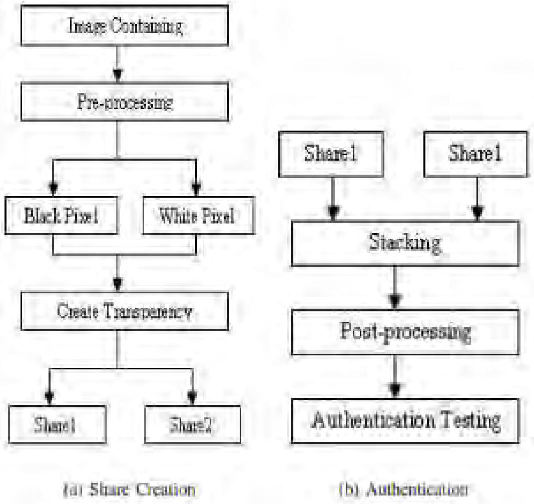
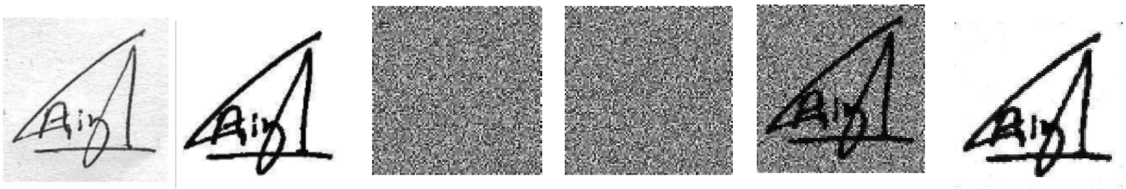


Figure 10: Signature based authentication.

They first pre-processed the original secret image. The signature, which is widely and most commonly used in banking applications for authentication, is considered as the original secret image. After the image is being pre-processed, shares are being created base on the pre-processed image.

In the authentication process, the shares are stacked one above the other and a post processing is done. The revealed secret signature then authenticates the customer of the bank as an authorized person to carry out transactions.



(a) (b) (c) (d) (e) (f)

Figure 11: (a) Original Signature (b) Signature after pre-processing (c) Share 1 (d) Share 2 (e) Revealed Signature (f) Signature after post-processing.

H. *Sheltered Iris Attestation*

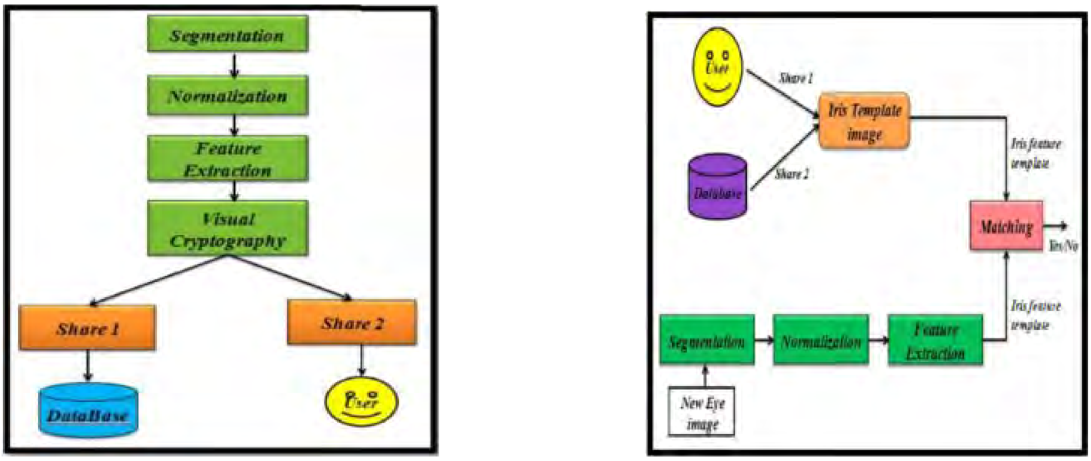
A sheltered iris attestation using Visual Cryptography is proposed by Sindhuja et al. [11]. Their method consists of two phases:

- Registration phase

In the registration phase an image of the user's eye is captured. The iris template is then extracted from it and is preprocessed. Shares are then created by pixel expansion. The shares are then recorded in the database along with the ID number. The user share is given to the user.

- Attestation phase

In the attestation phase, for accessing any resources the user have to provide his share as well as the ID number to the administrator. The user share and the share stored in the database are then overlapped to get the image of the iris of the user. If a match is found between the fresh iris image of the user and the iris image revealed by overlapping the shares, the user is granted access to the resource. The phases are shown in Figure 12 (a) and Figure 12 (b).



(a)

(b)

Figure 12: (a) Registration phase (b) Attestation phase.

I. Tongue based Security Improvisation

Suryadeva et al. [12] proposed a method of using tongue as a biometric authentication feature in banking system. They used Visual Cryptography to improvise the security of the banking system. They used 3D tongue capture technique to capture the image of the tongue. The steps are shown below:

- Location of human head-it is the place where user has to set his head for taking tongue images.
- Digital camera 1-placed at front of the location of human head to take frontal view.
- Digital camera 2-placed at one side of location of human head to take profile view.
- Laser locator-system finds the correct pose with assistance of the laser locator.
- Platform-a processing platform containing the computers, electronics and software necessary to compute the system.

Figure 13 shows the complete setup for capturing the image of the tongue.

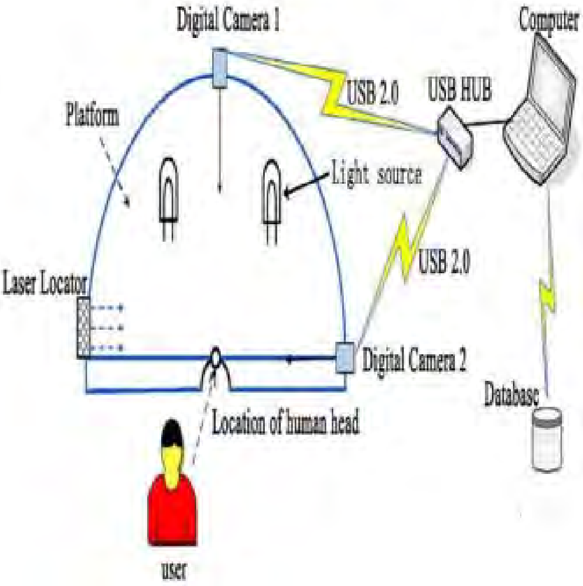
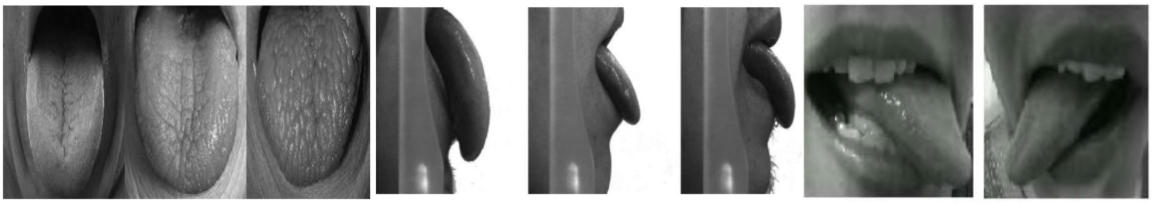


Figure 13: The set-up of capturing the image of the tongue.

The tongue is captured in three views as shown in Figure 14:



(a) (b) (c)

Figure 14: (a) Frontal View (b) Profile View (c) Lateral View.

The complete process of tongue based authentication is shown in Figure 15.

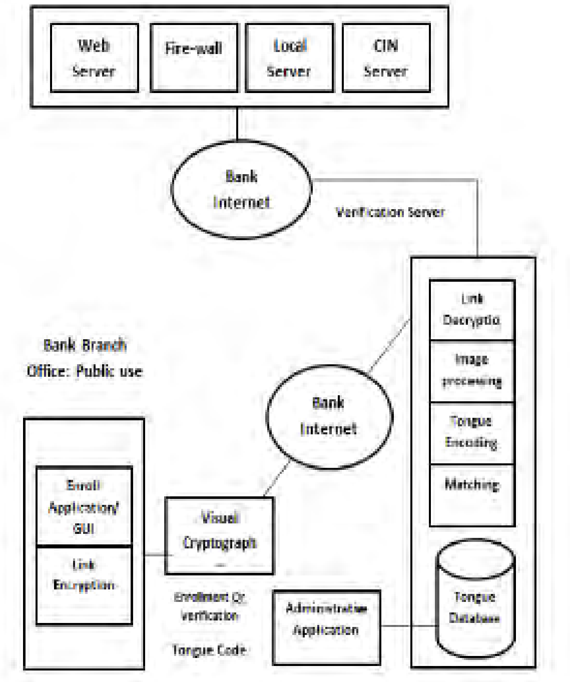


Figure 15: Complete authentication process.

J. Full Proof Lock and Key

Tunga and Mukherjee [13] proposed a scheme that describes a safety mechanism based on Visual Cryptography. The mechanism described consists of a lock and a key. For every pair of lock and key there is a unique image associated. The unique image is even unknown to the owner of the lock and key. This image is stored in the lock's internal memory. The secret image is then divided into two parts. One of these two parts is stored in the lock and the other part is stored in the key. The lock is attached to the door of the safe which has a power source. The lock contains an internal memory and can transmit signals to and from the key. The lock also contains a mechanism which can change the pixel distribution in the lock and the key. The secret images whereas remains the same only the division changes. The lock consists of the first part of the first secret image and the key consists of the second part of the first secret image. The key contains a power port. So, when the key is inserted it gets connected to the lock's power source. For the combination of the safe another secret image is used called as the second secret image. This second secret is similarly divided into two parts and stored similarly like the first secret. Hence the safety of the safe is controlled by two secret images. The lock of the safe opens only when both the shares of both the secret images get correctly matched.

K. Encryption of Cell-oriented Computer Generated Hologram

Yi et al. [14] described a method of encrypting Cell-oriented Computer Generated Hologram using Visual Cryptography. Hologram can be defined as the frequency pattern of an object and is usually recorded and recovered through the interference process of the reference wave and the object wave. Another way of recording a hologram is the Computer Generated Hologram (CGH). It synthesizes the hologram in the ideal condition through mathematical manipulation of the frequency pattern of the object.

The core of the CGH is the coding technique of the frequency spectrum in the form of complex value of real valued pattern. Two kinds of coding techniques are available:

- Point-oriented coding using graylevel.
- Cell-oriented coding using binary level.

Cell-oriented coding is done through the way where the complex value is represented by several binary cells. The number of white cells represents the amplitude and the position of the phase.

Since the secret in the hologram is reconstructed in the optical medium, the best way to decrypt a hologram is by the use of Visual Cryptography. In the encryption process, a cell is selected to substitute for the sub-cells. Then the value is distributed into several subpixels. Figure 16 (a) below shows the reconstructed result of the pure CGH. Figure 16 (b) and Figure 16 (c) represents the reconstructed result of the binary CGH image after encryption and decryption.

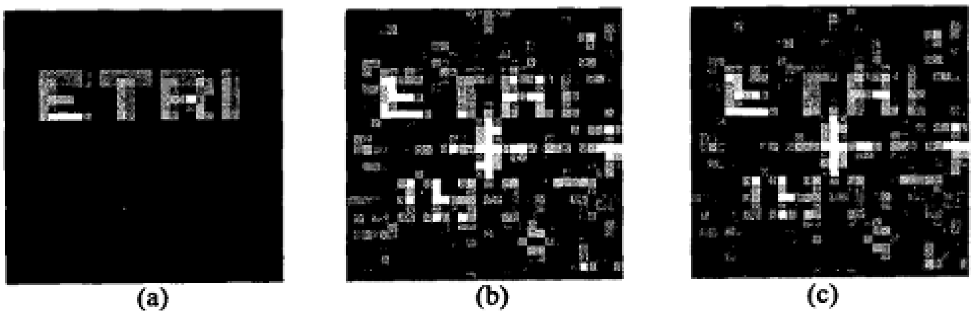


Figure 16: (a) Reconstructed result of pure binary CGH (b) Reconstructed result after encryption (c) Reconstructed result after decryption.

III. CONCLUSION

Visual Cryptography is a very creative technique of sharing secrets. It is generally used either for sharing any secret among individuals or is used for authentication purpose.It can be used in different fields and different area to ensure security. This paper is a compilation some of the major applicable areas of Visual Cryptography. There are still many areas which have not been coupled with Visual Cryptography which otherwise would prove beneficial.

REFERENCES

[1] M. Naor and A. Shamir, “Visual Cryptography”, Advances in Cryptology: Eurpocrypt’94, Springer-Verlag, Berlin, 1994, pp. 1-12.

[2] Wei-Qi Yan, Duo Jin, Kankanhalli, M.S., Visual cryptography for Print and Scan applications, Proceedings of the International Symposium on Circuits and Systems, 2004.

[3] K. Kim, J. Park and Y. Zheng, Human-machine Identification using visual cryptography, In Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems(1998) pp. 178–182.

[4] T.Katoh and H.Imai, “An Application of Visual Secret Sharing Scheme Concealing Plural Secret Images to Human Identification Scheme”, Proc. Of SITA’96, December 1996, pp.661-664.

[5] S.Droste, “New Results on Visual Cryptography”, Advanced in Cryptology-CRYPT’96, Aug. 1996, pp.401-415.

[6] M. Agnihotra Sharma and M. Chinna Rao, “ Visual Cryptography Authentication for Data Matrix Code”, International Journal of Computer Science and Telecommunications, Volume 2, Issue 8, November 2011, pp. 58-62.

[7] Wen-Pinn Fang, “Offline QR Code Authorization Based on Visual Cryptography”,Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2011, pp. 89-92.

[8] A.Vinodhini and L. Jani Ambarasi, “Visual Cryptography for Authentication Using CAPTCHA”, International Journal of Computer and Internet Security,Vol. 2,No. 1,2010, pp 67-76.

[9] Y.V Subba Rao, Yulia Sukonkina, Bhagwati Chakravarty and Umesh Kumar Singh, “Fingerprint Based Authentication Application using Visual Cryptography Methods”, TENCON 2008-2008 IEEE Region 10 Conference, pp.-1-5.

[10] Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik, “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”, ADCOM 2008, pp. 65-72.

[11] R. Sindhuja, R. D. Sathiya and V. Vaiythiyanathan, “Sheltered Iris Attestation by means of Visual Cryptography (SIA-VC)”, IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012, pp. 650-655.

[12] Sowmya Suryadevara, Rohaila Naaz, Shweta, Shuchita Kapoor, Anand Sharma,” Visual Cryptography Improvises the Security of Tongue as a Biometric in Banking System”, International Conference on Computer & Communication Technology (ICCCT)-2011, pp.412-415.

[13] Harinandan Tunga and Soumen Mukherjee, “ Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012, pp.-182-186.

[14] Yi, S. Y., Chung, K. L., Ryu, C. S., Cha, K. H., Lee, S. H., and Kim, E. S., (1999). “Encryption of Cell-oriented Computer Generated Hologram by using visual cryptography”, Proceedings of the Pacific Rim Conference on Lasers and Electro-Optics (CLEO/Pacific Rim 2001), Seoul, South Korea, Vol. 3, pp. 817-818.

AUTHORS PROFILE

Anushree Suklabaidya received her B.E from Rural Engineering College, Bhalki affiliated to Visvesvaraya Technological University, Belgaum. She is currently pursuing her M.Tech from Birla Institute of Technology, Mesra. Her research interest includes information security, network security, image processing and pattern recognition.

G. Sahoo received his MSc in Mathematics from Utkal University in the year 1980 and PhD in the Area of Computational Mathematics from Indian Institute of Technology, Kharagpur in the year 1987. He has been associated with Birla Institute of Technology, Mesra, Ranchi, India since 1988, and currently, he is working as a Professor and Head in the Department of Information Technology. His research interest includes theoretical computer science, parallel and distributed computing, cloud computing, evolutionary computing, information security, image processing and pattern recognition.