

Applications of Visual Cryptographic Scheme

[Jyoti Rao, Dr. Vikram Patil]

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. 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.

Keywords—Visual Cryptography, Shares, Authentication, Privacy

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 sub pixel pattern based on the secret pixel according to Figure 1.















Pixel				
Probability	50%	50%	50%	50%
Share 1				
Share 2				
Stack 1 & 2				

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

Jyoti Rao (Research scholar)
J.J.T. University
Jhunjhunu, Rajasthan,
India

Dr. Vikram Patil
Research Guide at J.J.T. University, Rajasthan
Principal at KBP College, Satara, India

The inferred structure can be described in the form of $m \times n$ matrix of Boolean $S = [s_{ij}]$ where the term $s_{ij}=1$ iff the term j th sub pixel of the pixel of i th share is black. These subpixels are then printed on transparent sheets so that overlapping the transparent sheets reveals the secret message. The gray level value of this combination of shares is equal to the value of Hamming Weight $H(V)$ of the V "or" ed m -vector of the V . The gray level is visualized as black if $H(V) \geq d$ and white if $H(V) \leq d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ 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) VSS Scheme which contains of two collections of matrix with values $n \times m$ Boolean matrices with C_0 and other is 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 value to the k of the n rows from matrix that satisfies $H(V) \geq d$.

For any subset $\{i_1, i_2, \dots, i_q\}$ of $\{1, 2, \dots, n\}$ with $q < k$, the two collections of $q \times m$ matrices D_t for t obtained by restricting each $n \times m$ matrix in C_t (where $t = \{0, 1\}$) to rows i_1, i_2, \dots, i_q are. 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 total number of pixels that are present in a share. Which 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.

A. Visual Cryptography Authentication for Data Matrix Code

Sharma and Rao [2] proposed a Visual Cryptography authentication used for Data Matrix Code in Identity cards. This 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 2 and Figure 3.

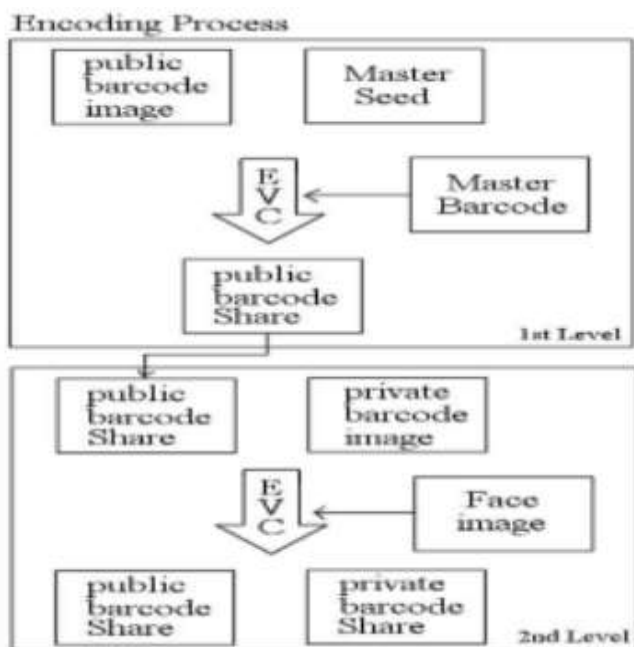


Figure 2 Encoding Process

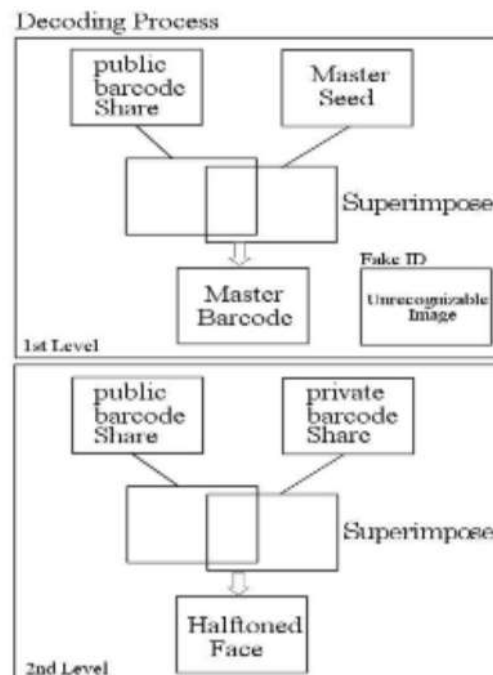


Figure 3 The decoding process

B. Human machine identification using Visual Cryptography

Kim et al. [3] proposed scheme which is used for the identification of human and terminal. That can be further extended into scheme which is in more generalized form, in which their extended form concealed several query images in a single display image. And then the next extended scheme that can 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 is cited below with the aid of Figure 4:

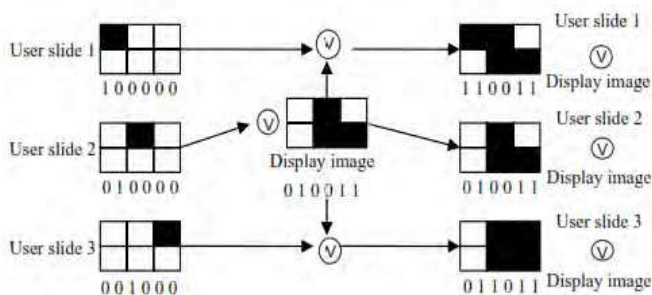


Figure 4: Generalized scheme of Katoh and Imai by Kin et al.

According to Figure 4, 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 scheme is cited below with the help of Figure 5.

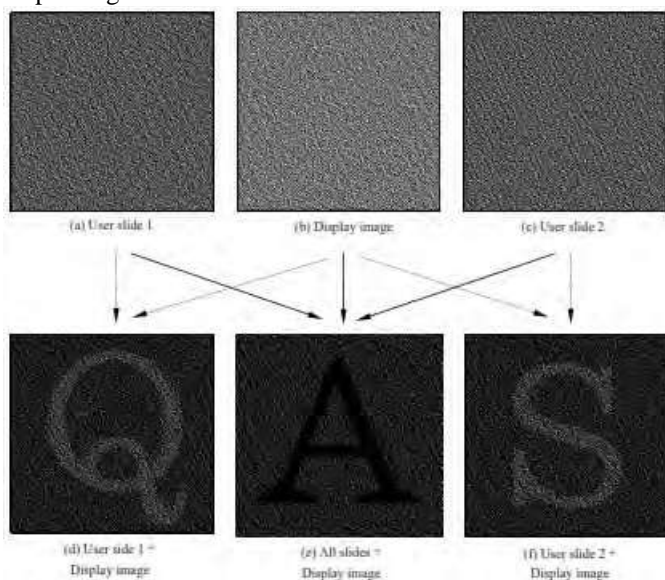


Figure 5: Generalized scheme of Droste by Kim et al.

According to Figure 5, 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. Authentication using Captcha and Visual Cryptography

Vinodhini and Ambarasi [4] proposed 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.

D. Fingerprint based Authentication

Rao et al. [5] proposed important work done 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 6 and Figure 7.

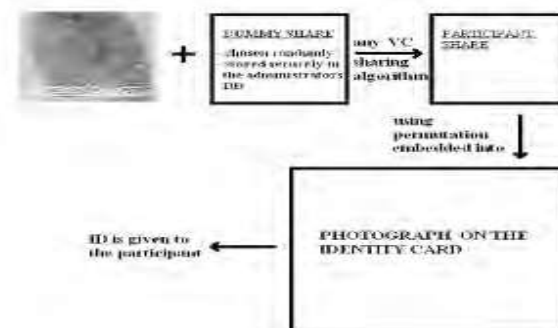


Figure 6: Registration process

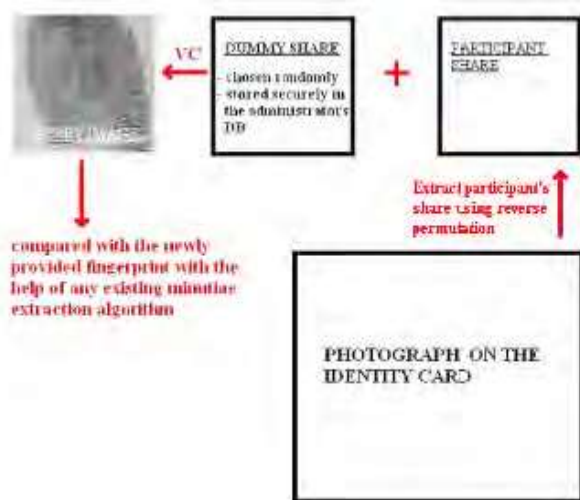


Figure 7: Authentication process.

E. Full Proof Lock and Key

Tunga and Mukherjee [6] 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.

F. Encryption of Cell-oriented Computer Generated Hologram

Yi et al. [7] 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 gray level.
- 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 8 (b) and Figure 8 (c) represents the reconstructed result of the binary CGH image after encryption and decryption.

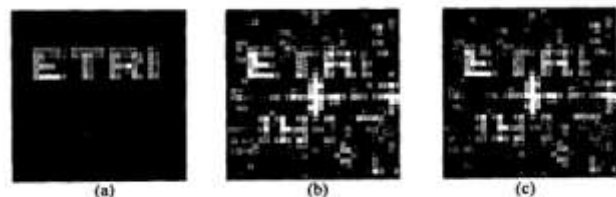


Figure 8: (a) Reconstructed result of pure binary CGH (b) Reconstructed result after encryption (c) Reconstructed result after decryption

Conclusion

Visual Cryptography is a very useful scheme for privacy protection of images as well as applications like authentication. In this paper we have compiled some of the applications of Visual cryptography though it is not limited to above applications. There is still more scope to integrate different areas with Visual Cryptography which can help in privacy protection

Acknowledgment

I would like to express my gratitude towards my guide Dr. Vikram Patil, Principal at K.B.P. College Satara for his constant support and motivation in carrying out my research work. It was because of his guidance I could complete this paper.

References

- [1] M. Naor and A. Shamir, "Visual Cryptography", Advances in Cryptology: Eurocrypt'94, Springer-Verlag, Berlin, 1994, pp. 1-12.
- [2] 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. 58-62.
- [3] Y. Zheng ,K. Kim, and J. Park, "Human-machine Identification using visual cryptography", In the Proceedings of the 6th IEEE International Workshop on the Intelligent Signal Processing and Communication Systems(1998) pp. 178–182

- [4] 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.
- [5] Y.V Subba Rao, Yulia Sukonkina, Bhagwati Chakravarty and Umesh Kumar Singh, “The Finger print Based Authentication Application using Visual Cryptography Methods”, *TENCON 2008-2008 IEEE Region 10 Conference*, pp.-1-5.
- [6] Harinandan Tunga and Soumen Mukherjee, “ Design and Implementation of the Novel Authentication Algorithm for the Fool-Proof Lock-Key System which Based On the Visual Secret Sharing Scheme”, *International Journal of Computer Science Issues*, Vol. 9, Issue 3, No 1, May 2012, pp.-182-186.
- [7] K. H., Lee, S. H., and Kim, E. S., Yi, S. Y., Chung, K. L., Ryu, C. S., Cha, (1999). “The 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

About Author (s):



Jyoti Rao is a research scholar at J.J.T.University Rajasthan, India. Her Research area is Visual Cryptography. She is working as Assistant Professor at D.Y.Patil Institute of Engg and technology, Pimpri Pune, Maharashtra, India



Dr. VikramPatil is Principal at K.B.P. College of Engineering, Satara, India. He is research guide at J.J.T.University, Rajasthan, and Shivaji University, Maharashtra, India