Compartive Analysis of Visual Crptography Schemes

Pramod Kumar Soni*
Madhu Chauhan**

Abstract

Visual cryptography is a technique to encrypt images, any handwritten notes or typed text which is in the form of images. Security is major aspect when transmitting information in modern era of information technology. Cryptography is basically uses the techniques of mathematics to provide the basic aspects of information technology such as confidentialities, data security, and authentication. The VCS is a method that hides a secret image by partitioning it into small parts. A distinguish property of VCS is that one can easily decrypt the encrypted image by superimposing parts without any mathematical computation as we did in cryptography.

In this work we are analyzing the different techniques in Visual Cryptography on parameters of security efficiency and computation techniques.

Keywords: Visual cryptography; Halftoning,Watermarking.

I. Introduction

Visual cryptography is a cryptographic technique that allows us to encrypt text or pictures without any requirement decryption algorithm or technique. To decrypt the data, human eye or analysis is required. This method was developed by Naor and Shamir in 1994. This is one of the methods to securely share our data .In this scheme the image is divided or broken into certain number of shares, say n. the original data or image can only be decrypted if all these n shares are combined. If any. of the share is missing, the data cannot be decrypted. This technique is used to broadcast secret message.

The basic model proposed by Naor and Shamir work on binary image, in which a image is divided into m number of parts (shares). Each pixel of image is denoted by n sub pixels in m image parts (shares). The resulting structure of each sub image is described by a unit matrix A where A=[A_{ij}] an [m x n] matrix A_{ij}=1 if the j^{th} sub-pixel in the i^{th} sub image is black A_{ij}=0. If the j^{th} sub-pixel in the i^{th} parts (share) is white. When the parts (shares) are grouped together in last in first out manner secret image can be obtained but the size of image is increased by n times. The grey levels of each pixels in decrypted image is proportional to the hamming weight H(V) of the OR – ed Vector "V, where vector "V is the grouped sub pixels for each original pixel. A solution of the "n out of "m visual secret sharing consists of two collections of m x n Boolean Matrices M_0 and M_1 .To share a white pixel, randomly choose one of the matrices from M_0, and to share a black pixel, randomly choose one of the matrices from M_1.The following conditions are considered for the construction of the matrices:

Advantage of Visual Cryptography

- The major benefit of visual cryptography is that decryption algorithm is not required.
- This Technique is easy to implement.
- Computational cost is low as secret message can be identified by human eyes.
- Cipher text can be send using e-mail and fax.

Disadvantage of Visual Cryptography

- When the message is decoded, there is some change in aspect ratio which may lead to loss of information as there is pixel expansion (to almost double) during decoding
- Sometimes it becomes difficult to align the transparencies in proper manner.
- For colored images some additional processing is required.

Pramod Kumar Soni*
Department of Information Technology
Institute of Innovation in Technology and Management

Madhu Chauhan**
Department of Information Technology
Institute of Innovation in Technology and Management

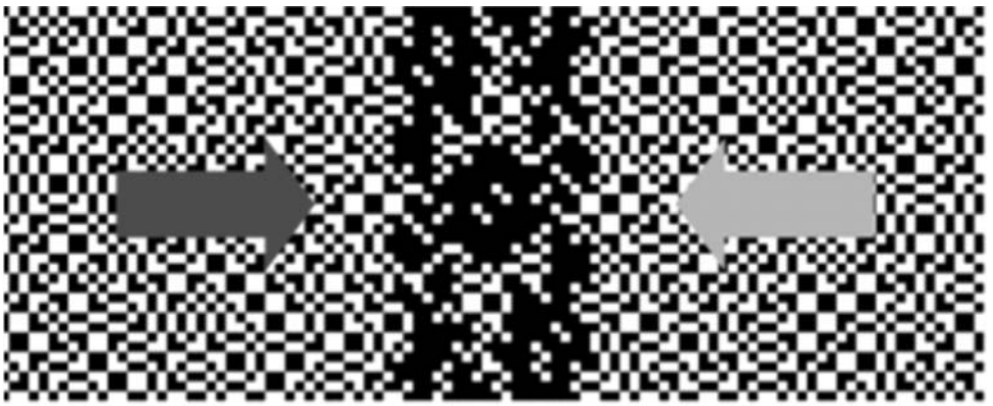

Figure 1: Overlapping of shares

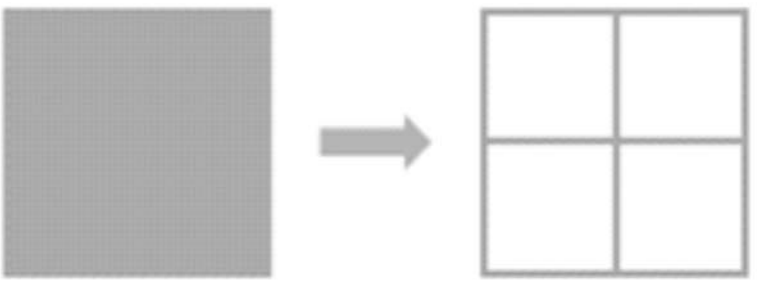

Figure 2: Division of pixels into parts

Major Application Areas of Visual Cryptogrpahy

- Remote Electronic Voting
- Biometric System
- Bank customer Identification
- Watermarking
- Steganography

II. Visual Cryptography Techniques

A. Visual cryptography for gray level image

Earlier efforts in visual cryptography were limited to binary images which is inefficient for real time processing. ChouLin proposed visual cryptography for gray level images by dithering techniques. A dithering technique is used to transform gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to complete the work of creating parts (shares). The effect of this scheme is satisfactory in terms of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

B. (k: n) Scheme of visual cryptography

K by n scheme can be considered as an extension to to the basic model which was proposed by Naor and Shamir. In this scheme n shares are generated out of original image. Original image can reconstructed only if k or more shares are stacked together such that 2<k<n. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained i.e. the original image can never be obtained if one has k-1 shares. If k=n, then all participants are required to reconstruct the secret.

C. Halftone visual cryptography scheme

Halftone visual cryptography introduces digital halftoning technique which has broadened the area of visual cryptography. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. These schemes make use of error diffusion as it less complex and provide good quality halftone shares. The text/image to be encrypted is embedded into binary valued shares and these shares are half toned by error diffusion technique.

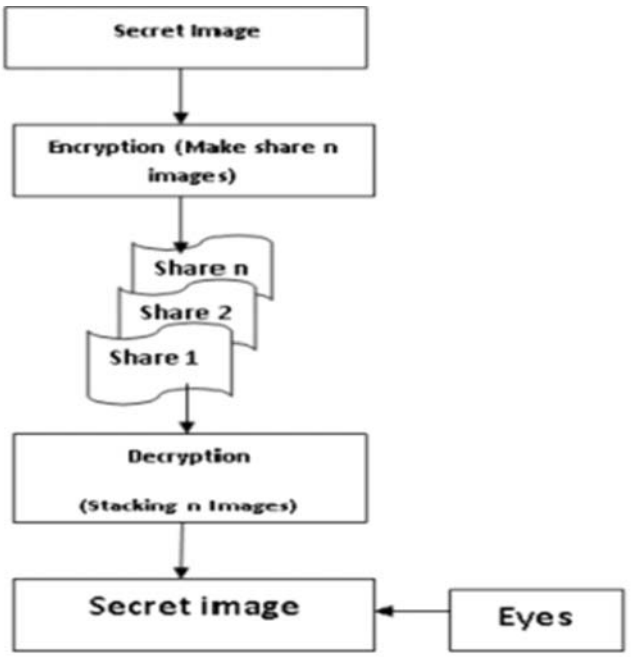

Figure 3: Basic Model of Visual Cryptography

D. Extended Visual Cryptography

Traditional VCS produces distorted images on decryptions. It suffers the problem of managing pixels on decryptions; because of these readers cannot visual identify the shares. This shortcoming is solved by EVCS (extended Visual cryptography scheme), which alters the working of traditional visual cryptography by adding a meaningful information to each share i.e., a cover page. In EVCS consists of two phases in first phase, a meaningless share is constructed using an OT and traditional Visual Cryptography scheme is used for construction. In later phase additional information in the form cover page by a stamping algorithm. The result shows that the problem of pixel expansion is also resolved.

E. Random Grid Visual Cryptography

A random grid based Visual cryptography scheme used to generate meaningful as well as meaningless shares. First, analyze the distribution of pixels on the share image and stack image. A probability allocation method is introduced which is capable of producing the better visual quality in share image and stack image. With this method, it not only hide the secret image by using different cover images, but also visual quality of images is improve as needed. The important part is improvement of contrast of both secret and stack images to their theoretical maximum. This method is superior to past methods for visual secret sharing.

Pixel expansion and visual quality are major problems in VSS. To solve the pixel expansion problem random grid approach is used, which consider share as big as original secret image. Here, Contrast enhanced VSs [8] and void-and-cluster base post processing [8] methods are introduced to improve contrast of reconstructed image. In VAC algorithm, arrays are constructed which works in terms of majority pixel and minority pixel. If less than half pixels are black then they are minority pixels and majority pixels are white. Cluster and void are used for arrangement of minority pixel in background of majority pixel. In homogeneous distribution, minority pixels are added in center of large void and majority pixels are added in center of tight cluster. So, optimal visual quality is obtained by applying contrast enhanced RGVSS and reconstruction of secret image is obtained by VAC based post processing method.

F. Multiple secret sharing VC

All the earlier research works in visual cryptography were aiming on securing only singe image at a time. Wu and Chen [10] were first researchers, who invented a visual cryptography scheme to share multiple secret images in two shares. In this technique, two secret

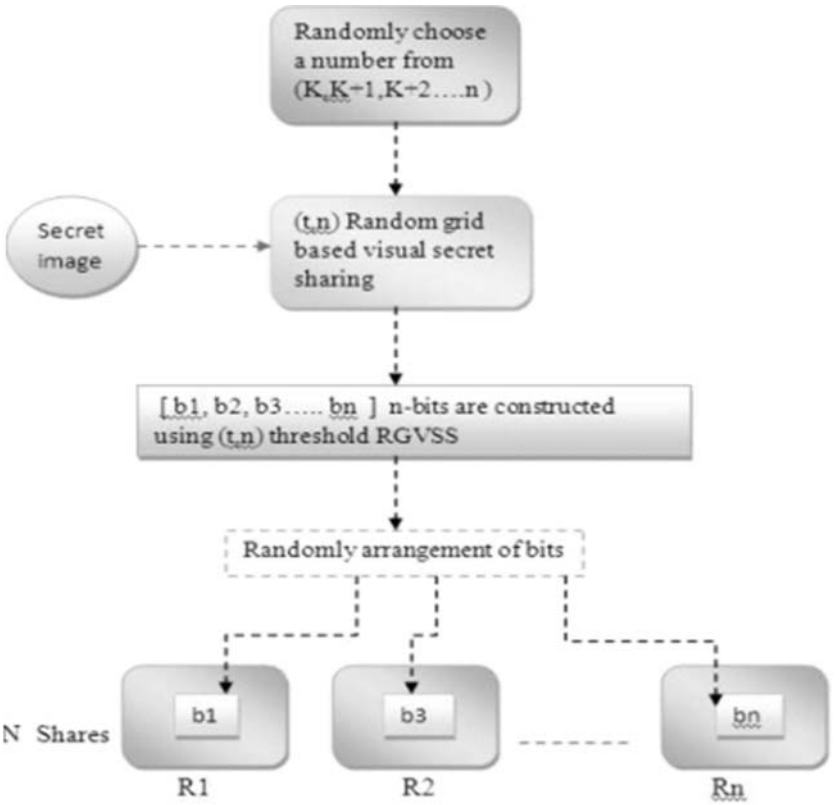

Figure 4: Random Grid Visual Cryptography

binary images can be hidden into two randomly generated shares, namely X and Y, such that the first secret can be seen by stacking the two shares, denoted by X—"Y, and the later secret can be obtained by rotating X by 90 degree anti-clockwise. J Shyu et al [11] proposed a scheme for multiple secrets sharing in visual cryptography, where more than two secret images can be secured at a time in two shares. Later the angle the restriction of rotating angles of 90^0, 180^0 and 270^0 is removed by Wu and Chen.

G. Progressive Visual Cryptography Technique

In progressive visual cryptography scheme for color images without any pixel expansion based on the halftoning technique. Progressive visual cryptography scheme is a special encryption technique which can be utilized to recover the secret image gradually by stacking more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of shares being stacked, the details of the hidden information can be generated progressively. Firstly, a chromatic image is divided into three monochromatic images in tones of RGB (Red, green and Blue). These three images are transformed into binary images by halftone technique. The secret image shares from binary images are obtained by the unexpanded VC algorithm. To prevent attack from hackers, the secret image shares are watermarked with different cover images (additional information) and are transmitted. At the receiver end the cover images are extracted from the shares and stacked one by one which reveals the secret image progressively. This scheme provides a more efficient way to hide colour images in different meaningful shares without any pixel expansion, providing high security and recovered images with high contrast.

III. Comparison of Different Visual Cryptography Techniques

Factors on which VCS schemes are compared and final summary is presented.

- Improve visual quality
- User Friendly
- Meaningless share
- Improved contrast in share and stack images.

Table No. 1: Comparison of Different Visual Cryptography Techniques

Technique used	Number of secret image	Merits	Merits
Traditional VC	1	Provide security for binary image	Not generate meaningful share image
Extended VC	1	Generate meaningful share	Contrast loss occur
Multiple secret sharing VC	2	Image can encrypt two secret images between two shares. Rotating angles is 90^0	Size of the shares is 4 times the size of the main secret image.
Progressive VC	1	No pixel expansion	No absolute guarantee on the correct reconstruction of the original pixel
Halftone VC	1	Provide meaning full share images	Tradeoff between pixel expansion and contras of original image

- Reduction of restriction for encryption process
- Visual quality analysis
- Security Analysis
- User friendly

IV. Conclusion & Future Scope

In day to day life, it is important to provide security to digital information. Since, Visual Cryptography is one of the techniques used for secret sharing of images.

It uses a general access structure (GAS) algorithms and provides an image of high resolution with outstanding visual quality. In this user-friendly secret sharing method not only security is provided but pixel expansion problem is also removed. It also produces meaningful shares which is easy to carry and manage. Encryption is performing on all pixels in the cover image and secret image, which guarantees that visual quality of share and stack image can reach the theoretical maximum.

Also, Encryption method is flexible to use. In this paper we had presented a comparative analysis of different visual cryptography techniques used by programmers and researchers in computer science on different parameters as discussed above.

Visual cryptography is the current area of research where lot of future scope exists. Right now different cryptographic techniques are is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. Visual cryptographic work can be extended with the format of color images, three dimensional Images, better quality color images, more number of shares and multiple secret images.

References

1. M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptology EUROCRYPT'94, LNCS 950, 1995, pp. 1–12.
2. R. I to, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fund. Electron, Communication Computer Science.
3. C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, no. 4, pp. 481–494, 2004.

4. S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," Imag. Sci. J., vol. 55, no. 2, pp. 90–101, 2007.

5. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, Jun. 1987.

6. Xiaotian Wu, Wei Sun, "Random grid-based visual secret sharing with abilities of OR and XOR decryptions", J. Vis. Commun. Image R. 24 (2013) 48–62

7. Xiaotian Wu, Wei Sun, "Improve visual quality of Random grid based Visual Secret Sharing", Signal Processing 93 (2013) 977–995

8. Kai-Hui Lee and Pei-Ling Chiu, "An Extended color Visual Cryptography algorithm for general access structure", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February 2012

9. Young-Chang Hou, Shih-Chieh Wei, And ChiaYin Lin, "Random-Grid-Based Visual Cryptography Schemes", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 24, No. 5, May 2014

10. T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.

11. D. C. Lou, H. H. Chen, H. C. Wu, and C. S. Tsai, "A novel authenticatable color visualsecret sharing scheme using nonexpanded meaningful shares,"Displays, vol. 32, no. 3, pp. 118–134, 2011.

12. mizuho nakajima, yasushi yamaguchi, "extended visual cryptographyfor natural images",