ISSN: 2321-7782 (Online)
Volume 1, Issue 4, September 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Visual Cryptography Schemes using Compressed Random Shares

L. N. Pandey[1]
M.Tech Scholar (CTA)
Gyan Ganga College of Technology
Jabalpur - India

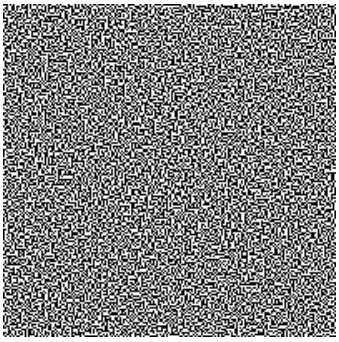
Neeraj Shukla[2]
HOD & Professor of Computer Science
Gyan Ganga College of Technology
Jabalpur - India

Abstract: ***Visual cryptography is one of the most secure techniques the allows the user to encrypt the secret images by transforming them into printable transparent sheets and these sheets can be distributed to different intended person through various mediums (physically, internet). On receiving the intended person may regenerate the original image by stacking all transparent sheets on each other. There are many visual cryptography schemes available that facilitates user to encrypt any various types and formats of images to encrypt and. This paper presents a visual cryptography scheme that can generate n number of transparent shares with reduced size and supports a variety of image formats and presents an integrated approach for binary, Gray and color image visual cryptography by maintaining the visual quality and pixel expansion.***

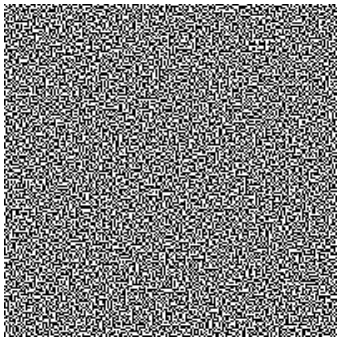
Keywords: Component of Visual Cryptography, Integrated approach, Compression, Random shares.

I. INTRODUCTION

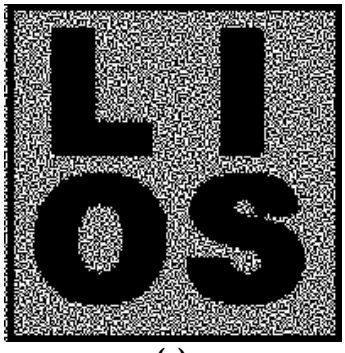
First and foremost, Naor and Adi Shamir [5] suggested an encryption scheme that was able to encrypt an images they call it visual Cryptography scheme. VCS is a type of cryptography in which images can be securely encrypted by dividing them in a distorted image called transparent shares and transmitted through physically by printing these shares on transparency sheets to the intended user. Figure 1 shows the basic idea of the visual cryptography scheme suggested by Naor and Adi Shamir in 1995.



(a)



(b)



(c)

In the figure shown above (a) and (b) are two shares generated by applying traditional VCS encryption scheme that can be printed on a transparent sheet separately. When received by the user the original image can be retrieved by stacking these shares of the user. The basic motive behind this scheme was to encrypt a secret image and send over unsure medium to the target user to share it. The beauty of this scheme is that the share generates by this scheme does not reveal any information about the original image and the number of shares generated in this scheme ensures the security of the content held in the share. This makes VCS scheme a completely secure scheme. VCS is a very important scheme and it is applicable in a wide variety of applications where it can be used. For instance it can be used by any person who has no information about cryptography can use it very easily. Some common example of the application area of VCS is military operations that are held in such a place where

normal communication technology does not work and such situations in which more than one person must be available to take a crucial decision.

II. Literature Survey

The associated secret sharing problem and its physical properties such as contrast, pixel expansion, the number of share generated and integrated user interface facility were comprehensively studied by researchers worldwide. For example, Naor *et al* [5] showed constructions of basic VCS with perfect reconstruction of the black pixels. Extended visual cryptography scheme (EVCS) was first proposed by Naor *et al.* [5], where a simple example of (2, 2) -EVCS was presented.

A. *Black And White Visual Cryptography Schemes*

Naor and Shamir's [5] proposed an encryption scheme to convert a binary image into two shares. In this scheme each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is visible only when both shares are stacked on each other. Visual secret sharing schemes based on the Threshold value of mixed XOR and OR operation with reversing and based on binary linear error- correcting code was suggested by Xiao-Qing and Tan [16]. The disadvantage of the above schemes is that only one set of confidential messages can be embedded, therefore for large amounts of confidential messages several shares have to be generated. One specific rotation based cryptographic technique was suggested by Zhengxin Fu, Jonathan Weir, WeiQi Yan [14] suggested a special type of scheme in which multiple images can be hidden. Wen-Pinn Fang [13] suggested non pixel expansion scheme in which the pixel expansion was minimal. These all schemes have their own disadvantages.

B. *Color Visual Cryptography Schemes*

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg [17]. Colored secret images can be shared with the concept of arcs to construct a colored VCS. In colored VCS one pixel is converted into m subpixels, and each subpixel is further divided into c color regions. In each subpixel, there is exactly one color region is colored, and other color regions are black. The color of one pixel depends on the interrelations between the stacked subpixels. For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3. Yang and Laih [18] improved the pixel expansion to c × 2 of Verheul and Van Tilborg [17]. But in both of these schemes share generated were random. To share true-color images Lukac and Plataniotis [20] developed bit-level based scheme by operating directly on S-bit planes of a secret image.

To hide a color secret image into multiple colored images it is desired that the generated camouflage images contain less noise. For this purpose R. Youmaran et al [19] invented an improved visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme provides improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. By considering color image transmission over bandwidth constraint channels a cost effective visual cryptography scheme was invented by Mohsen Heidarinejad et al [9]. This scheme offers a perfect reconstruction while producing shares with size smaller than the size of input image using maximum separable distance. This scheme provides pixel expansion less than one. Haibo Zhang et al [8] presented a multi-pixel encoding which can encode a variable number of pixels for each run to improve the speed of encoding. F. Liu [6] developed a color visual cryptography scheme under the visual cryptography model of Naor and Shamir with no pixel expansion. In this scheme the pixel expansion is not increasing the number of colors of a recovered secret image is increased.

C. *Extended Visual Cryptography Schemes*

The term of the extended visual cryptography scheme (EVCS) was first introduced by Naor in [5], where a simple example of (2,2) -EVCS was presented. One scenario of the applications of EVCS is to avoid the customs inspections, as the shares of EVCS are meaningful images, therefore there are less chances for the shares to be detected. There have been many EVCSs proposed in

the literature. Nakajima et al. [10] Proposed a (2,2) -EVCS for natural images. Furthermore, Zhou et al. [11] presented an EVCS by using halftoning techniques that can process gray-scale images. This scheme uses the complementary images to cover the visual information about the share images. Recently F. Liu and C. Wu [1] have suggested an EVCS by embedding shares behind the covering shares.

D. VCS for General Access Control

VCS for a general access structure with Multi-pixel encoding [8] is one of the emerging method in visual cryptography that can encode more than one pixel for each run. However, its encoding efficiency is not fast enough. This scheme offers a novel multi-pixel encoding that can encode a variable number of pixels for each run. The encoding length at one run is equal to the number of the successive same pixels met during scanning the secret image. Proposed scheme works well for general access structure for chromatic images without pixel expansion. The experimental result shows that it can achieve high efficiency for encoding and good quality of overlapped images.

III. Existing Methodology

The existing methodology is based on the embedded model of Visual Cryptography Scheme by covering shares proposed by Feng Liu and Chuankun Wu [1]. This model takes a gray scale image as input and images and generates and shares based on the count of the user groups. This approach is as follows.

Step 1: Create Dithering matrix to convert a grey scale image to binary.

Step 2: Initialize Basis Matrix to generate the secret shares.

Step 3: Create Covering Shares using different grey scale images.

Step 4: Embed the encrypted shares into each covering share.

Step 5: To regenerate the original image, stack all the covering shares.

Above scheme has some definite drawbacks such as limited image format support, only supports grey scale images etc.

IV. Proposed System

The proposed system uses a well known compression scheme for the security of the secret shares in place of the embedding process as it increases the execution time of the entire system and it also degrades the quality of the regenerated image. It also does not provide the reduction of the size of the covering shares in any way. Proposed system provides an integrated environment to process images. Most of existing cryptography tools support only single image format. The application can process .gif and .png (portable network graphics) formatted images and it is developed using Java technology, hence provides a simple user interface.

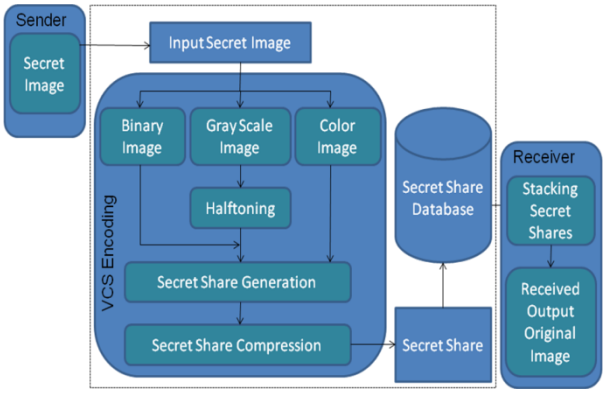


Fig.2. Proposed System Architecture.

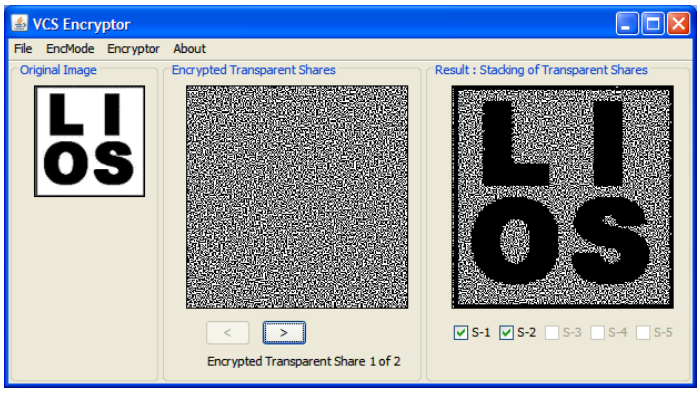


Fig.3. User Interface of proposed application.

The proposed system consists of three basic operations these are compressed share generation, encoding and decoding. Encoding is done by secret share generation and compression of these secret shares. Decoding is done by the stacking of the secret shares at the receivers end. The user interface of the proposed system is shown in fig. 3.

The basic idea of proposed system requires the following steps:

[S1] Select the image as input

[S2] Create encrypted shares using an appropriate encoding algorithm for intended secret image.

[S3] Prepare the dictionary for encrypted shares.

[S4] In dictionary replaces strings of characters with Single codes.

[S5] In the compression of encrypted share, select the secret pixels.

[S6] Then generation halftone shares using error diffusion Method.

[S7] Filter process is applied to the output encrypted shares.

[S8] Filters are used to improve the quality of the reconstructed image to minimize the noises for sharpening the input secret image.

These steps are discussed in detail in upcoming sections

A. *Secret Random Share Generation*

The secret shares are generated by using the random permutation of a pre selected basis matrix. The process of the encryption is implemented on the basis of the number of the required secret shares. These parameters are: I – Secret Image, N – Number of secret shares to be generated from I. Share – Encrypted image created using I.

To encrypt the secret image a well known LZW compression technique is used. It is a lossless compression algorithm suggested by Abraham Lempel, Jacob Ziv, and Tery Welch published in 1984 it has been improved by many of the researchers to get best results from it. This algorithm is implemented in following steps

Step1: Create the dictionary that contains all the strings of one character.

Step2: Find a string W with longest length that matches to give input.

Step3: Produce the index for W in the dictionary to give output and eliminate W from the input.

Step4: Append W followed by the next character in the given input to the dictionary.

Step5: Repeat from Step2. Until finished.

B. *Decoding*

Decoding is a very simple process by reading a value from the encrypted input and producing the related string form the generated dictionary. During this the next value from the input is obtained and added to the dictionary by concatenation of the string and the first character of the string accessed by decoding the next value. This process is continued for the next input value and repeated the process until all inputs are finished. Decoder creates a dictionary that is identical to that used by the encoder; this dictionary is used to decode subsequent input values. The advantage of this scheme is that the full dictionary is not required to send with encoded data.

V. CONCLUSION

The proposed VCS system is easy to use. Many VCS schemes are premeditated and their performance is analyzed on four criteria: number of secret images, pixel expansion, image format and type of share generated. Security is the primary concern of today's communication world; proposed system is competitive with some well known schemes. It provides a safe and secure transmission as it involves multiple manipulations for encryption and so is it with decryption. This System provides a simple user interface to process images. Furthermore, the proposed system is very easy to use and anybody can use this system without having any cryptographic knowledge. This system can be used in both ways i.e. shares can be printed on the transparent sheet and carried by users or it may be transmitted by the network and secret image may be regenerated by the system using the required number of eligible shares.

Acknowledgement

The paper could not be in physical form without the kind guidance and support of my seniors and near ones. I express my deep gratitude to all the dignitaries who made the efforts in the completion of this paper.

References

1. Feng Liu and Chuankun WO, "Embedded Extended Visual Cryptography Schemes" IEEE Trans., IFS, Vol.6, No.2, June 2011.
2. Ateniese G., Blundo C., De Santis A., and Stinson D. R. (1996), "Visual cryptography for general access structures" Inf. Computat., vol. 129, pp. 86.106.
3. Daoshun Wang, FengYi, XiaoboLi, "On General Construction For Extended Visual Cryptography Schemes", Pattern Recognition 42 (2009), pp 3071 – 3082, 2009.
4. Z. M. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.
5. Moni Naor, Adi Shamir, "Visual Cryptography", advances in cryptology– Eurocrypt, Berlin, Germany, 1995, vol. 950, Springer-Verlag, LNCS. pp 1-12.
6. F. Liu, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.
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. M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images", in Proc. WSCG Conf. 2002, 2002, pp. 303–412
9. Z. Zhou, G. R. Arce, and G. DiCrescenzo, "Halftone visual cryptography", IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
10. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.
11. 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.
12. Zhengxin Fu, Bin Yu, "Research on Rotation Visual Cryptography Scheme", International Symposium on Information Engineering and Electronic Commerce, pp 533-536, 2009.
13. Jonathan Weir, WeiQi Yan, "Sharing Multiple Secrets Using Visual Cryptography", 978-1-4244-3828-0/09, IEEE, pp 509-512, 2009.
14. Xiao-qing Tan, "Two Kinds of Ideal Contrast Visual Cryptography Schemes", International Conference on Signal Processing Systems, pp. 450-453, 2009.
15. E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." Designs, Codes and Cryptography, 11(2) , pp.179–196, 1997.
16. C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes". Designs, Codes and cryptography, 20, pp. 325–335, 2000.
17. R. Youmaran, A. Adler, A. Miri, "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343, 2006.
18. R. Lukac, K.N. Plataniotis, "Bit-Level Based Secret Sharing For Image Encryption", Pattern Recognition 38 (5), pp. 767–772, 2005.

AUTHOR PROFILE

L. N. Pandey completed his master degree in Master of computer application from IGNOU Delhi, India. And currently he is a scholar of Master of Technology (CTA) RGPV University Bhopal India.