Visual Cryptography Schemes Using Secrete Sharing: Survey Report

[1]Shubhangi Rathod, [2]Rahul Jadhav, [3]Dipti Pawade, [4]Harshada Sonkamble
[1]Dept. of IT, P. I. I. T. M. S. R., Navi Mumbai, India
[2]Vishwakarma Institute of Technology, Pune, India
[3,4]Dept. of IT, K. J. Somaiya College of Engineering, Mumbai, India

Abstract

Visual cryptography is a cryptographic technique which encrypt a visual information (e.g. text, handwritten notes and pictures) in such a way that the decryption done by the human visual system. It needs neither cryptography knowledge nor complex computation. For security purposs, it also ensures that hacker cannot obtain any clues about a secret image from individual sharess. Naor and Shamir proposed the basic model of visual cryptography in 1994. Visual cryptography scheme eliminates complex computation problem at the decryption the secret images can be restored by stack operation. The important issue of visual cryptography is quality of relevant image. Performance of visual cryptography scheme depends, such a number of image(single, multiple), types of image(binary, gray, color),share generation(meaningful, meaningless), security, accuracy pixel expansion, complexity,) encrypted by the scheme.

Keywords

We would like to encourage you to list 4 to 5 keywords in this section.

I. Introduction

It is now common to transfer multimedia data via the Internet such as military maps and commercial identifications. While using secret images, security issues should be taken into consideration because, it also ensures that hacker cannot obtain any clues about a secret image from individual shares. The coming era of electronic commerce, there is an urgent need to solve the problem of ensuring information safety in today's increasingly open network environment. The hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various tools of secrete sharing schemes have been developed

Visual cryptography is introduced by first in 1994 Noar and Shamir [1]. Visual cryptography is a cryptographic technique which encrypt a visual information (e.g. text, handwritten notes and pictures) in such a way that the decryption done by the human visual system. Visual cryptography scheme eliminates complex computation problem at the decryption the secret images can be restored by stack operation. In the visual secrete sharing scheme an image is split into n number of shares. When all n shares are combining, the original image would appear. While n-1 share does not provide the information about original image so someone with all n shares.

II. Black And White Visual Cryptography Schemes

A. Secret Sharing

In 1994 the Naor and Shamir [1] proposed the visual cryptographic scheme for secrete sharing which encrypt a visual information in such a way that the decryption done by the human visual system called as Visual Cryptography Scheme (VCS). The simplest Visual Cryptography scheme is given by the following setup. A secret image combination of black and white pixels each pixel operated separately for generating the share. The encoding scheme a binary image can split into two shares. According to table 1 if the pixel is white then one of above two rows is chosen for generating share1 and share2.Similarly if the pixel is black then one of below two rows is chosen for generating share1 and share2. By Naor and Shamir's scheme for encoding a binary pixel into two shares, each share pixel is encoded into two white and two black pixels each share alone gives no clue about the pixel whether that pixel is black or white. Secret image is shown only when both shares are superimposed.

To decode the hidden messages, embedding images can be overlay. Balancing the performance between pixel expansion and contrast Liguo Fang [6] recommend a (2, n) scheme based on permutation. Threshold visual secret sharing schemes combine XOR and OR operation with reversing and based on binary linear error correcting code was suggested by Xiao-Qing and Tan [5].

To encode the secret, we split the original image into n modified versions (referred as shares) such that each pixel in a share now subdivides into m black and white sub-pixels. To decode the image, we simply pick a subset S of those n shares and Xerox each of them onto a transparency. If S is a "qualified" subset, then stacking all these transparencies will allow visual recovery of the secret. Fig. 2, provides an example of such construction. Suppose the secret image "A" is divided into 2 shares. Along with this basic setup, Naor and Shamir also proposed (k, n) threshold model as its extension. This extended scheme is created such that any k shares can be mound together to obtain the original secret, but any k-1 shares do not gain the information about secret.

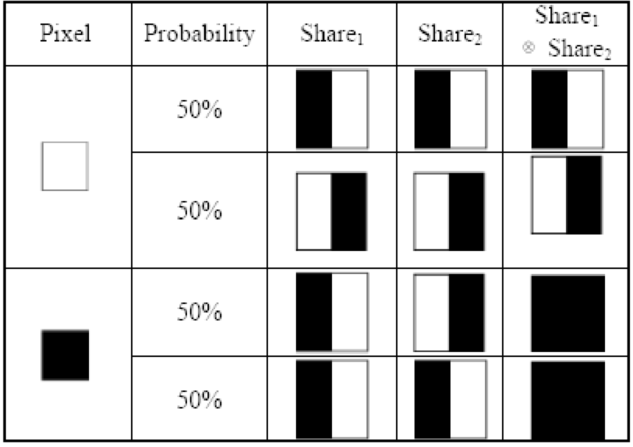


Fig. 1(a): Naor and Shamir's Scheme for Encoding a Binary Pixel Into Two Shares

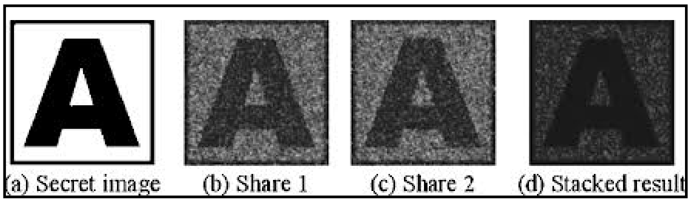

(a) Secret image (b) Share 1 (c) Share 2 (d) Stacked result

Fig. 1(b): Example of Secret Sharing Scheme

III. Gray-Level Visual Cryptography

A. 2-Out-of-Two Scheme

The (2, 2)–VCS scheme is introduce the basic concepts of threshold visual secret sharing schemes. In the encryption process, secret image is divide into two shares, and each share belongs to the corresponding secrete image. In the decryption process, two corresponding shares are mound together to retrieve the secret image. With (k, n) threshold visual cryptography scheme for gray level images using dithering technique, the reduction the reduction size of decrypted image compared to [10] technique is obtain but the quality of decrypted image depends upon the quality of halftone image. The half toning is performed by Adaptive order technique of gray-level image by using a space-filling curve to perform an adaptive variation of the cluster size.

For the encryption [12] using half-toning technique gray level image is changed into approximate binary image or halftone image having pixel value 0 and1. By considering the case of (2, 2) - VCS, the step is divide the secrete image into two shares. For decryption the original image is reconstructed by mound binary shares.

Sandeep Katta[7] proposed Two-out-of-Three Scheme Here he design the shares such a way that when combining any two shares will reveal the original bit information, but not the whole share just half of each single share will give high quality image when reconstructed. He explains this scheme by taking a value from the grayscale block and divides that value into shares.

254: [1 1 1 1 1 1 1 0]

Table 1: Bit Transform from Gray Scale to Binary

share	1st half	2nd half
Share 1	01010100	11011010
Share 2	10101010	11101110
Share 3	00100100	10010100

```
Share1 (1st half): 0 1 0 1 0 1 0 0
Share2 (1st half): 1 0 1 0 1 0 1 0
                    --------------------
                      1 1 1 1 1 1 1 0 = 254

Share3 (1st half) : 0 0 1 0 0 1 0 0
Share1 (2nd half): 1 1 0 1 1 0 1 0
                   -------------------
                    1 1 1 1 1 1 1 0 = 254

Share2 (2nd half): 1 1 1 0 1 1 1 0
Share3 (2nd half): 1 0 0 1 0 1 0 0
                   -------------------
                    1 1 1 1 1 1 1 0 = 254
```

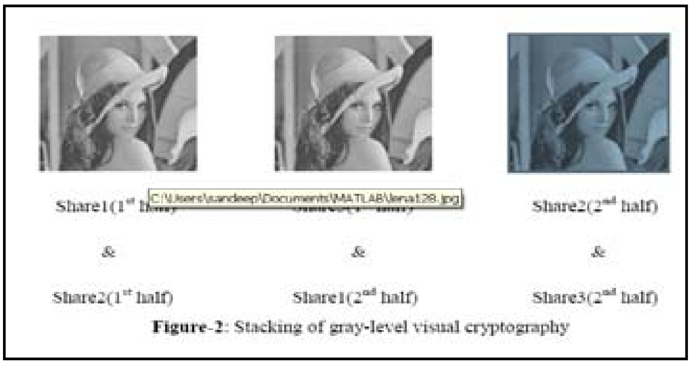


Fig. 2: Example of Gray level Visual Cryptography

Combining any two half shares will give exact bit and by doing the same procedure for the whole grayscale block gives perfect high quality image when reconstructed without any loss of contrast.

IV. Visual Cryptography for Color Image

A. 2 out of Two secret Sharing Schemes

Until the year 1997 visual cryptography schemes were applied to only black and white Images. Color visual cryptography becomes an interesting research topic after the formal introduction of visual cryptography by Naor and Shamir in 1995. First colored visual cryptography scheme was developed by Verheul and Van Tilburg [10].The idea is to hide a secret message (text, , picture, etc…) in different images called shares or cover images. Each share carries some information which does not reflect any information directly. the decryption of the secret image requires neither the knowledge of cryptography nor complex computation.

In this scheme the input images (original image) allow to share a secrete massage among group of participant such a way that decryption is done with all share. If any one of share is not present then reconstruction of original images is not done .In this scheme [9] the Input image divide secret information into exactly 2 shares. When these two shares are observed separately, no one can reveal the secret information. Among this two share one act as a encrypted text (cipher text) and other is a secrete key. The single pixel is divided into 4*4 matrix(Figure) Encoding of original can be done using horizontal pixels, vertical pixels or diagonal pixels The original image is reconstructed by superimposing two output share(cipher text and key) on transparency together. This is X-OR operation between the shares to obtain the secrete information. The input image provide RED, GREEN, BLUE and ALPHA components of each pixel using algorithm and these three components are used to generate the shares using2 out of 2 secret sharing scheme. 32 bit pixel divided into four parts red, green, and blue, alpha each with 8 bit alpha part represented degree of transparency.

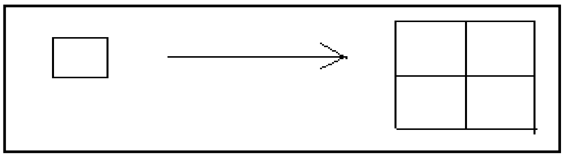


Fig. 3: Pixel Expansion

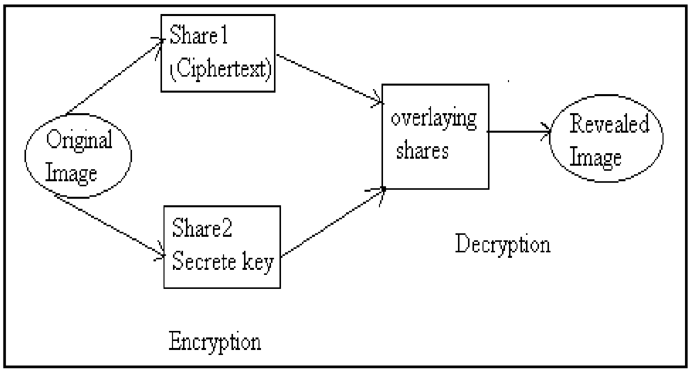
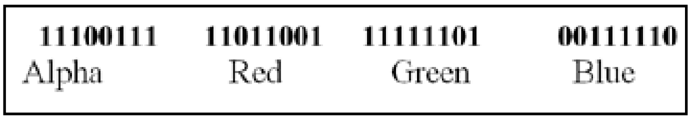


Fig. 4: 2 Out of Two Secrete Sharing Scheme

A 32 bit sample pixel is represented in the following [8]



11100111	11011001	11111101	00111110
Alpha	Red	Green	Blue

Fig. 5: Structure of 32 Bit Pixel

Example: [11]

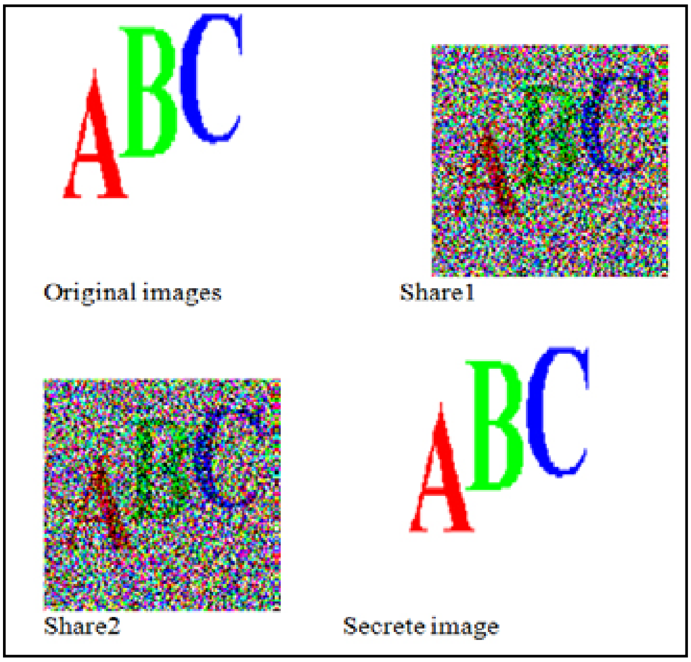


Fig. 6: Example of Color Visual Cryptography

V. Conclusion

In this paper the authors provide a brief review survey of visual cryptography schemes is studied and their performance is evaluated on the basis of secret sharing methods among participants. The secrete sharing method uses the two share visual cryptography scheme it eliminates complex computation problem at the decryption the secret images can be restored by stack operation. The various advantages of VCS is provided in private as well as public sector, because VCS is totally based on human visual system. The (2,2) secrete sharing scheme is extended for generating multiple shares rather than generating two share for secrete image.

References

[1] Moni Naor, Adi Shamir,"Visual Cryptography", Advances in cryptology, 1995.

[2] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare,"Survey of Visual Cryptography Schemes", International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010

[3] Young-Chang Hou,"Visual cryptography for color images", National Central University, Jung Li, Taiwan 320, ROC Received 6 June 2002, Accepted 26 August 2002

[4] JIM CAI,"A short survey on visual cryptography schemes".

[5] Xiao-qing Tan,"Two Kinds of Ideal Contrast Visual Cryptography Schemes", International Conference on Signal Processing Systems, pp. 450-453, 2009

[6] Liguo Fang, BinYu,"Research On Pixel Expansion Of (2,n) Visual Threshold Scheme", 1st International Symposium on Pervasive Computing and Applications, pp. 856-860, IEEE.

[7] Sandeep Katta,"Visual Secret Sharing Scheme using Grayscale Images", Department of Computer Science, Oklahoma State University Stillwater, OK 74078

[8] Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara3", Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011.

[9] Pallavi V. Chavan R. S. Mangrulkar,"Encrypting Informative Color Image using Color Visual Cryptography", Third International Conference on Emerging Trends in Engineering and Technology.

[10] E. Verheul, 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.

[11] Ms. KIRAN KUMARI, Prof. SHALINI BHATIA,"Multi-pixel Visual Cryptography for color Images with Meaningful Shares", International Journal of Engineering Science and Technology, Vol. 2(6), 2010, pp. 2398-2407

[12] Nagaraj V. Dharwadkar, B.B. Amberker, Sushil Raj Joshi,"Visual Cryptography for Gray-Level Image using Adaptive Order Dither Technique", Journal of Applied Computer science, No. 6 (3) /2009, Suceava.