IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 4) Pages (85-94)

Journal home page: www.ijreb.org

VISUAL CRYPTOGRAPHY SCHEMES FOR COLOR IMAGES – A SURVEY

D.R. Denslin Braja[1] and V.S.Dharun[2]

1Assistant professor, Department of Information Technology, Noorul Islam University Kumaracoil, Tamilnadu

2 Head of the Department, Department of Biomedical Engineering, Noorul Islam University Kumaracoil, Tamilnadu

ABSTRACT

Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex traditional cryptography algorithms. This technique allows audio, video, image, text etc to be encrypted so that decryption can be performed by the human visual system with no need of complex cryptographic algorithms. In this technique a secret image is encrypted into shares using visual cryptographic schemes. Stacking these shares reveals the secret image. Shares are usually presented in transparencies. This paper provides an overview of emerging techniques in color visual cryptography and analysis these schemes basis of number of secrets, pixel expansion, image format and type of shares generated.

KEYWORDS: Visual cryptography, pixel expansion, contrasts

IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 4) Pages (85-94)

Journal home page: www.ijreb.org

I. INTRODUCTION

With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed. Cryptography is the study of mathematical techniques related aspects of Information Security such as confidentiality, data security, entity authentication and data origin authentication, but it is not the only means of providing information security, rather one of the techniques.

Visual cryptography is a technique which provides information security. In traditional cryptography uses complex, computationally intensive algorithms for encryption and decryption. But in visual cryptography schemes generate shares and apply simple algorithm for encryption, and for decryption there is no need of any algorithm, simply stacking shares reveals original image. Shares are usually presented in transparencies. Some important goals while developing a visual cryptography is to have (i) optimum number of shares, (ii) good quality of reconstructed image and (iii) keeping the size of share small.

In 1994, Naor and Shamir [1] introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS). In this a secret image consists of a collection of black and white pixels where each pixel is treated independently. To encode the secret, 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, 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.

To illustrate basic principles of Visual Cryptography scheme, consider a simple (2, 2)-VC scheme in Fig. 1. Each pixel p from a secret binary image is encoded into m black and white subpixels in each share. If p is a

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

white (black) pixel, one of the six columns is selected randomly with equal probability, replacing p. Regardless of the value of the pixel p, it is replaced by a set of four subpixels, two of them black and two white. Thus, the subpixel set gives no clue as to the original value of p. When two subpixels originating from two white p are superimposed, the decrypted subpixels share two white and two black pixels. On the other hand, a decrypted subpixel having four black pixels indicates that the subpixel came from two black p pixels [5].

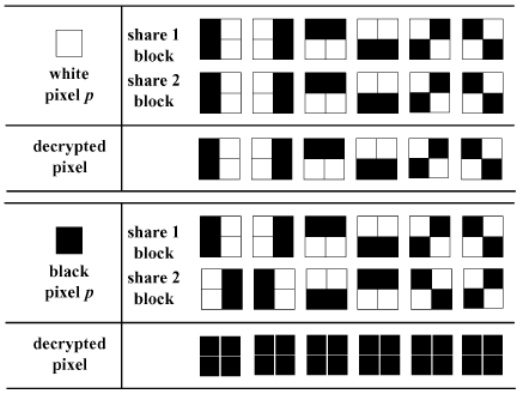

Fig 1: (2,2) Visual cryptography scheme

Wen-HsiangTsai [2] proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares.

Zhi Zhou, Arce G.R., Di Crescenzo G. [3] proposed a general framework of halftone visual cryptography. A halftone image is made up of a series of dots rather than a continuous tone. Applying the rich theory of blue noise halftoning into the construction mechanism of conventional VC, the proposed method generates visually pleasing halftone shares carrying significant visual information. It can be broadly used in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash, etc.

II. VCS FOR COLOR IMAGES

The requirement of encrypting natural image makes researchers focus on the VCS schemes for color images. In [16], Hou firstly proposed three methods for encrypting color images. In his paper, he proposed three methods for gray-scale and color images based on black-and-white visual cryptography, halftone technology, and color decomposition method. His methods have the backward compatibility with the black-and-white visual cryptography and can be easily applied to gray-

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

scale and color images. Subtractive model is used in all the methods.

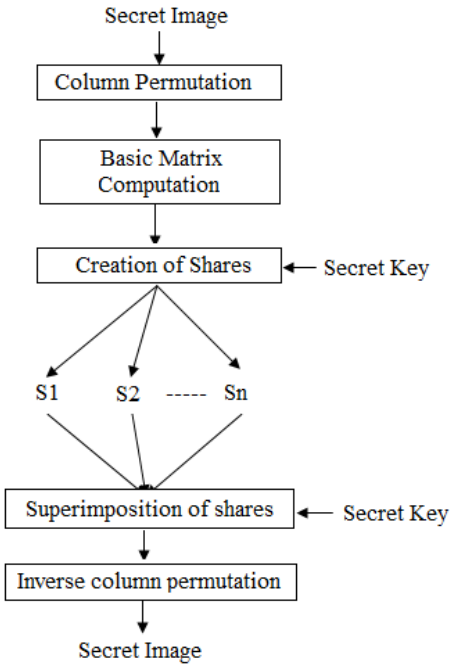

Fig 2: Visual cryptography model

The original colored image is firstly be decomposed into three primary-color images under the subtractive model, namely, *C* (Cyan), *M* (Magenta) and *Y* (Yellow). The size of the three images is equal to that of the original one. Then each primary-color image is dithered so that each image will have two color levels. Dithering is a technique used to create an illusion of color depth in images with limited color palette. The principle is to pack pixels in higher density for representing darker colors and distribute the pixels sparsely for representing lighter colors. Each pixel is mapped to a 2£2 block which consists of two black pixels and two white pixels. To generate the *C*, *Y* and *M* shares, the dithered *C*, *M* and *Y* primary-color images of the original secret image are scanned pixel by pixel.

This paper provides an overview of emerging techniques in color visual cryptography in detail.

A. Progressive Visual Cryptography

In traditional Color Visual Cryptography, loss of contrast makes VCS practical only when quality is not an issue, which is quite rare. The application of digital half toning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. Young-Chang Hou and Zen-Yu Quan [8] proposed a new encoding method that enables us to transform gray-scale and color images into monochrome ones without loss of any information. Incorporating this new encoding scheme into visual cryptography technique allows perfect recovery of the secret grayscale or color image. When more than one share is stacked together, the hidden information will appear little by little. Only a sketch will be recovered when a few shares are

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

being stacked and more details will be recovered when more shares are being stacked. Along with the increase of the shares, the hidden information will be recovered progressively.

B. Regional Incrementing Visual Cryptography

Shyong Jian Shyu and Hung-Wei Jiang[12] proposed region incrementing visual cryptography scheme (RIVCS). It deals with the sharing of an image consisting of multiple regions with different secrecy levels, which can be incrementally revealed as the number of shares increases. The linear programming concept is used to construct n-regions in RIVCS. The object function aims at minimizing the pixel expansion subject to the constraints satisfying the region incrementing requirements. Unit matrices are introduced as the building blocks and the numbers of the unit matrices chosen to form the basis matrices of *n*-RIVCS are set as the decision variables.

The 'n' level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares with the following features:

(a) Each share cannot obtain any of the secrets in S,

(b) Any t(2<t<n+1) shares can be used to reveal (t-1) levels of secrets

(c) the number and locations of not-yet revealed secrets are unknown to users,

(d) all secrets in S can be disclosed when all of the (n+1) shares are available.

C. Extended Visual Cryptography Algorithm

To hide secret images noise-like random random pixels on shares are generated by conventional visual secret sharing schemes. These method dealers cannot visually identify each share. This problem is overcome by the extended visual cryptography scheme (EVCS). Here we add a meaningful cover image in each share. The previous approaches involving in the EVCS under goes the pixel expansion problem. Further a code book design for various schemes is needed in VC based approach. To solve these problems the general approach is used for binary secret images in non computer-aided decryption environments. It includes two phases, where we construct meaningless shares using an optimization technique and cover

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

images are added in each share directly by a stamping algorithm.

D. Color Extended Visual Cryptography

It relies on two fundamental principles used in the generation of shares, namely, error diffusion and visual information pixel (VIP) synchronization. InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee [11], proposed color extended visual cryptography using error diffusion method. Error diffusion is a simple but efficient algorithm for images halftone generation. The quantization error at each pixel is filtered and fed to future inputs. The error filter is designed in such a way that the low frequency differences between the input and output images are minimized and consequently it produces pleasing halftone images to human vision.

Synchronization of the VIPs across the color channels improves visual contrast of shares. In color VC schemes, the colors of encrypted pixels and the contrast can be degraded due to random matrix permutation. VIP synchronization prevents the color and contrast of original images from degradation even with matrix permutation.

A. Visual Cryptograms of Random Grids

In 2013, Shyong Jian Shyu[16], proposed visual secret sharing for general access structures by using visual cryptograms of random grids (VCRG). Two effective algorithms (Γ_0 and Z_M) are used to produce a set of VCRG. So that the members in each qualified set can reconstruct the secret image by superimposing their shares. One algorithm based on Γ_0 to produce a set of (Q_j,Q_j) VCRG for each Qj€ Γ_0 and distribute the constituent shares according to the inclusion matrix. Another algorithm focused on Z_M by generating a set of (Z_M,Z_M) VCRG and dispatching the universal shares according to the exclusion matrix.

III. ANALYSIS OF VISUAL CRYPTOGRAPHY SCHEMES

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir[1] suggested two main parameters: pixel expansion m and contrast. Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast is the relative

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

difference in weight between combined shares that come from a white pixel and a black pixel in the original image.

In progressive visual cryptography [8], is a novel scheme with unexpanded pixels. In this scheme the probability to appear as a black pixel is only 1/*n* on each share, which guarantees the security of the information. When any *k* (*k* = 2 − *n*) shares are stacked, the probability of appearing black pixels on the stacked shares increases to *k/n*; while for the white pixels, the probability of appearing as black pixels remains 1/*n*. That is to say we can get a contrast of (*k*−1)/*n* on the stacked image. After stacking all shares, black regions of the secret image could be completely reconstructed and the contrast between white and black rises to (*n* − 1)/*n*, which is better than the conventional VC that can only obtain 50% contrast. The stacked image, therefore, could be easily recognized by human eyes without any difficulties.

In RIVC scheme [12] ,the number of secrets that can be revealed is proportional to the number of participants engaged in the decoding process. The contrasts of different secret regions can also be designated in the constraints. This enhances the adaptability and flexibility of RIVCS in practical applications.

Extended visual cryptography algorithm [13]needs extra pixel expansion in addition to m. It requires 2n pairs of collection of nxm' binary matrices$\{C_0^{c1,\ldots,cn}, C_1^{c1,\ldots,cn}\}$ to encrypt meaningful shares for n participants, where m′ is the pixel expansion of the black and white (k,n). Each matrix has rows having predefined contrast differences in accordance with bit values $c_1,\ldots,c_n$ of original images. In this the display quality of the recovered image is near to that of conventional visual cryptography scheme.

In color extended visual cryptography[11], pixel expansion is only m. This feature reduces needless space for one pixel encryption and finally produces shares with as less as possible pixel expansion. There is no need to save all 2^n pairs of matrices of size n x m' ahead of the encryption stage, but need space for only two matrices S_0 and S_1. It generates high quality of meaningful color shares as well as the colorful decrypted share with as less as possible pixel expansion.

The approach of visual cryptograms of random grids[16], reduce the pixel expansion

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

and the light contrasts of a particular qualified set derived from the two algorithms (Γ_0 and Z_M) may be different. But, the ability of reconstruction is not perfect, due to small white region might be reconstructed as black region. To obtain a higher contrast choose the members in Z_M is quite small or the members in Γ_0 constitute a partition of p.

Table 1. Comparison of visual cryptography schemes

Sl No	Authors	Year	No. of secrets	Pixel expansion	Image format	Type of shares generated
1	Naor and Shamir[1]	1995	1	m	Binary	Random
2	Wen and Chang [2]	2002	1	9	Gray	Meaningful
3	Zhi Zhou,Gonzalo [3]	2006	1	m	Color	Random
4	Young and Zen-Yu [8]	2011	1	1	Color	Random
5	InKoo Kang, Gonzalo [11]	2011	1	m	Color	Meaningful
6	Shyong and Wei Jiang [12]	2012	n	1	Color	Random
7	Young and Zen-Yu [13]	2012	n	log2C·m	Color	Random
8	Shyong Jian Shyu[16]	2013	n	1	Color	Meaningful

IV. CONCLUSION

This paper discusses the different visual cryptography schemes for color images. In order to hide the secrecy we go for expansion and increasing the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Visual cryptography can be applied for copyright for images, access control to user images, Visual authentication and identification any kind images of images like (normal or digital). This paper compares various visual cryptography schemes in terms of security, quality of images, contrast, and reliability of images. Hence research in VC is towards maintaining the contrast at the same time maintaining the security.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

[2] Chang-Chou Lin , Wen-Hsiang T sai,"Visual cryptography for gray-level images by dithering techniques", Pattern Recognition Letters, v.24 n.1-3.

[3] Sudharsanan S," Shared key encryption of JPEG color images", IEEE Transactions on Consumer Electronics, Volume: 51 , Issue: 4, 2005 , Page(s): 1204 – 1211.

[4] Zhi Zhou,Gonzalo R. Arce, and Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing, Vol. 15, No. 8, August 2006.

[5] Zhongmin Wang, Gonzalo R. Arce, and Giovanni Di Crescenzo," Halftone Visual Cryptography Via Error Diffusion", IEEE Transactions on Information Forensics And Security, Vol. 4, No. 3, September 2009.

[6] Feng Liu, Chuankun Wu and Xijun Lin," Step Construction of Visual Cryptography Schemes", IEEE Transactions on Information Forensics And Security, Vol. 5, No. 1, March 2010.

[7] Ran-Zan Wang and Shuo-Fang Hsu," Tagged Visual Cryptography", IEEE Signal Processing Letters, Vol. 18, No. 11, November 2011.

[8] Young-Chang Hou and Zen-Yu Quan," Progressive Visual Cryptography with unexpanded Shares", IEEE Transactions on Circuits And Systems For Video Technology, Vol. 21, No. 11, November 2011.

[9] Shyong Jian Shyu and Ming Chiang Chen," Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes", IEEE Transactions on Information Forensics And Security, Vol. 6, No. 3, September 2011.

[10] Pei-Ling Chiu and Kai-Hui Lee," A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes", IEEE Transactions On

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (85-94)
IJREB
Journal home page: www.ijreb.org

Information Forensics And Security, Vol. 6, No. 3, September 2011.

[11] InKoo Kang, Gonzalo R. Arce, and Heung-Kyu Lee," Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on Image Processing, Volume: 20 , Issue: 1 , 2011 , Page(s): 132 – 145.

[12] Shyong Jian Shyu and Hung-Wei Jiang," Efficient Construction for Region Incrementing Visual Cryptography", IEEE Transactions on Circuits and Systems For Video Technology, Vol. 22, No. 5, May 2012.

[13] Kai-Hui Lee and Pei-Ling Chiu,"An Extended Visual Cryptography Algorithm for General Access Structures", IEEE Transactions on Information Forensics and Security, Volume: 7, Issue: 1 , 2012 , Page(s): 219 – 229.

[14] Mitsugu Iwamoto," A Weak Security Notion for visual Secret Sharing Schemes", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.

[15] Sian-Jheng Lin and Wei-Ho Chung," A Probabilistic Model of Visual Cryptography Scheme with Dynamic Group", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, February 2012.

[16] Shyong Jian Shyu, "Visual cryptograms of Random Grids for General Access Structures", IEEE transaction on Circuits and Systems for Video Technology, Vol.23, No.3, March 2013.