www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9, September 2014 Page No. 8372-8376

Survey of Visual Cryptography Schemes without Pixel Expansion

Asst. Prof. Jyoti Rao[1], Dr. Vikram Patil[2], Ms. Smita Patil[3]

Dr.D.Y.Patil Institute of Engineering and Technology, Pimpri, Pune-18[13]
Sanjeevan Engg & Tech Institute, Sanjeevan Knowledge city, Panhala, Kolhapur-India[2]
[1]jyoti.aswale@gmail.com
[2]vikrams.patil@gmail.com
[3]smita.khot85@gmail.com

Abstract: ***The basic idea of the Visual Cryptography is to encrypt a secret image into n number of meaningless share images. The Visual Cryptography technique cannot leak the encrypted information of the shared secret by virtue of any combination of the n share images combined together. This share images are printed on separate transparencies and distributed as shares such that, when the share images are superimposed, the concealed secret image is discovered. Thus, the human visual system can recognize the shared secret image without using any computational devices. There is no need of cryptography knowledge and complex computation. The traditional visual secret sharing scheme uses a pre-defined pattern book to generate shares, which leads to a pixel expansion problem on share images. Basically, the performance of visual cryptography scheme depends on different measures like pixel expansion, security, contrast, computational complexity, accuracy, share generated, number of secret images and type of secret images encrypted by the scheme. Objective of this paper is on study and performance analysis of the visual cryptography schemes without pixel expansion, number of secret images, type of the image and type of shares generated (meaningless or meaningful).***

Keywords: cryptography, image processing, visual secret sharing scheme, Contrast, Pixel expansion, Image security.

1. Introduction

In today's competitive world of Liberalization, Privatization and Globalization, every field has already become computerized and technologically advanced for sharing secret images, the best possible way with less effort. Visual cryptography is basically a cryptographic technique which encrypts visual information like pictures, text, etc. in such a way that decryption process becomes a mechanical operation that does not require computational devices. Naor and Shamir developed Visual Cryptography technique, in 1994. They demonstrated a visual secret sharing scheme, where an secret image was split up into n shares so that only someone with all n shares could decrypt the secret image, while any n − 1 shares discovered no information about the original secret image. The shares were printed on a separate transparency, and decryption was performed by superimposing the shares. When all n share images were overlaid, the original secret image would recovered. The fundamental properties of Visual Cryptography are Pixel expansion, Contrast and Security. A basic 2-out-of-2 or (2, 2) visual cryptography scheme produces 2 share images from an original secret image and must stack both share images to reproduce the original secret image [6].

Generally, a (k, n) threshold VC scheme produces n share images and only requires combining k share images to recover the original secret image. Each pixel in the original secret image can be interchanged in the share images by a 2 × 2 block of sub pixels ,to reserve the aspect ratio for the recovered secret image for a (2, 2) scheme.

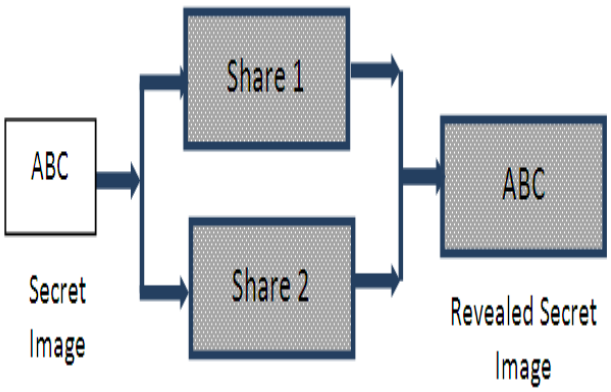

Figure 1: Example of Traditional Visual Cryptography

In general, pixel expansion and luminance difference are two most important properties used to measure the efficiency to a VC scheme, the pixel expansion refer to the number of pixels

in a share used to encode a pixel of the secret image, and the contrast is the luminance difference between the area of black pixels and the area of white pixels in the stacked image. Smaller pixel expansion and higher contrast are considered good properties for a VC scheme, and are the mainly research topics in VC. In traditional visual cryptography schemes the generated share images has less contrast and the size of reconstructed image is large. The generated share images are meaningless and also the time required for construction of share image is large. It is observed that these are some shortcomings of existing visual cryptography. In traditional VSS schemes, the size of the share image is significantly stretched since each pixel of the secret image is mapped onto a block consisting of a number of pixels. In addition, the quality of the reconstructed secret image is normally violated in contrast, mainly for halftone images.

The above figure1 shows the example of traditional visual cryptography scheme which leads to pixel expansion. This paper provides summary of various visual cryptography schemes. Taking limited time and space complexity into consideration two criteria pixel expansion and number of share images encoded is of importance. Smaller pixel expansion results in smaller or same size of the share image. Encoding multiple secret images into the same share images requires less overhead while sharing multiple secrets. The security issues over the communication channels avoid attention of hacker considering meaningful shares. Gray and color image format should be encoded by the VC schemes to meet the demand of today's multimedia information. Other performance measures such as contrast, accuracy, security and computational complexity that affect the efficiency of visual cryptography are also discussed in this paper.

2. Black and White VCS without Pixel Expansion

The (n, n)-threshold visual secret sharing scheme, proposed by Naor and Shamir (1995), is used to share one secret image on n share images. The secret image is encrypted into n share images of which every one of the n share images is a meaningless random image and cannot reveal the secret image with n-1 share images. By stacking n share images together, the hidden secret image is revealed and can be recognized by the human visual system without any computation. The basic idea of visual cryptography can be illustrated with the traditional 2-out-of-2 scheme. In the (2, 2) scheme, every secret pixel of the image is converted into two share images and recovered by simply stacking two shares together. This is equivalent to using the OR operation between the shares. In this scheme, 4 sub pixels are generated from each pixel of the secret image in a way that 2 sub pixels are white and 2 are black. The sub pixels for each share are selected randomly. When a pixel from the original image is white, one of the six possible combinations of patterns are randomly selected to encode the pixel into 2 shares. Table 1 demonstrates encoding process. To reveal the binary secret image both shares are needed. After superimposing the two share images the original secret image is produced. The Naor and Shamir's VSS scheme uses pixel mapping technique, so that pixel expansion exists in their scheme [4].

In multilevel VSS scheme, which maps a block in a secret image onto one corresponding equal-sized block in each share image with no image size expansion. In this system they have implemented two types of techniques, including histogram width-equalization and histogram depth-equalization, are proposed to generate the consistent share blocks containing multiple levels rather than two levels based on the density of black pixels on the blocks for a secret block. In the visual secret sharing scheme, the gray-scale image histogram is obtained by evenly separating the range of the pixel, gray levels in the secret image, while in the latter the lots are created, so that the area of each bucket is approximately constant by containing the same number of pixels. It significantly improves the quality of the reconstructed secret image compared to several previous investigations. The histogram depth-equalization technique provides a better quality of reconstructed secret image than the histogram width-equalization technique, especially for an image with most of its pixel gray-scales ranging only within a small interval [1].

Wu and Chang (2005) were first researchers to advice a VSSM scheme with two circle share images, S1 and S2, which allow the rotation angle to be a factor of 360°.The rotation is not limited to 90°, 180° and 270° As in Wu and Chen's scheme, the sub-block used to create share images S1 and S2 consists of 4 sub-pixels but with different pattern types. There are 4 basic patterns in which each pattern of two white pixels and two black pixels is used to create share image S1. The sub-block used to create share image S2 consists of one white pixel and 3 black pixels. According to the corresponding pixel pair (pSE1, pSE2) on two secret images (SE1, SE2) and sub-block b1 selected from the 4 basic patterns, the pattern of b2 can be defined. Although, Wu and Chang improved the rotation angle so it was not limited to 90°, 180° and 270°, the critical pixel expansion problem, as in Wu and Chen's scheme (Wu & Chen, 1998) still exists [3].

N. Askari, H.M. Heys, and C.R. Moloney proposed in 'Extended Visual Cryptography Scheme with Preprocessing Halftone Images' two methods Simple Block Replacement (SBR) and Balanced Block Replacement (BBR). Straightforward approach and Very effective for unprocessed binary secret images which have large number of all white and black blocks these are some advantages of this SBR and BBR methods. The disadvantages of this methods are poor contrast, being darker than the original image, causes the loss of many fine details in the images. The Balanced Block Replacement method uses the concept of candidate block 'CB' which consists of block of two white and two black pixels. It improves the visual quality of the processed image. The BBR method tries to keep the local ratio of black to white pixels in the processed image close to the local ratio of black to white pixels in the original halftone secret image. The algorithm used for BBR method is as follows: a) the secret image is processed into halftone image, b) divide the image into four overlapping clusters each containing four secret block, c) compute no. of black pixels for each cluster and save in a template, d) leaving only black, white or candidate block other blocks are converted into black pixels, e) turned the candidate block into black or white block, based on the smallest difference between the threshold and no. of black pixels, f) Repeat the step (e) for remaining clusters and get the final processed image[6].

3. Color VCS without Pixel Expansion

The color models, additive and subtractive are widely used to describe the constitutions of colors. In the additive color model, the three primary colors are red, green, and blue (RGB), with desired colors being obtained by mixing different RGB channels. By controlling the intensity of red, green, blue channels, it can modulate the amount of red, green, blue in the compound light. The more the colors are mixed, the more the brightness of the light. When mixing all red, green and blue channels with equal intensity, white color will result. The computer screen is a good example of the additive color model. In the subtractive model, color is represented by applying the combination of colored-lights reflected from the surface of an object. By mixing cyan, magenta and yellow pigments, we can produce a wide range of colors. The more the pigments are added, the lower the intensity of the light is and, thus, the darker the light is. This is the reason it is called the subtractive model. Cyan, magenta, and yellow are the three primitive colors of pigment which cannot be composed from other colors [12].

The halftone technique is used to produce binary images for processing gray-level and color secret images. In color visual secret sharing scheme the general k-out-of-n threshold setting and dithering is required for preprocessing the original image. In 2005, Hou and Tu developed new color VC technique using multi-pixel encoding method [9]. This scheme also supports k-out-of-n threshold setting with no pixel expansion. Dithering is still required for preprocessing the original image before secret sharing. The k-out-of-n threshold VCS for color images in this scheme supports original images of any number of color levels. It is assume that without any loss the color of the original image is represented by the conventional 24-bit color primitives, R (red), G (green) and B (blue), each has 256 levels (i.e. 8-bits). For each pixel of the original secret image, the color quality is represented by three bytes of values; and each byte specifies the intensity of the corresponding color primitive: R, G and B. The scheme is divided into four parts Histogram Generation, Color Quality Determination, Grouping, and Share Creation. In the Histogram Generation three histograms representing the intensity distribution of R, G and B color primitives of the original image are first generated. In the histogram for R (resp. G or B), the horizontal axis represents the intensity of R (resp. G or B) ranging from 0 to 255; and the vertical axis represents the number of pixels of each intensity value. In the Color Quality Determination the user choose the number of intensity levels that the reconstructed secret image will have. The user is to determine this intensity level with the purpose of maximizing the quality of the reconstructed image. In Grouping for each color primitive histogram is created with the boundary color intensity between every pair of adjacent groups. At last in the Share Creation the secret shares are created which are of same size as that of original color secret image [9].

In the conventional Visual Cryptography a pixel expansion problem, or an uncontrollable display quality problem for recovered images, and lacks a general approach to construct visual secret sharing schemes. General and systematic approach to remove these issues is without sophisticated code design book. Thus, to avoid pixel expansion a set of column vectors are designed to encrypt secret pixels rather than using the conventional VC-based approach. To find the column vectors for the optimal VC construction a simulated-annealing-based algorithm is developed which solves the problem of pixel expansion. The existing VC schemes can be divided into two categories like threshold access structure and general access structure. The GAS enables to define reasonable combinations of shares as decryption conditions rather than to specify the number of shares. Koga proposed a general formula to find the basis matrices for (k,n)- VCSs by the exhaustive search method; its objective were to both maximize the contrast and minimize the pixel expansion [12].It is the first solution which formulate the construction problem solved by using optimization techniques without individually redesigning codebooks or basis matrices.

4. Performance Analysis of Visual Cryptography Schemes without Pixel Expansion

The performance of visual secret sharing scheme is basically measured by pixel expansion, quality of the revealed secret image, complexity of the VC scheme and contrast. In multilevel (k, k) VSS scheme two types of techniques called histogram width-equalization and histogram depth equalization are used. This scheme uses BASIS_MATRIX algorithm for encoding a secret block into share blocks. So the original secret image, reconstructed secret image and each share image have the same size. The security analysis of multilevel visual secret sharing scheme is good and also the quality analysis is satisfied for sharing secret over communication media without any computational devices.

In traditional VSS scheme generally two basis matrices are employing known as CP_B for black pixels and CP_W for white pixels. The contrast is obtained by taking difference between the probability that a black pixel on reconstructed secret image is generated from a white pixel on the secret image and the probability that a white pixel on reconstructed secret image is generated from a black pixel on the secret image. In Extended Visual Cryptography Scheme with Preprocessing Halftone Images two methods Simple Block Replacement (SBR) and Balanced Block Replacement (BBR) are used to share secret image. Straightforward approach and Very effective for unprocessed binary secret images which have large number of all white and black blocks these are some advantages of this SBR and BBR methods. The disadvantages of this methods are poor contrast, being darker than the original image, causes the loss of many fine details in the images. Compared with other VCS, the threshold visual secret sharing scheme for color images does not need to preprocess original image such as dithering, which would degrade the quality of reconstructed images. Also, the scheme does not have pixel expansion. Yang-Chen's [10] scheme also uses the probabilistic method and support color images. It has a fixed expansion rate 3. The scheme does not support tunable color levels for the reconstructed images [11]. The model of SIVCSs eliminates the disadvantages of the pixel-expansion problem from which conventional VC scenarios suffer. This method guarantees the blackness of black secret pixels which improves the display quality of the worst-case image [12].

Table -1: Different VSS scheme's with pixel expansion

Visual Secret Sharing Schemes	No. of Secrets	Pixel expansion	Shape of share image
Wu and Chen's scheme Wu and Chen(1998)	2	4	Square
Wu and Chang's scheme Wu and Chang(2005)	2	4	Circle
Shyu et al.'s scheme Shyu et al.(2007)	>=2	2x	Circle
Feng et al.'s scheme Feng et al.(2008)	>=2	3x	Cylinder
Xiaoyu Wu et al.'s scheme (2009)	1	1	Square
Tsung-Leih Lin, Horng,Lee,Chen et al.(2010)	2	1	Rectangular

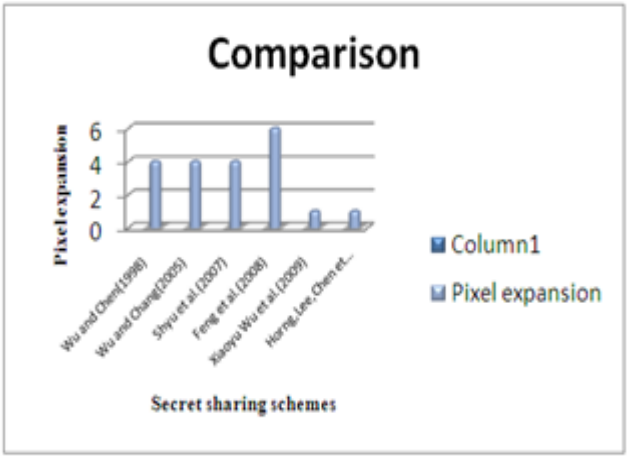

Chart -1: Graphical Representation of VSS schemes.

In the above Table 1 different Visual Secret Sharing Scheme's with number of secrets, shape of share image and pixel expansion exist in the scheme is shown and chart 1 is the graphical representation of VSS scheme's with pixel expansion.

5. Conclusion

In this paper various visual secret sharing schemes without pixel expansion are studied and their performance is evaluated on the basis of quality of reconstructed secret image. In the MLVSS the size of share image is small and the meaningless. So that security aspect is achieved. The goal of Block replacement method is less construction time for generation of share images in EVCS. The incorrect color problem is also eliminated in implementation of RIVCS without pixel expansion scheme. Most of the schemes discussed achieve the high contrast of the revealed secret image. In threshold VCS with color images the problem of arbitrary number of colors and preprocessing of original image is solved. It also supports k-out-of-n threshold setting and 'tunable' number of color levels in the secret share creation process. In Novel VSSS multiple secrets are shared with no pixel expansion and without using codebook to encrypt the secret images. To reveal the secret image no other devices were needed, just two share images are stacked and the original secret image is recovered. The share images in this scheme are meaningless so confirmed to the security rule of visual secret sharing scheme.

References

[1] Chen, Y. F., Chan, Y. K., Huang, C. C., Tsai, M. H., Chu, Y. P. (2007). "A multiple-level visual secret-sharing scheme without image size expansion" Information Sciences, 177, 4696-4710.

[2] Iwamoto, M., & Yamamoto, H. (2003). "The optimal n-out-of-n visual secret sharing scheme for gray-scale images" IEICE Transaction Fundamentals, E86-A (10), 2238-2247.

[3] Lin, Horng, Lee, Chiu, Kaoand, Chen." A novel visual secret sharing scheme for multiple secrets without pixel expansion", ELSEVIER journal 2010 0957-4174

[4] M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptology, 1994, vol. 950, LNCS, pp. 1-12

[5] N. Askari, C. Moloney and H.M. Heys "A Novel Visual Secret Sharing Scheme without Image Size Expansion ", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Montreal, pp. 1-4, 2012

[6] N. Askari, H.M. Heys, and C.R. Moloney "An extended visual cryptography scheme without pixel expansion for halftone images", 2013, 26th IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) 978-1-4799-0033

[7] Shyu, S. J., Huang, S. Y., Lee, Y. K., Wang, R. Z., & Chen, K. (2007). "Sharing multiple secrets in visual cryptography" Pattern Recognition, 40, 3633-3651.

[8] Yang, C. N., & Chen, T. S. (2008). "Colored visual cryptography scheme based on additive color mixing" Pattern Recognition, 41, 3114- 3129.

[9] Y.C. Hou and S. F. Tu, "A visual cryptographic technique for chromatic images using multi-pixel encoding method," Journal of Research and Practice in Information Technology, vol. 37, no. 2, pp. 179–191, May 2005.

[10] C. N. Yang and T. S. Chen, "Colored visual cryptography scheme based on additive color mixing," Pattern Recognition, vol. 41, no. 10, pp. 3114–3129, 2008.

[11] Xiaoyu Wu, Duncan S. Wong, and Qing Li, "Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion", Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09), Huangshan, P. R. China, 26-28,Dec. 2009, pp. 310-315

[12] Inkoo Kang, Gonzalo Arce, Heung-Kyu, "Color Extended Visual Cryptography Using Error Diffusion", Image Processing, VOL. 20, NO. 1, JANUARY 2011