

Refinement of visual secret sharing scheme without image size expansion

Ms. Smita Patil¹, Prof. Ms. Jyoti Rao²

Dr. D.Y.Patil Institute of Engineering and Technology, Pimpri, Pune-18^{1,2}

¹smita.khot85@gmail.com

²jyoti.aswale@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. The share images are printed on transparencies and distributed as shares such that, when the shares are superimposed, a concealed secret image is discovered. The human visual system can recognize the shared secret image without using any computational devices. It needs neither cryptography knowledge nor complex computation. The Visual Cryptography technique for multiple secrets is proposed, which encrypts more than one secret into the equivalent number of share images. The traditional visual secret sharing scheme uses a pre-defined pattern book to generate shares, which leads to a pixel expansion on share images. Thus to minimize the pixel expansion problem in VC scheme a new system is invented which can share two binary secret images on two rectangular share images without pixel expansion. The proposed approach, not only has good contrast, but also has an excellent recovery quality for secret image and the critical problem of pixel expansion is minimized.*

Keywords: Visual secret sharing scheme, Image processing, Pixel expansion, Contrast, Camouflage



1. Introduction

Visual cryptography is a cryptographic technique which allows visual information in the form of pictures, text, etc. to be encrypted in such a way that decryption does not require any computational devices and is done by the human visual system. Naor and Shamir developed one of the best-known techniques known as visual cryptography in 1994. Their research demonstrated a visual secret sharing scheme, where a secret image was split up into 'n' shares so that only someone with all 'n' shares could decrypt the secret image, while any one with less than 'n' shares discovered no information about the original secret image. The shares were printed on a separate transparency, and decryption was performed by stacking operation of the shares. When all 'n' shares were overlaid, the original secret image would be seen.

The fundamental properties of Visual Cryptography are Pixel expansion, Contrast and Security. A basic 2-out-of-2 or (2, 2) threshold visual cryptography scheme produces 2 share images from an original secret image and must stack both share images to reproduce the original secret image. Generally, a (k, n) threshold scheme produces 'n' shares, but only requires combining 'k' shares 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.

As shown in Table 1, if the original pixel is white, from the probability of white pixel, share pixels are randomly created. The possible probability for black pixels is also shown.

Table1: Pattern Book for pixel replacement

Black Pixel				White Pixel			
							
Probability	Expanded sub-block		stacked	Probability	Expanded sub-block		stacked
	s1	s2	s1+s2		s1	s2	s1+s2
1				1			
2				2			
3				3			
4				4			
5				5			
6				6			

After stacking the shares with white transparent and black dense, the original secret image will be discovered. Stacking can be viewed as mathematically ORing operation, where white pixel corresponds to "0" and black pixel corresponds to 1. It is observed that the resulting share images and the recovered secret image contain 4 times more pixels than the original secret image because each pixel of the original image was mapped to four sub pixels. It may also be noted that the recovered image has degradation in visual quality since, the contrast between white and black is minimized since a recovered white pixel is actually comprised of 2 white and 2 black sub pixels, while a black pixel is represented by 4 black sub pixels in the recovered image. The main concern in the proposed method is generation of share images with minimum pixel expansion from the original secret image. It provides a visual quality of

reconstructed image with better contrast and construction time. The encoding is programmed using Java to transform the image into shares such that while decoding stacking sufficient number of shares reveals the secret information. Unlike conventional cryptography no complicated computation is necessary for decryption. This generic system of encoding is very robust incurring very little digression in contrast. Also the image transformation is done by adding two sub pixels to each original pixel but with minimal pixel expansion.

2. Literature Review

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 despoiled in contrast, especially for halftone images. 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 [1]. 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. 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 shares images are meaningless. No one can recognize the secret image by staring at the shared images. The secret image is revealed by stacking the share images. The stacking operation prints n share images on n number of transparencies T_1, T_2, \dots, T_n . T_1, T_2, \dots , and T_n are overlapped together with an appropriate position. It is basically a "OR" operation for the corresponding pixels on transparencies T_1, T_2, \dots , and T_n of share images. According to the color level of the corresponding pixels on T_1, T_2, \dots , and T_n , the color level on the secret image can be revealed by this stacking operation. The digit 1 represents the black color level and digit 0 represents the white color level. If at least one pixel color is black ($=1$), the stacked result pixel is black ($=1$). Obviously, the color level on the stacked transparencies can reveal the secret image by an subtle encrypting method. The encrypting process of Naor and Shamir's VSS scheme is described in this subsection. The Naor and Shamir's VSS scheme uses pixel mapping technique, so that pixel expansion exists in their scheme. Pixel expansion means one pixel may be white or black will be expanded into one sub-block known as a candidate block. The size of the sub-block can be any one size, and pixel expansion is 4 (means $m = 4$), which is an appropriate ratio in realistic implementation [1].

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 previous technique, 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. The proposed schemes significantly improve 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 [3]. Wu and Chang (2005) proposed a VSSM scheme with two circle share images, S_1 and S_2 , which allow the rotation angle to be a factor of 360° . The rotation is not limited to $90^\circ, 180^\circ$ and 270° . As in Wu and Chen's scheme, the sub-block used to create share images S_1 and S_2 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 S_1 . The sub-block used to create share image S_2 consists of one white pixel and 3 black pixels. According to the corresponding pixel pair (pSE_1, pSE_2) on two secret images (SE_1, SE_2) and sub-block b_1 selected from the 4 basic patterns, the pattern of b_2 can be defined. Although, Wu and Chang improved the rotation angle so it was not limited to $90^\circ, 180^\circ$ and 270° , the critical pixel expansion problem, as in Wu and Chen's scheme (Wu & Chen, 1998) still exists [4].

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 [2].

3. Proposed System

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 the generated share images has less contrast and the size of reconstructed image is large. Also the time required for construction of shares is large and the generated share images are meaningless. It is observed that these are some shortcomings of existing visual cryptography. The objective of this proposed system is to design a system for generation of share images with minimum pixel expansion from the original secret image. So that the reconstructed secret image has the properties like-

1. Better contrast ratio

It improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme because pixel expansion is not done, instead of that pixel rearrangement is done.

2. Less construction time

In share generation process as per the number of participants the share images are generated so that the time required to generate the shares is more. But as per the encryption module defined by the proposed system the time required for share generation is less because it uses three different processes in Encryption Module.

3. Size is same as original secret image

This is achieved using a (k, n) secret sharing scheme. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

In this proposed visual secret sharing scheme, there is no pixel expansion and which does not need a pattern book. The proposed visual secret sharing scheme consists of encryption and decryption blocks of module. In encryption block there are three processes as Divide and Separating process, Sticking process and Camouflaging process. Input to the system should be a binary image and through encryption process the share images are generated. These share images are given as input to the Decryption process and secret image is revealed by stacking these share images. If the secret image is color or gray scale image then preprocessing (binary image) is done and then given as input to the encryption process.

Fig1. Shows the complete encryption process, which includes three processes:

3.1 DSP (dividing and separating process)

At the start, two blank share images (i.e., no black pixel) with a size equal to that of the secret image must be generated. Then, each secret image must be divided into M blocks with n x n size, that is $M = (h/n) \times (w/n)$. According to the position of each black pixel and the sum of black pixels on the block, the difference in the number of black pixels between the two subsets must be equal to or less than one, and one block can be arbitrarily separated to two subsets. For one block, the two subsets are noted as C^q and C^{q+1} , then

$$|H(C^q) - H(C^{q+1})| \leq 1 \quad (1)$$

So, every block of every one secret image was separated into two subsets without any meeting point by this separation rule. To execute the separation for every block, the separated subsets of one secret image slightly, but not completely, reflected the original pattern of the secret image, except by stacking C^1 and C^2 . During DSP, the separation of one block randomly generated two matrixes C^{p+1} with size n x n for one block of original secret image by the following formulas and conditions [4]

$$\begin{aligned} \forall k, \\ a_{i,j}^{1,k} &= c_{i,j}^1 + c_{i,j}^2, \\ a_{i,j}^{2,k} &= c_{i,j}^3 + c_{i,j}^4, \end{aligned} \quad (2)$$

$$|H(C^1) - H(C^2)| \leq 1 \text{ And } |H(C^3) - H(C^4)| \leq 1$$

3.2 SP (sticking process)

The sticking operation executes logic ‘‘OR’’ operation between the separated subset and the share images during the sticking process. The goal is to build the patterns of two blocks $b^{1,k}$ and $b^{2,k}$ for share images S_1 and S_2 . The sticking results are generated according to the decrypting function. The secret image SE_1 is revealed by directly stacking share images S_1 and S_2 , by the defined decrypting process in the proposed scheme.

But, it needs to rotate the share image S_2 with 180° angle and stack with S_1 . According to the rule of the decrypting process, the two subsets, C^1 and C^3 , separated from DSP for secret images SE_1 and SE_2 , respectively, can be stuck together to build one corresponding block for share image S_1 . To build the corresponding block of share image S_2 , it must be rotated 180° , with C^4 separated from share image S_2 by DSP and stuck with the corresponding block of C^2 .

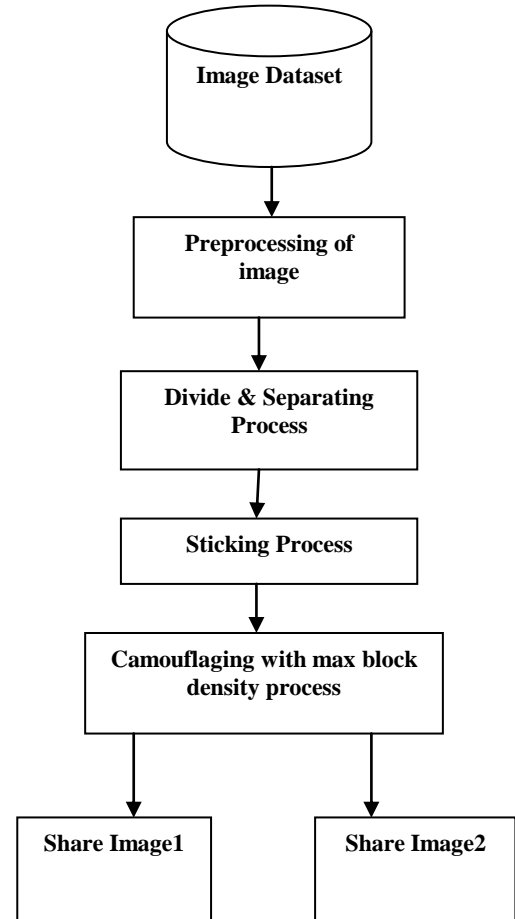


Figure 1: Encryption Process (Share generation process)

To generate share image S_2 , C^2 is another separated subset of S_1 is used. It was obvious that every pixel was moved from one position to another related position by the 180° rotation angle. For example, the pixel on the right-bottom position was moved to the left-top position, and vice versa. So, for building the blocks of share image S_2 , the first sticking operation was to stick C^2 with empty share image S_2 , and then to stick with the matrix with C^4 by rotating the share image S_2 with 180° [4].

$$\begin{aligned} b_{i,j}^{1,k} &\leftarrow c_{i,j}^1 \vee c_{i,j}^3, \\ b_{i,j}^{2,k} &\leftarrow b_{i,j}^{2,k} \vee c_{i,j}^2 \text{ And} \\ b_{n+1-i, n+1-j}^{2,k+1-k} &\leftarrow b_{n+1-i, n+1-j}^{2,k+1-k} \vee c_{i,j}^4, \forall k. \end{aligned} \quad (3)$$

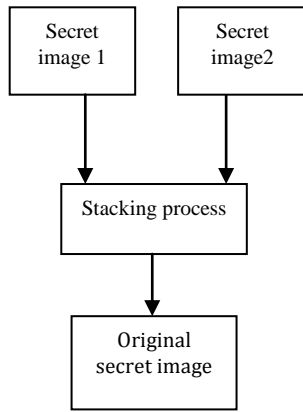


Figure 2: Decryption process

3.3 CMP (camouflaging with max. block density process)

Two camouflaging processes must be executed for every block of two share images obtained from the sticking process, in order to make the share image meaningless to anyone but an unauthorized user. Based on the maximum of block density, the camouflaging process makes the black pixel density of every block equal, so that every block appears to have the same pattern and the whole image will be a meaningless image. One attribute matrix $F^{p,k}$ with $n \times n$ size is defined here for finding the black area size for one block. $F^{p,k}$ is used to represent the color attribute of every pixel on k th block by stacking two secret images without executing the separation. For $p = 1$, $F^{p,k}$ was obtained by stacking secret image SE_1 and secret image SE_2 . For $p = 2$, $F^{p,k}$ was obtained by stacking secret image SE_1 and secret image SE_2 with a rotated 180° . Let $f_{i,j}^{p,k}$ represent the element of $F^{p,k}$. Every $f_{i,j}^{p,k}$ can be obtained according to the following formulas[4]:

$$f_{i,j}^{1,k} = a_{i,j}^{1,k} \vee a_{i,j}^{2,k},$$

$$f_{i,j}^{2,k} = a_{i,j}^{1,k} \vee a_{n+1-i, n+1-j}^{2, k+1-k}$$

$$\forall k, 1 \leq k \leq k, 1 \leq i, j \leq n. \quad (4)$$

4. An Improved Scheme

4.1 Encryption Process

1. Input the secret image from the image database for the encryption process.
2. Preprocessing of secret image corresponding to their color and size is performed.
3. Initialize the share image with black pixels on transparencies.
4. For divide and separation process, separate two secret images into two sets without any intersection.
5. Output of divide and separating process is given as input to the sticking process. In sticking process, it sticks the sets to the corresponding share images.
6. Output of sticking process is given as input to the camouflaging process. The camouflaging process calculates the

7. block density and finds max block density of share images.
8. Camouflage the block density of white pixels for all blocks of same storage image.
9. Camouflage the block density of black pixels for all blocks of share images.

4.2 Decryption Process

In the decryption process the share images are superimposed together and the first secret image is revealed. By using the linear array the coordinates of candidate blocks can be created and shuffled. Contrast of the revealed secret image is good because the pixel expansion is not done; only rearrangement of pixel is done. Contrast is the ratio of total number of black and white pixels on share image and secret image. To calculate the contrast of the revealed secret image the proposed system is referring the following formula [4]:

$$\text{Contrast} = 1 - \frac{\sum_{k=1}^k H(S^{p,k}) - \sum_{k=1}^k H(A^{p,k})}{w \times h - \sum_{k=1}^k H(A^{p,k})} \quad (5)$$

5. Experimental results and discussions

The first experiment encoded the gray-scale secret image shown in Figure 3(a) by using the proposed cryptography technique. The secret image Lena is given as input to the proposed system algorithm. The size specifications of the secret image are 256×256 for the further processing. The key image is generated with size specification for the encryption process of secret image to generate share image. In Figure 3 (a) Shows input secret image Lena, (b) Shows generated key image as share 1 (c) shows the encrypted secret image Lena as a generated share image 2 and (d) shows the recovered secret image.

The results indicate that proposed technique can provide a better quality for the reconstructed secret image. Input to the proposed scheme can be binary image, gray-scale image, color image. The size of the reconstructed secret image is same as that of original secret image Lena. The pixel expansion problem is removed in this technique. The share image(a) and share image (b) are meaningless.

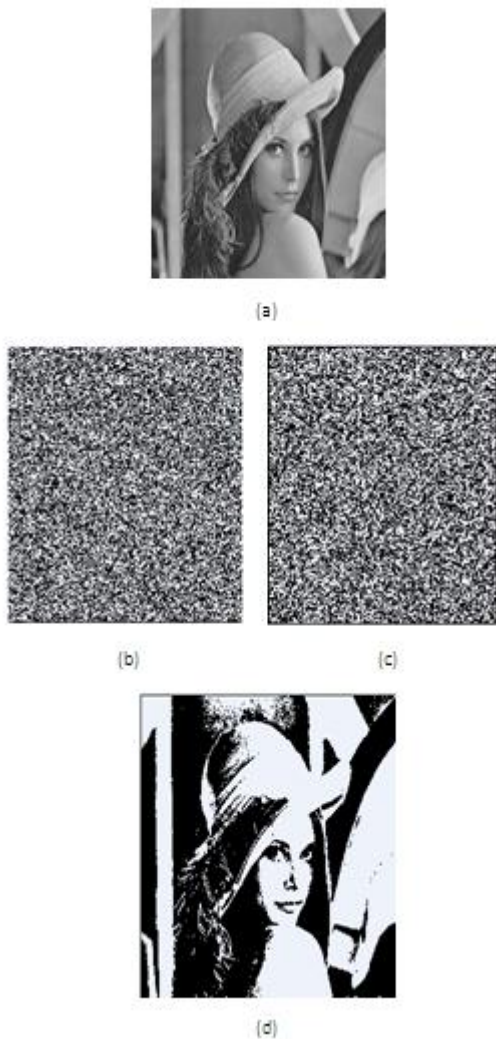


Figure 3: Experimental results: (a) Gray-scale secret image Lena (256×256), (b) share image 1, (c) share image 2, (d) Reconstructed secret image Lena (256×256).

6. Conclusion

Visual Cryptography is generally used either for sharing any secret among individuals or is used for authentication purpose. VC is a very creative technique of sharing secrets. It can be used in different fields and different area to ensure security. Less contrast and size of share image are the shortcomings of existing visual cryptography schemes. By using the proposed encryption process for generation of shares it is observed that these shortcomings are minimized. The share images are generated with no pixel expansion and have better contrast. Through the separation and camouflaging process, the share images become meaningless images. The meaningless share images did not leak any information of secret image, so that the security rule of visual secret sharing schemes conformed. By the human visual system the secret image is revealed by stacking the generated share images. No other computational devices were needed to recover the secret image. The system can be further modified for sharing color secret images and proposed another camouflaging process.

References

- [1] M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptology, 1994, vol. 950, LNCS, pp. 1-12
- [2] 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
- [3] 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.
- [4] Lin,Horng, Lee,Chiu,Kao and Chen." A novel visual secret sharing scheme for multiple secrets without pixel expansion", ELSEVIER journal 2010 0957-4174
- [5] Yang, C. N., & Chen, T. S. (2008). "Colored visual cryptography scheme based on additive color mixing" Pattern Recognition, 41, 3114-3129.
- [6] 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.
- [7] 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
- [8] 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.