International Journal of Computer Applications Technology and Research
Volume 2– Issue 3, 350 - 356, 2013, ISSN: 2319–8656

Modified Visual Cryptography Scheme for Colored Secret Image Sharing

Joshi Jesalkumari A.
Thakur College Of Engineering and Technology
Mumbai, India

R.R.Sedamkar
Thakur College of Engineering & Technology
Mumbai, India

Abstract: Intent of this paper is to prove the better performance of the XOR Based visual cryptography schemes and traditional VCS on the basis of quality of reconstructed image and type of shares generated for colored images. The visual cryptography scheme (VCS) is a scheme which encodes a secret image into several shares. Here we are working with (2, 2) VCS. XOR-Based visual cryptography is capable to overcome the drawbacks of the visual cryptography scheme (VCS) the small contrast of the recovered secret image.

Keywords: Halftone, Visual Cryptography, Image decomposition, superimpose, Pixel Expansion

1. INTRODUCTION

In Visual cryptography mainly visual information is encrypted using encryption algorithm but here there is no need of decryption algorithm to reveal the visual information. Here the decryption process is done simply by human visual system. During the encryption process we simply add some noise in the original image to hide the original information and during the decryption process we reduce the noise to unhide the original information. The technique was proposed by Moni Naor and Adi Shamir in 1994.Visual Cryptography uses two transparent images. They demonstrated a visual secret sharing scheme, where an image was broken up into *n* shares so that only someone with all *n* shares could decrypt the image, while any *n-1* shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all *n* shares were overlaid, the original image would appear. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. [4]

The secret image is composed of black and white pixels. The original secret image can be recovered by superimposing the two share images together. The underlying operation of such a scheme is the logical operation OR. Generally, a(k, n)-VCS takes a secret image as input, and outputs share images that satisfy two conditions: First, any k out of n share images can recover the secret image; second, any less than k share images cannot get any information about the secret image. Similar models of visual cryptography with different underlying operations have been proposed, such as the XOR operation introduced in [2]–[6], and the NOT operation introduced in [7], which uses the reversing function of the copy machines.

2. PRELIMINARIES

In a VCS, there is a secret image which is encrypted into some share images. The secret image is called the *original secret image* for clarity, and the share images are the encrypted images (and are called the transparencies if they are printed out). When a qualified set of share images (transparencies) are stacked together properly, it gives a visual image which is almost the same as the original secret image; we call this the *recovered secret image*. In the case of black and white images, the original secret image is represented as a pattern of black and white pixels. Each of these pixels is divided into subpixels which themselves are encoded as black and white to produce the share images. The recovered secret image is also a pattern of black and white subpixels which should visually reveal the original secret image if a qualified set of share images is stacked. In this paper, we will focus on the black and white images, where a white pixel is denoted by the number 0 and a black pixel is denoted by the number 1. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a One-time Pad system and will offer unbreakable encryption.

Table 1. Basic Encoding Idea in Naor and Shamir's Scheme

p	probability	s_1	s_2	$s_1 \otimes s_2$
□	1/2	□■	□■	□■
	1/2	■□	■□	■□
■	1/2	□■	■□	■■
	1/2	■□	□■	■■

Naor and Shamir's[4] proposed encoding scheme to share a binary image into two shares Share1 and Share2. If pixel is white one of the above two rows of Table 1 is chosen to generate Share1 and Share2. Similarly If pixel is black one of the below two rows of Table 1 is chosen to generate Share1 and Share2. Here 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 shown only when both shares are superimposed. Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [4] suggested two main parameters: pixel expansion m and contrast α. 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 α is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image.

3. VISUAL CRYPTOGRAPHY SCHEME

The visual cryptography scheme (VCS), introduced by Naor and Shamir in 1994 [4] is a type of secret sharing scheme which can split secret information into *n* shares and recover them by superimposing the shares. In VCS, the secret to be hidden is a black and white image and each share is compromised of groups of *m* black and white subpixel used to recover a pixel of the secret image. It is assumed that a white pixel in a share is transparent and a black pixel is opaque. It is impossible to get any information about the secret images from shares individually. The other advantage of VCS is that, unlike other cryptography techniques, this secret recovery does not need difficult computations. The secret information can easily be recovered with enough shares and requires human vision instead of special software or hardware devices. Naor and Shamir proposed a *k* out of *n* scheme and assumed that the image or message is a collection of binary 1 and 0 displayed as black and white pixels. According to their algorithm, the secret image is turned into *n* shares and the secret is revealed if any *k* of them are stacked together. So the image remains hidden if fewer than *k* shares are stacked together [5].

Image contrast and the number of subpixels of the shares and recovered image are two main parameters in visual cryptography schemes. The number of subpixels represents expansion of the image and should be as small as possible, while the contrast, which is a relative difference between the maximum value of Hamming weight for a black pixel and the minimum value of Hamming weight for white pixel, needs to be as large as possible [4]. Some researchers have focused on contrast degradation and introduced methods to improve the contrast of the reconstructed secret image.

3.1 The Basic Model

The basic 2 out of 2 visual cryptography model consists of a secret message encoded into two transparencies, one transparency representing the ciphertext and the other acting as a secret key. Both transparencies appear to be random dots when inspected individually and provide no information about the original clear text. However, by carefully aligning the transparencies, the original secret message is reproduced. The actual decoding is accomplished by the human visual system.
Naor and Shamir further describe the visual cryptography scheme as a visual secret sharing problem in which the secret message can be viewed as nothing more than a collection of black and white pixels. Each pixel in the original image is represented by at least one subpixel in each of the ***n*** transparencies or shares generated. Each share is comprised of collections of ***m*** black and white subpixels where each collection represents a particular original pixel. An example of the encoding of white and black pixels in a 2 out of 2 scheme can be seen in Figure 1. Here two shares out of the two generated would be needed to recover the original image. Since only two shares are generated, ***n*** = 2. Figure 1 represents a single white or black pixel in the original image and subpixel assignments that would be given to shares #1 and #2 respectively. The number of subpixels per share used to represent the original pixel is four (***m*** = 4). Finally, Figure 1(d) represents the overall visual effect when shares #1 and #2 are correctly aligned on top of one another. Notice that when the shares in this example are combined the original black pixel is viewed as black; however, the original white pixel takes on a grey scale.

The structure obtained from either white or black pixel representation in Figure 1 can be described by an ***n*** x ***m*** Boolean matrix ***Sp*** where ***p*** ε {white, black}. Any given element of the matrix ***S*** say ***s***ij, is considered to be 1 iff the *j*th subpixel in the *i*th transparency is black. When the ***n*** transparencies are properly aligned, the resulting black subpixels are the Boolean OR of the columns for each row ***i***1, ***i***2, … , ***i***n of ***S***. Shares #1 and #2 of Figure 1 would represent ***i***1 and ***i***2 respectively. Therefore, the following 2 x 4 Boolean matrices would be derived:
Swhite = { {1, 0, 0, 1}, {1, 0, 0, 1}} and
Sblack = { {1, 0, 0, 1}, {0, 1, 1, 0} }.
The matrix elements represent share assignments for share #1 and share #2 respectively Since ***m*** subpixels constitute one original pixel and the overall visual effect of a black subpixel in any one of the shares causes that particular subpixel when combined to become black, inspection of the grey level is the method of determining the original color of a pixel.

3.2 Algorithm

Encryption:

Step 1: Input the image with secret image.

Step 2: Initialize two collections of ***n*** x ***m*** Boolean matrices ***S0*** and ***S1. S0*** acts as a pool of matrices from which to randomly choose matrix ***S*** to represent a white pixel while ***S1*** acts as a pool of matrices from which to randomly choose matrix ***S*** to represent a black pixel.

Step 3: Using the permutated basis matrices, each pixel from the secret image will be encoded into two subpixels on each participant's share. A black pixel on the secret image will be encoded on the *ith* participant's share as the *ith* row of matrix *S1*, where a 1 represents a black subpixel and a 0 represents a white subpixel. Similarly, a white pixel on the secret image will be encoded on the *ith* participant's share as the *ith* row of matrix *S0.*

Decryption:

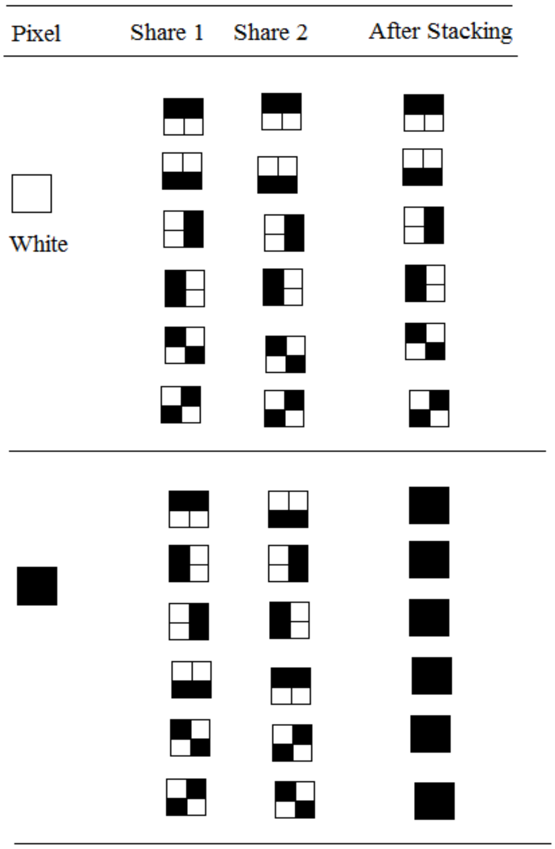
Stacking all the qualified participant’s share and ORing the stacked pixel to reconstructed the image.

We illustrated it with 2-out-of-2 scheme. In the 2-out-of-2scheme, every secret pixel of the image is converted into two shares and recovered by simply stacking two shares together. This is equivalent to using the OR operation between the shares. As illustrated in Table1 [4], 4 subpixels are generated from a pixel of the secret image in a way that 2 subpixels are white and2 pixels are black. The pixel selection is a random selection from each pattern. For example, when the corresponding pixel is white, one of the first six rows of Table 2 is randomly selected to encode the pixel into2 shares. It is easy to see that knowing only one share value does not reveal the other share and the secret image pixel. However superimposing all the shares reveals the corresponding binary secret image.

Experimental result

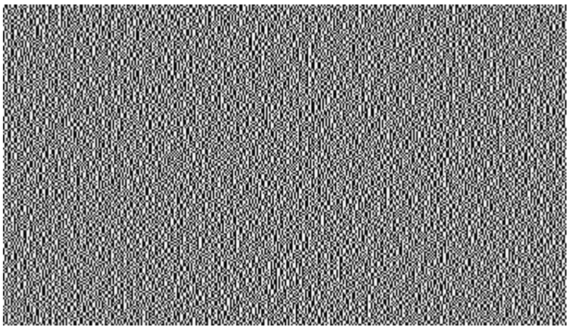
Figure 1 shows an example of Traditional Visual Cryptography scheme applying the (2, 2) with 4-subpixels layout visual secret sharing scheme, where the share images are larger than the original secret image in each dimension. That is, the share uses 4 subpixel for the original pixel. As illustrated in Figure1, (a) is the secret image, (b) and (c) are two random shares, and (d) shows the reconstructed image from superimposing the two shares.

Table 2.
(2, 2) VISUAL CRYPTOGRAPHY SCHEME

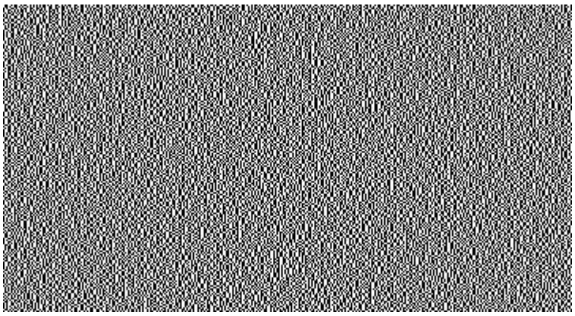


Here it is applied to binary image. However, the shortcomings of visual cryptography are as salient as its merits.

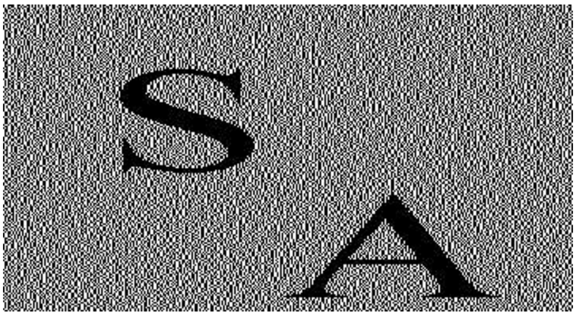
(a)



(b)



(c)



(d)

Figure 1. (a) Original Image (b) Share 1 (c) Share 2 (d) Reconstructed Image

There are three main drawbacks in visual cryptography:

- It results in a loss of resolution. The restored secret image has a resolution lower than that of the original secret image.
- Its background contrast is lost.
- Its original formulation is restricted to binary images. For color images, some additional processing such as halftoning and color-separation are required.
- The superimposition of two shares is not easy to perform unless some special alignment marks are provided. The manual alignment procedure can be tedious especially for high resolution images.

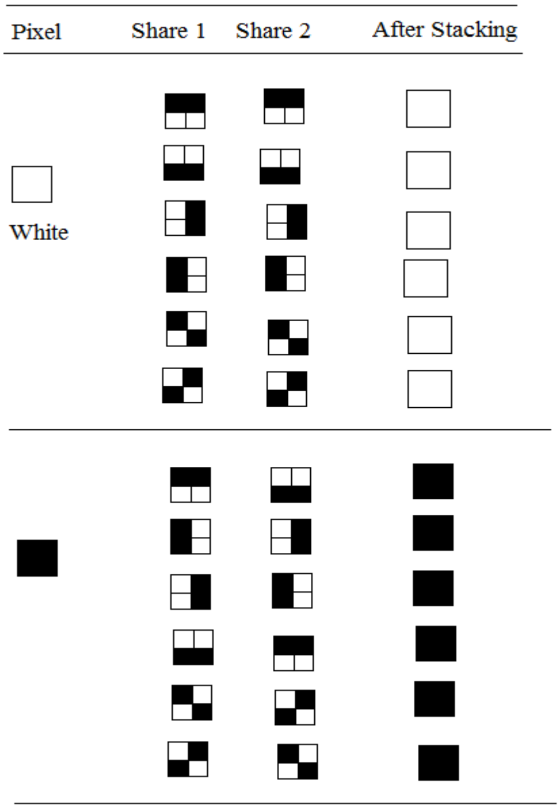
The biggest advantage of traditional method is the hard copy of the shares will give the same result as soft copy that too just by stacking the together.

4. XOR-BASED VISUAL CRYPTOGRAPHY

A (k; n) visual cryptography (VC) scheme [16] is a type of secret sharing scheme with the special property that a secret image can be recovered visually by the human eye and does not require any calculation on a computer. However, the recovered secret image has low quality. In this case, some researchers attempt to consider other different approaches to improve the quality (contrast)of the recovered image. Lee et al. [2] presented a VC scheme using an XOR process to share a binary image.

Based on the definition of Naor and Shamir [6], Verheul and van Tilborg [10] gave a more general definition. Following the notation from [16, 20], a definition of k out of n XOR-based visual cryptography scheme is given by Tuyls in Reference [7]. A (k, n) VC scheme S = (C0,C1) consists of two collections of n x m binary matrices C0 and C1.

TABLE 3.
(2, 2) XOR-BASED VISUAL CRYPTOGRAPHY SCHEME


Pixel
Share 1
Share 2
After Stacking
White

To share a white (black) pixel, the dealer randomly chooses one of the matrices in C0(C1) and distributes its rows as shares among the n participants of the system.

Table 2 [4], shows that 4 subpixels are generated from a pixel of the secret image in a way that 2 subpixels are white and 2 pixels are black. The pixel selection is a random selection from each pattern. For example, when the corresponding pixel is white, one of the first six rows of Table 2 is randomly selected to encode the pixel into 2 shares.

4.1 Algorithm

Step 1: Input the image with secret image.

Step 2: Initialize two collections of ***n*** x ***m*** Boolean matrices ***S0*** and ***S1. S0*** acts as a pool of matrices from which to randomly choose matrix ***S*** to represent a white pixel while ***S1*** acts as a pool of matrices from which to randomly choose matrix ***S*** to represent a black pixel.

Step 3: Using the permutated basis matrices, each pixel from the secret image will be encoded into two subpixels on each participant's share. A black pixel on the secret image will be encoded on the *ith* participant's share as the *ith* row of matrix *S1*, where a 1 represents a black subpixel and a 0 represents a white subpixel. Similarly, a white pixel on the secret image will be encoded on the *ith* participant's share as the *ith* row of matrix *S0.*

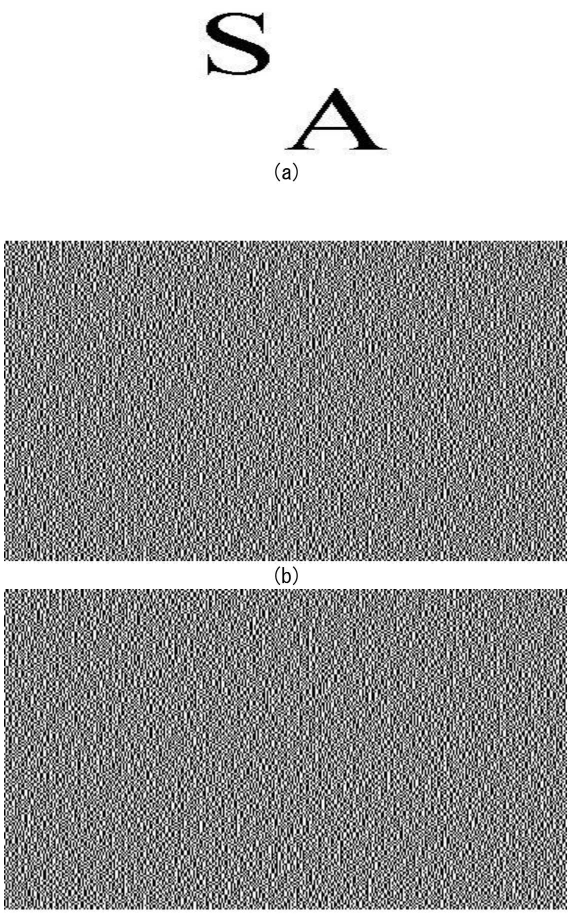
Decryption:

Stacking all the qualified participant’s share and XORing the stacked pixel to reconstructed the image.

We illustrated it with 2-out-of-2 scheme. In the 2-out-of-2scheme, every secret pixel of the image is converted into two shares and recovered by simply stacking two shares together. This is not equivalent to the OR operation between the shares but we have to XOR the pixels. As illustrated in Table2 [4], 4 subpixels are generated from a pixel of the secret image in a way that 2 subpixels are white and2 pixels are black. The pixel selection is a random selection from each pattern. For example, when the corresponding pixel is white, one of the first six rows of Table 2 is randomly selected to encode the pixel into2 shares. It is easy to see that knowing only one share value does not reveal the other share and the secret image pixel. However superimposing all the shares reveals the corresponding binary secret image.

Experimental Result

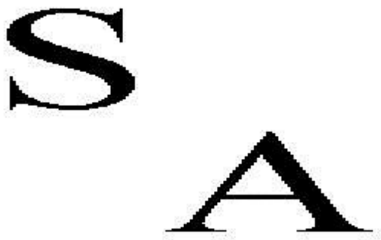
Figure 2 shows an example of Traditional Visual Cryptography scheme applying the (2,2) with 4-subpixels layout visual secret sharing scheme, where the share images are larger than the original secret image in each dimension. That is, the share uses 4 subpixel for the original pixel. As illustrated in Figure 2(a) is the secret image, (b) and (c) are two random shares, and (d) shows the reconstructed image from superimposing the two shares.



(a)

(b)

(c)



(d)

Figure 2 (a) Original Image (b) Share 1 (c) Share 2 (d) Reconstructed XORed Image

5. COMPARISON

Traditional Visual Cryptography has almost double pixels in its reconstructed image same as XOR-Based Visual Cryptography. The Reconstructed image in traditional Visual Cryptography had lost its original contrast specially in background but in XOR-Based Scheme the contrast is regained. If the decryption is done by software for stacking shares then both the method gives expected result but if the hard copy of shares are to be stacked then traditional VCS will have same output as softcopy but XOR-Based VCS will not have output as softcopy stacked.

TABLE 4.
Comparison

VCS type	Pixel Expansion	Contrast	Softcopy Decryption	Hardcopy Decryption
Traditional	More	Lost	Same as algorithm	Same as algorithm
XOR Based	More	Retained	Same as algorithm	Not Same

6. PROPOSED METHOD

In this paper, we have proposed a visual cryptography method for colored images. Following flowchart shows the Procedure:

Input a colored image which should be in rgb color model.Then split the image in CMY model.The purpose of using CMY is in printers usually CMY model is used. Because the subtractive model is more suitable for printing colors on transparencies, we will use the CMY model to represent colors in what follows. Because (R, G, B) and (C, M, Y) are complementary colors, in the true color model, (R, G, B) and (C, M, Y) possess the following relationships: C = 255−R, M = 255−G, Y = 255−B: Thus, in the (C, M, Y) representation, (0; 0; 0) represents full white and (255; 255; 255) represents full black. So here first we will split RGB spaces in original model. Then using following equation RGB is converted to CMY model. It is implemented in matlab 6.1.

c = 1-(double(r) /255);

m = 1-(double (g)/255);

y = 1-(double (b)/255);

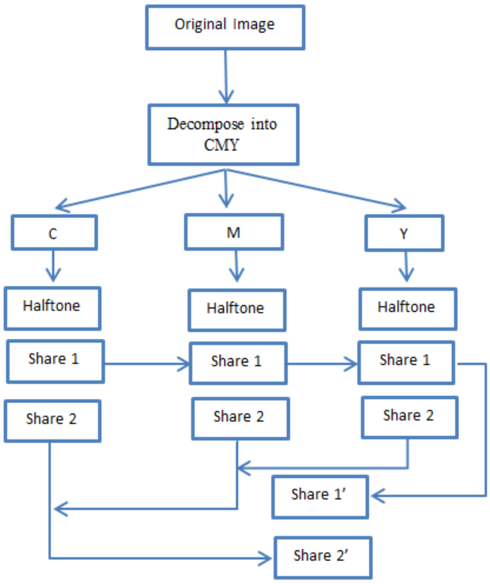


Figure 3. Generating Shares of colored images

Here, r, g, b contains red, green and blue spaces respectively and c,m,y for cyan, magenta and yellow. Color decomposition is mainly to separate C, M, and Y a color from colors within every pixel of the image. These three components form three monochromatic images. Each one looks gray-scale image on the monitor. Matlab do not support CMY color model. So decomposition of image does not show C, M and Y color on the screen.

Then we applied halftone algorithm on this three images separately. There are many halftone algorithms. Here I have used floyed's algorithm. This gives three halftoned images for each Cyan, Magenta and Yellow. Here each pixel is compared against threshold (T=127) and if intensity is greater than T make it 255 else 0.

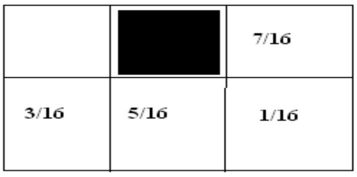


Figure 4. Coefficients' of Floyd's method

These Halftoned images are now given as an input to our Visual cryptography algorithm for (2,2). Two shares are generated for each halftoned image. Now share 1 of each image is combined which makes share1' and same for share 2.

These share 1' and share 2' are final shares that are to be given to participants.

Decoding side these shares are XORed opposite to traditional VCS. It gives better visual quality.

7. RESULTS

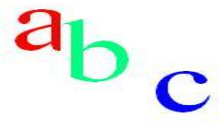
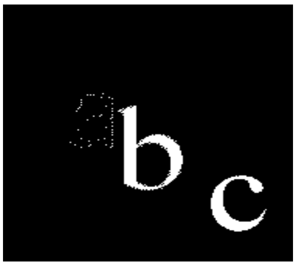
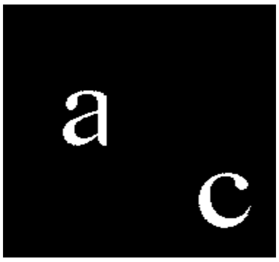


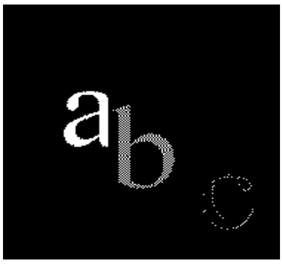
Figure 5. (a) Original Image



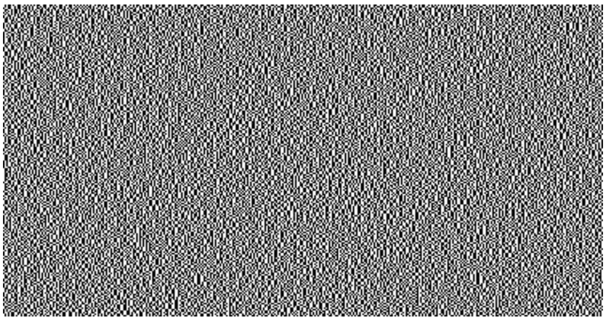
(b) Cyan



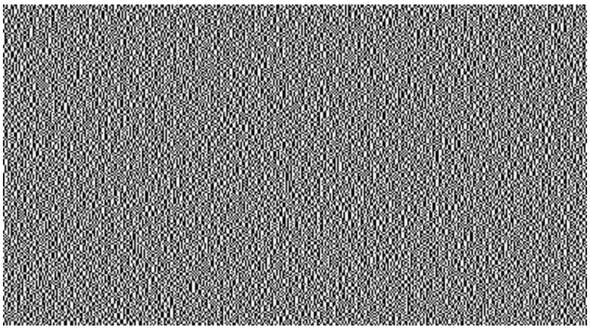
€ Magenta



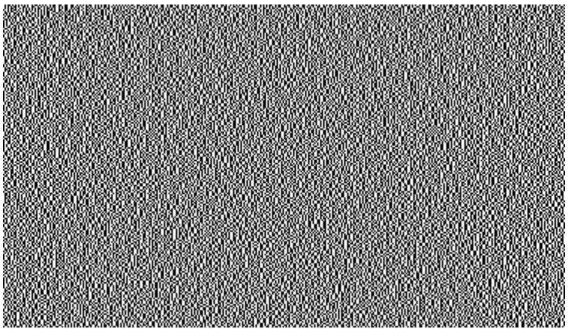
(d) Yellow



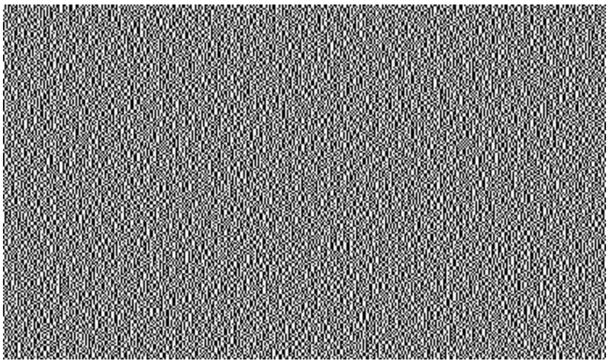
(e)Cyan Share 1



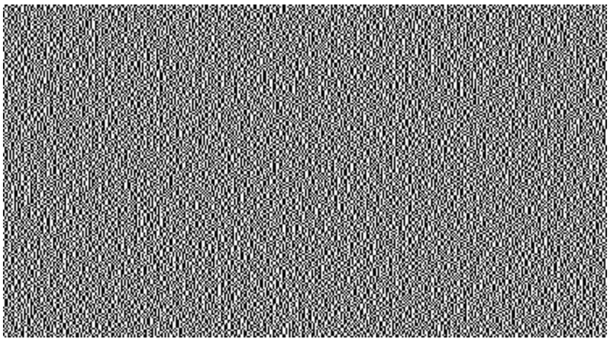
(f) Cyan Share 2



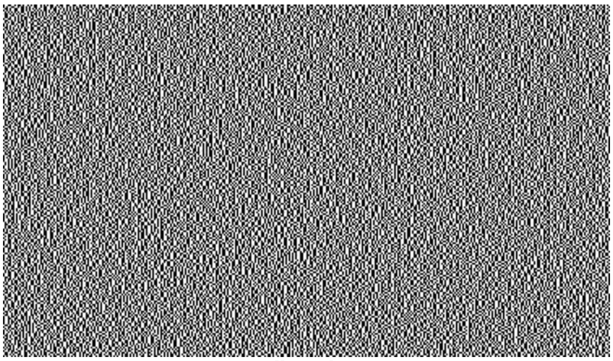
(g)Magenta Share1



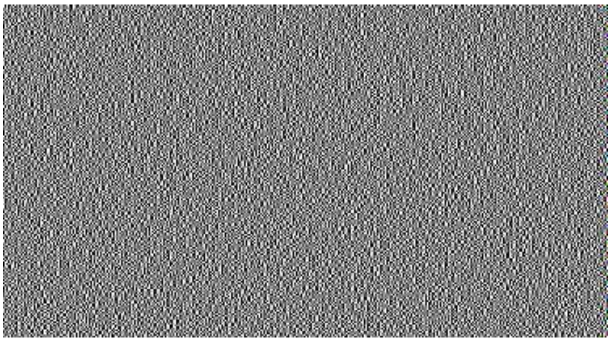
(h) Magenta Share 2



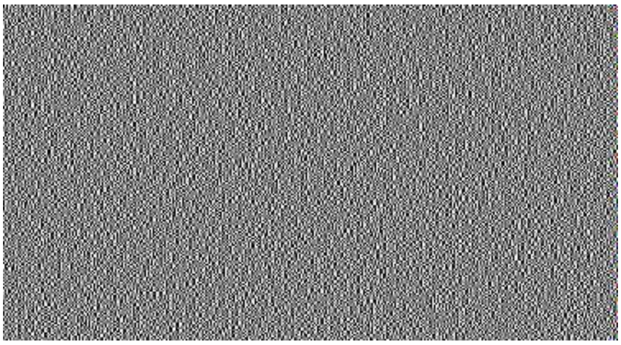
(i) Yellow Share 1



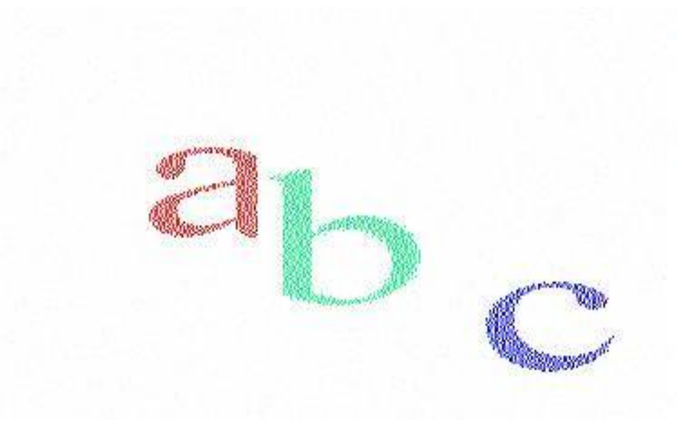
(j) Yellow Share 2



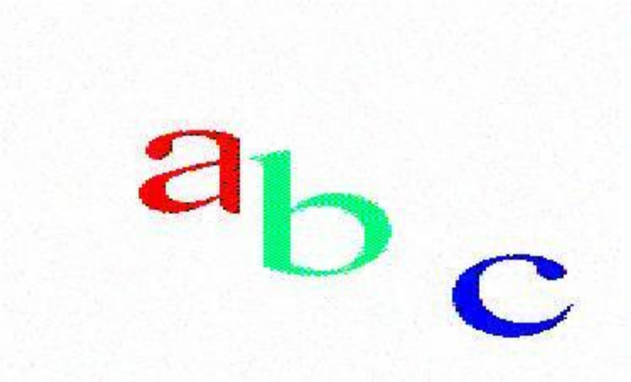
(k) Generated share 1'



(l) Generated Share 2'



(m) Traditionally Decrypted by ORing shares



(n) XORed Shares
Figure 5. Results of Proposed Method

8. CONCLUSION

Comparing traditional VCS with XOR based visual cryptography; XOR based visual Cryptography gives better visual quality. Generated shares are random dots so it doesn't reveal secret information. This proposed method can deal with both grey level and colored images. Colored image is decomposed into primary colors C,M,Y but grey level image can be directly transformed into a binary image, it can be further extended for extended visual cryptography where shares are having visual meaning.

9. REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. .

[2] D. Q. Viet and K. Kurosawa, "Almost ideal contrast visual cryptography with reversing," *Topics in Cryptology—CT-RSA*, pp. 353–365, 2004.

[3] E. Biham and A. Itzkovitz, "Visual cryptography with polarization," in *RUMP Session of CRYPTO'98*, 1997.

[4] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Visual cryptography for general access structures", Information and Computation 129 (1996), 86-106.

[5] M. Naor and A. Shamir, "Visual cryptography II: improving the constrast via the cover base, in Security Protocols", M. Lomas, ed., Lecture Notes in Computer Science 1189 (1997), 197-202.

[6] M. Naor and A. Shamir, Visual cryptography, in "Advances in Cryptology { EUROCRYPT '94", A.De Santis, ed., Lecture Notes in Computer Science 950 (1995), 1-12.

[7] P.S.Revenkar, Anisa Anjum, W .Z.GandhareGovernment College of Engineering, Aurangabad, M.S., India"Survey of Visual Cryptography Schemes" International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[8] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents, technical report TR001001, Florida State University (2000).

[9] R. Gonzalez and R. Woods, Digital Image Processing using MATLAB, Fourth Impression, 2008.