Efficient Visual Cryptography

Er. Supriya Kinger
CSE Department, Chitkara Institute of Engineering and Technology,
Rajpura, Punjab, India
Email: ahujasupriya@gmail.com

Abstract **– Visual cryptography scheme (VCS) is a secret-sharing scheme which allows the encryption of a secret image into n shares that are distributed to n participants. The beauty of such a scheme is that, the decryption of the secret image requires neither the knowledge of cryptography nor complex computation. Colour visual cryptography becomes an interesting research topic after the formal introduction of visual cryptography by Naor and Shamir in 1995. It is a powerful technique which combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics. A binary image can be divided into shares which can be stacked together to approximately recover the original image. Unfortunately, it has not been used much primarily because the decryption process entails a severe degradation in image quality in terms of loss of resolution and contrast. Its usage is also hampered by the lack of proper techniques for handling grayscale and color images. In this paper, I have developed a novel technique which enables visual cryptography of color as well as grayscale images. The physical transparency stacking type of decryption allows for the recovery of the traditional visual cryptography quality image. An enhanced stacking technique allows for the decryption into a halftone quality image. And finally, a computation based decryption scheme makes the perfect recovery of the original image possible. Based on this basic scheme, I have then established a progressive mechanism to share color images at multiple resolutions. I extracted shares from each resolution layer to construct a hierarchical structure; the images of different resolutions can then be restored by stacking the different shared images together. I have implemented our technique and present results.**

Index Terms **– Secret sharing, Color halftoning, image sharing, multiple resolutions, secret sharing, and visual cryptography**

I. Introduction

Visual cryptography was originally proposed for the problem of secret sharing. Secret sharing is one of the early problems to be considered in cryptography. The idea of the visual cryptography model proposed in [1] is to split an image into two random shares (printed on transparencies) which separately reveal no information about the original secret image other than the size of the secret image. The image is composed of black and white pixels. The original image can be recovered by superimposing the two shares. The underlying operation of this visual cryptography model is OR.

Visual cryptography is a unique technique in the sense that the encrypted messages can be decrypted directly by the human visual system. Therefore, a system employing visual cryptography can be used by anyone without any knowledge of cryptography. Another interesting thing about visual cryptography is that it is a perfectly secure cipher. There is a simple analogy of the one time-pad cipher to visual cryptography.

II. Background On Visual Cryptography

Besides introducing the new paradigm, Naor and Shamir also provided their constructions of visual cryptographic solutions for the general *k* out of *n* secret sharing problem. One can assume that every secret message can be represented as an image, and furthermore that the image is just a collection of black and white pixels i.e. it is assumed to be a binary image. Each original pixel appears in *n* modified versions (called shares) of the image, one for each transparency. Each share consists of *m* black and white sub-pixels. Each share of sub-pixels is printed on the transparency in close proximity (to best aid the human perception, they are typically arranged together to form a square with *m* selected as a square number). The resulting structure can be described by a Boolean matrix $M = (m_{ij})_{n*m}$ where $m_{ij} = 1$ if and only if the *j*-th sub-pixel of the *i*-th share (transparency) is black. The important parameters of the scheme are:

1. *m*, the number of pixels in a share. This parameter represents the loss in resolution from the original image to the recovered one.
2. α, the relative difference in the weight between the combined shares that come from a white pixel and a black pixel in the original image. This parameter represents the loss in contrast.
3. γ, the size of the collection of C_0 and C_1. C_0 refers to the sub-pixel patterns in the shares for a white pixel and black refers to the sub-pixel patterns in the shares for the 1 pixel.

The constructions can be clearly illustrated by a 2 out of 2 visual cryptographic scheme. Here we define the following collections of 2*4 matrices:

C_0 = all the matrices obtained by permuting the columns of

$$\begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{vmatrix}$$

C_1 = all the matrices obtained by permuting the columns of

$$\begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{vmatrix}$$

doi:10.4304/jetwi.2.2.137-141

The six patterns of shares created based on the above matrices are shown in figure 1. Note that *one* pixel of the original image now corresponds to *four* pixels in each share.

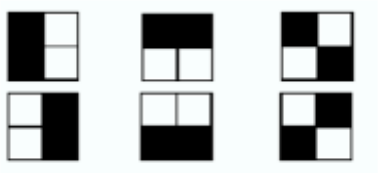


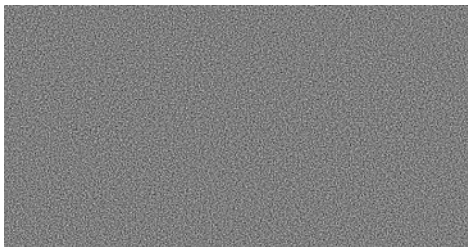
Fig 1: The six patterns of 4 pixel shares: vertical, horizontal and diagonal

A visual cryptography scheme can then be constructed by picking shares in the following manner:

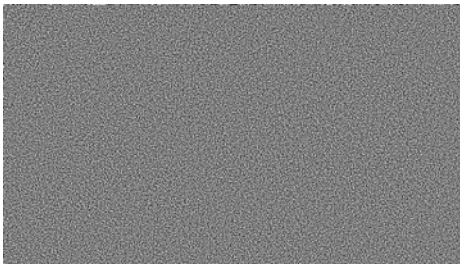
a) If the pixel of the original binary image is white, randomly pick the same pattern 0 of *f our* pixels for both shares. It is important to pick the patterns randomly in order to make the pattern random.
b) If the pixel of the original image is black, pick a complementary pair of patterns, i.e., the patterns from the same column in figure 1.

It can be easily verified that the resultant scheme has the parameters [m = 4; α= 12 ; γ= 6]: any two shares of C_0 cover *two* out *f our* of the pixels, while any pair of shares from C_1 covers all the *f our* pixels. An example of the above scheme is shown in figure 2. The first image is the original image, the next two are the shares and the last image is the recovered original image obtained by performing the equivalent of physically stacking two image shares on top of each other (assuming that they are printed on transparencies). It should be noted that the last three images in figure 2 are four times as large as the first one but I have scaled them to the same size as the original image.

(a) Sample of monochrome image



(b) The first Share



(c) The second share

(d) The stacked Image

Fig 2. Implementation of existing methodology

III. Related Work

There has been a steadily growing interest in visual cryptography. Despite its appearance of being a simple technique, visual cryptography is a secure and effective cryptographic scheme. Since the origin of this new paradigm, various extensions to the basic scheme have been developed to improve the contrast and the areas of application have also been greatly expanded.

In [1], the construction of (n,n)-VCS was extended for (k,n)-VCS. In 1996, the same authors introduced the idea of cover based semi-group to further improve the contrast [3]. Ateniese et al. [4] provided the first construction of (2, n)-VCS having the best possible contrast for any n·2. Blundo et al. [5] provided a contrast optimal (3,n)-VCS and gave a proof on the upper bound on the contrast of any (3,n)-VCS. [1] first considered the problem of concealing the existence of the secret image. [6] provided a general solution for that problem.

The random nature of secret shares makes shares unsuitable for transmission over an open channel. [6] used a modified scheme to embed some meaningful images into the shares. [7] used different moiré patterns to visualize the secret instead of different gray levels. As far as extending to color images goes, [8] provided a primitive scheme for images of 24 colors. Hou [9] then proposed a novel approach to share color images based on halftoning. Other interesting topics include visual authentication [10] and watermarking based on visual cryptography [11]. Recently, there has been an attempt to build a physical visual cryptographic system based on optical interferometry [12]. However, all of these earlier works result in a decrypted image of reduced quality.

IV. Our Contribution

The state of the art in visual cryptography leads to the degradation in the quality of the decoded images, which makes it unsuitable for digital media (image, video) sharing and protection. This is quite obvious in figure 2 where the white background of the original image becomes gray in the decrypted image.

Through this paper, I propose a visual cryptographic schemes that not only can support grayscale and color images, but also allow high quality images including that of perfect (original) quality to be reconstructed.

The nagging presence of the loss of contrast makes traditional visual cryptography scheme practical only when quality is not an issue which is quite rare. I have therefore focused our attention on specifically overcoming this problem by primarily devoting our efforts towards improving the quality of the reconstructed images. I first extend the basic scheme from [1] to allow visual cryptography to be directly applied on grayscale and color images. Image halftoning is employed in order to transform the original image from the grayscale/color space into the monochrome space which has proved to be quite effective.

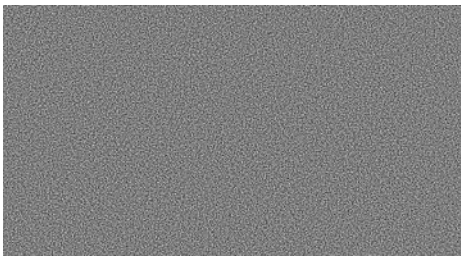
It is a well known fact that the digital halftoning is always a lossy process [2], which means that whenever a halftoning is used for the transformation, it is impossible to fully reconstruct the original secret image. A new encoding scheme has therefore been developed which allows for perfectly lossless transformation between monochrome, grayscale and color spaces. This new encoding scheme can be seamlessly incorporated into the proposed scheme for visual cryptography and it allows the original secret image to be perfectly restored. I believe this advancement in visual cryptography can be useful in secret sharing of images, in transmission of secret images over multiple untrustworthy channels, in e-commerce of digital media and in digital rights management of digital media.

V. Our Approach

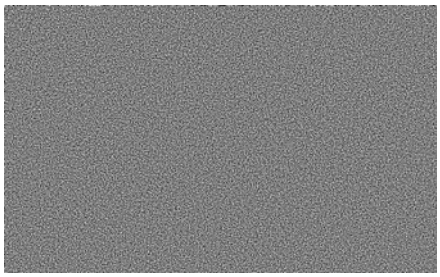
A. For Monochrome Images

Using XOR to Fully Restore Monochrome Secret Images :-I, first made the crucial observation that with just one additional computational operation; even traditional visual cryptography can allow full recovery of the secret binary image. Normally, when we superimpose the two shares printed on transparencies, this stacking operation is computationally modeled as the binary OR operation which causes the contrast level to be lowered. By simply substituting this OR operation with the XOR operation, the original binary image can be recovered without any loss in contrast. Thus, the produced image could have a more visually pleasant appearance with less storage space requirement. However, the XOR operation needs computation - the physical stacking process can only simulate the OR operation. Figure 3 recovers the same secret image as in figure 2 using the XOR operation and thus it is clearly evident that the contrast of the original image is restored.

(a) Sample of monochrome image



(b) The first Share



(c) The second share

(d) The stacked Image with XOR

Fig 3. Implementation of proposed methodology

As we have seen earlier, the application of digital halftoning 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. We will refer to this proposed scheme as EVCS (Efficient Visual Cryptographic Scheme).

The novelty of my approach is that it not only allows the secret image to be just seen but allows the secret image to be reconstructed with perfect quality. The advantage of this approach is that it still retains the crucial advantages of traditional visual cryptography like simplicity, visual decoding and perfect security. The extra feature is that depending on whether additional computing resources are provided, images of different

quality can be decoded from the same set of shares. If only the stacking operation is allowed (i.e. no computations), then our scheme recovers the original visual cryptographic quality. If the XOR operation is provided (instead of the OR operation of stacking), then we can fully restore the original quality image.

B. For Colored Images (Halftone-based Grayscale and Color Visual Cryptography)

Digital halftoning has been extensively used in printing applications where it has been proved to be very effective. For visual cryptography, the use of digital half toning is for the purpose of converting the grayscale image into a monochrome image. Once we have a binary image, then the original visual cryptography technique can be applied. However, the concomitant loss in quality is unavoidable in this case.

For color images, there are two alternatives for applying digital halftoning. One is to split the color image into channels of cyan, magenta and yellow. Then each channel is treated as a grayscale image to which halftoning and visual cryptography are applied independently. After the monochrome shares are generated for each channel, channels are combined separately to create the color shares. This is the approach presented in [9]. The alternative approach would be to directly apply color halftoning, then perform the separation into color channels followed by the application of visual cryptography to each channel independently. Actually, these two approaches lead to the same results finally. There are many mature halftoning techniques available for selection like dispersed-dot dithering, clustered-dot dithering and error diffusion techniques.

Halftoning based visual cryptographic scheme can be summarized as follows:

a) **Encryption***:* This stage is for the creation of shares. This can be further divided into the following steps:

i. *Color halftoning:* Standard algorithms such as the ones described in [2], [13] and [14] can be used for this step. One could do the color channel splitting first and then do the grayscale halftoning for each channel:

$$I \xrightarrow{split\ \ CMY} [I^C, I^M, I^Y] \xrightarrow{halftoning} [I^C_{hft}, I^M_{hft}, I^Y_{hft}]$$

Or one could do color halftoning first followed by the splitting:

$$I \xrightarrow{color\ \ halftoning} I_{hft} \xrightarrow{split\ \ CMY} [I^C_{hft}, I^M_{hft}, I^Y_{hft}]$$

ii. *Creation of shares:* Considering the case of (2,2)-VCS, the steps are

$$I^C_{hft} \xrightarrow{(2,2)-VCS} [S^C_0, S^C_1]$$
$$I^M_{hft} \xrightarrow{(2,2)-VCS} [S^M_0, S^M_1]$$
$$I^Y_{hft} \xrightarrow{(2,2)-VCS} [S^Y_0, S^Y_1]$$

b) **Decryption:** This stage is for the reconstruction of the original secret image. This can be further divided into the following steps:

i. *Stacking of shares:* The following stacking (OR) operation needs to be performed:

$$[S^C_0, S^C_1] \xrightarrow{stacking} I^{mg}_C$$
$$[S^M_0, S^M_1] \xrightarrow{stacking} I^{mg}_M$$
$$[S^Y_0, S^Y_1] \xrightarrow{stacking} I^{mg}_Y$$

ii. *Subsampling for reconstruction:* These operations need to be performed where every block of *f our* pixels is sub-sampled into *one* pixel of the final image. This step is optional and should be used only with the XOR recovery described in Section III-B.1 to achieve better quality.

$$[I^{mg}_C, I^{mg}_M, I^{mg}_Y] \xrightarrow{combine\ CMY} I^{mg}$$

Then, for every 2*2 block $B(i; j)$ of I, where

$$B(i,j) = \begin{bmatrix} I^{mg}(2i,2j) & I^{mg}(2i,2j+1) \\ I^{mg}(2i+1,2j) & I^{mg}(2i+1,2j+1) \end{bmatrix}$$

$$I^{subsampled}(i,j) = I^{mg}(2i,2j)$$

It is clear that our technique, though independently developed, is quite similar in spirit to the one described in [9]. So both share the same drawback that digital halftoning always leads to permanent loss of information which means that the original image can never be perfectly restored. Inverse halftoning is a possible solution that can attempt to recover the image. The best results can obtain a restoration quality of 30 dB measured in PSNR, which is quite good. But this is not sufficient for applications which require that the original image be faithfully recovered. In fact, in all other cryptographic techniques, it is taken for granted that the decryption of a ciphertext perfectly recovers the plaintext. But visual cryptography has been a glaring exception so far.

VI. CONCLUSION

In this paper, I have extended traditional visual cryptography by employing new schemes which overcome its limitations. I propose a technique for grayscale and color visual cryptography. Our insight is that the OR operation in the traditional visual cryptography can be replaced by the XOR operation in order to allow for lossless decryption. However, there are some practical issues that need careful consideration. First, the transparencies should be precisely aligned in order to obtain a clear reconstruction. Secondly, there is usually some unavoidable noise introduced during the printing process. Thirdly, the stacking method can only simulate the OR operation which always leads to a loss in contrast. Proper alignment is absolutely essential when superimposing the shares. In real experiments, we have found that obtaining perfect alignment is always troublesome. As visual cryptographic schemes operate at the pixel levels, each pixel on one share must be matched correctly with the corresponding pixel on the other share. Superimposing the shares with even a slight shift in alignment results in a drastic degradation in the quality of the reconstructed image. In the worst case, even a single pixel shift can render the secret image totally invisible. This alignment problem can be resolved if the boundary of each share is clearly marked which can act as guides for the alignment.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology -EUROCRYPT'94*, A. D. Santis., Ed., vol. 950. Springer-Verlag, 1995, pp. 1–12.

[2] H. R. Kang, *Digital Color Halftoning*, ser. SPIE/IEE Series on Imaging Science and Engineering, E. R. Dougherty, Ed.Bellingham, Washington USA and New York: Copublished by SPIE Optical Engineering Press and IEEE Press, 1999.

[3] M. Naor and A. Shamir, "Visual cryptography 2: Improving the contrast via the cover base," 1996, a preliminary versionappears in "Security Protocols", M. Lomas ed. Vol. 1189 of Lecture Notes in Compute Science, Springer-Verlag, Berlin,pp.197-202, 1997.

[4] A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in *23rd International Colloquium on Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, F. M. auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416–428.

[5] C. Blundo, P. D'Arco, A. D. Snatis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM Journal on Discrete Mathematics, available at: http://citeseer.nj.nec.com/blundo98contrast.html*, vol. 16, no. 2, pp. 224–261, April 1998.

[6] G. Ateniese, C. Blundo, A. D. Santis, and D. Stinson, "Extended schemes for visual cryptography," *Theoretical ComputerScience*, vol. 250, pp. 143–161, 2001.

[7] Y. Desmedt and T. V. Le, "Moire cryptography," in *the 7th ACM Conference on Computer and Communications Security'00*, Athens, Greece, 2000.

[8] V. Rijmen and B. Preneel, "Efficient color visual encryption for shared colors of benetton," 1996, EUCRYPTO'96 RumpSession. Availabe at http://www.iacr/org/conferences/ec96/rump/preneel.ps.

[9] Y. C. Hou, C. Y. Chang, and S. F. Tu, "Visual cryptography for color images based on halftone technology," in*International Conference on Information Systems, Analysis and Synthesis. World Multiconference on Systemics, Cyberneticsand Informatics. Image, Acoustic, Speech And Signal Processing: Part II*, 2001.

[10] M. Naor and B. Pinkas, "Visual authentication and identification," *Lecture Notes in Computer Science*, vol. 1294, pp. 322–336, 1997. [Online]. Available: citeseer.nj.nec.com/67294.html

[11] Q. B. Sun, P. R. Feng, and R. Deng, in *International Conference on Information Technology: Coding and Computing (ITCC '01), available at: http://dlib.computer.org/conferen/itcc/1062/pdf/10620065.pdf*, Las Vegas, April 2001.

[12] S.-S. Lee, J.-C. Na, S.-W. Sohn, C. Park, D.-H. Seo, and S.-J. Kim, "Visual cryptography based on an interferometric encryption technique," *ETRI Journal*, vol. 24, pp. 373–380, 2002, available at http://etrij.etri.re.kr/etrij/pdfdata/24-05-05.pdf.

Supriya A. Kinger was born in Haryana, India on 15th july 1982. She did her Master's in technology in field of computer science from YMCA, Haryana in year 2005, India and Bachelor's in technology in Computer Science from KU, Haryana, India. In year 2003.Currently she is doing research in field of Software Engineering (Component Based Software Engineering).

She has more than 5 Years of experience in teaching and research. She has attended and organized a number of workshops and conferences. She hosted a conference ASET-2006 at CIET and acted as convener in it. She has presented number of papers in national and international conferences of repute on the topics of web crawlers, Component based software Engineering, Information Security and Networks. Currently she is Working with Chitkara Institute of Enginnering and Technology, Punjab, India as Senior Lecturer. Earlier she has worked at Institute of Engineering and Technology. She is life member of ISTE