(n, n) Visual Cryptography based on Alignment of Shares

Abhishek Kr Mishra
Research Scholar
IFTM University,Moradabad
India

Ashutosh Gupta
Department of CSIT
Associate Professor, MJP
Rohilkhand University, Bareilly,
India

Ashish Kumar
Department of CSE
Associate Professor
IFTM University, Moradabad

ABSTRACT
According to visual cryptography the decryption is performed by human visual system. It is well known that visual cryptography encryption process generates shares. Proposed method based on alignment of shares at the time of superimposition. Using these shares the source image can be recovered only if the shares are superimposed with proper predefined alignment. Proper alignment of these shares at the time of superimposition plays an important role in finding the source image. Here, we are proposing a new way of aligning the shares for getting the source image and this is the only way to obtaining the source image.

Keywords
Cryptography, Secret Sharing, visual cryptography

1. INTRODUCTION
The computer technologies have grown significantly in the few past years. More and more multimedia products such as digital cameras have become popular, so digital images are shared and transmitted widely over Internet. However, transmitting secret or important images, Such as military or commercial images, over Internet is very dangerous [8]. Malicious users may monitor Internet and try to eavesdrop these valuable images. To protect these images visual cryptography is necessary for secure communications over Internet.

Visual Cryptography was originally invented and pioneered by Moni Naor and Adi samir in 1994 at Eurocrypt Conference**.** Visual cryptography is a new type of cryptographic scheme that is based on secret sharing [3, 11]. Secret sharing (SS**)** refers to any method for distributing a secret among a group of participants, each of which allocates a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. Secret Sharing can be applied to achieve the goal of visual cryptography. Visual cryptography uses the idea of hiding secret within the images. These images are encoded in such a way that decoding can be performed by simple as a superimposing of encoded images, which allows the source image to be recovered.

2 RELATED WORK

(2, 2) Visual Cryptography[1,2] is the basic model of VC but less secure because encrypted information shared at only two places, by combining these encrypted information the hidden information can be achieved. (2, 2) visual cryptography extended to (n, n) visual cryptography by which encrypted information may be shared on n different places and by combining all encrypted information the source information can be achieved but handling of these n shares in encryption process is difficult.(2, n) and (k, n) are other access structure used in the visual cryptography.(2, 2) access structure is the basic model of visual cryptography. Table 1 Shows the all six cases when a single pixel partitioned into four sub pixels. Layer1, Layer2 shows the positions of subpixels on the share1 and share2 respectively. When pixel is white then half area is black and half is black and pixel is black then full pixel recovered. It means all the information recovered. So information loss is Zero percent at the time of recovery of source image.

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 [13]

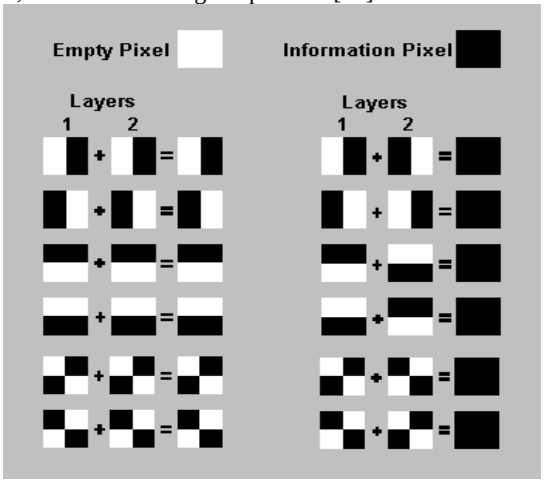


Table1

3 PROPOSED METHOD OF VISUAL CRYPTOGRAPHY

In Proposed solution (2, 2) Visual Cryptography is used for generating the n shares. When we combine all n shares in predefined alignment the source image can be achieved. In encryption process (2, 2) VC is used, and (n, n) VC is used in the decryption process. So it is the combination of (2, 2) VC and (n, n) VC that is used in our proposed solution.

3.1 Encryption: A simple (2, 2) visual cryptographic scheme using m=4 is applied, i.e., one pixel divided into four sub pixels. Source image is partitioned horizontally into three portions of image, p1, p2 and p3. By applying (2, 2) visual cryptography on image portion p1, the shares share1 and share2 are generated. Same process is applied to image portion p2 to generate the shares share3 and share4. The process is repeated on image portion p3 to generate the shares share5 and share6. By this approach the complete source image is encrypted into 6 shares. Fig1 shows the encryption process.

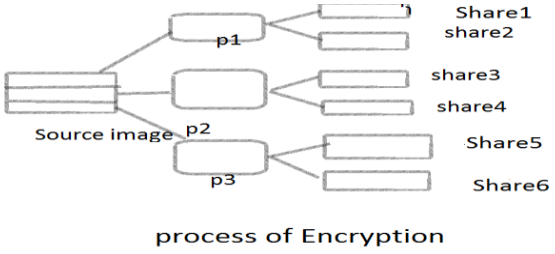
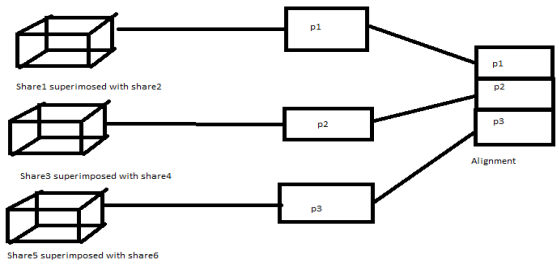


Fig 1

3.2 Decryption: We can find the source image by superimposition of these shares. Alignment of these shares at the time of superimposition plays an important role in decryption. The first pixel of first share is superimposed on the first pixel of second share. Continuing in this manner all pixels of share1 are superimposed on the corresponding pixels of share2. This will provide the top one third portion of the source image. The superimposition of share3 and share4 provides the middle third portion of the image. Similarly, the bottom one third Portion is obtained by superimposing share5 and share6. Having obtained the three parts of the image, the top one third portion is placed first. The middle third portion is appended at the bottom of the top portion. Finally, the bottom portion is appended at the bottom of the middle portion to reconstruct the original image.

Having obtained the three horizontal portions, constructed by superimposing a couple of shares in respective manner, the next task is to align these portions in a proper sequence to get the source image. The clear advantage of our approach manifests itself in dealing with large sized image. Since we have divided the image in three portions we have to deal with smaller portions for superimposition thereby facilitating the encryption and decryption of the large sized images. If all six shares are superimposed, as usually done in (n, n) visual cryptography the source image cannot be obtained.

In our proposed solution it is possible that by combining all the shares we can not obtained the source image still all information is available in these shares. If we combined all n shares but we cannot obtained the source image. If we change the alignment of these shares we are in the position to getting the source image. In our proposed method if we combine only k (k=2) predefined shares and obtained some portion of the source image after this we again combined another k (k=2) predefined shares and obtained another portion of source image. This procedure continues till all the set of k (k=2) predefined shares ended. This portion of information also combined as parts of any image for obtaining the source image. Here we do not superimpose parts of image. Align this resultant portion of image for obtaining the source image. In our Result analysis we consider the value of k=2, and share1 and share2 for one portion of image, share3 and share4 for one portion of image and lastly share5 and share6 for one portion of image.



Decryption process

Fig 2

3.3 Advantage of Proposed Method

This scheme is most suitable in such cases when the source image size is large. When the size of shares is large and not compatible on slide then this is very much suitable because source image braked in more images so shares size resize and take less place on transparencies,

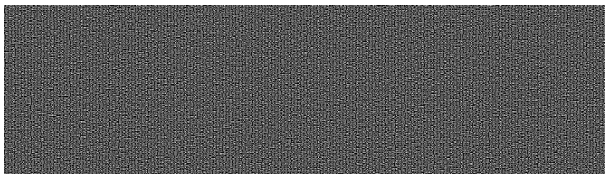
4 RESULT ANALYSES

In this section, we provide experimental results to illustrate the effectiveness of the proposed method. Experiment based on black and white image.proocessing of back and white image easy in comparison of color image .same proposed method may be applied for color image. The result of the proposed Method is implemented in MATLAB 7.9 running on Windows 7 computer. We consider Lena image as a source image of size 480*306. We apply (2, 2) visual cryptography scheme for this image and share1 to share6 of size 960*204

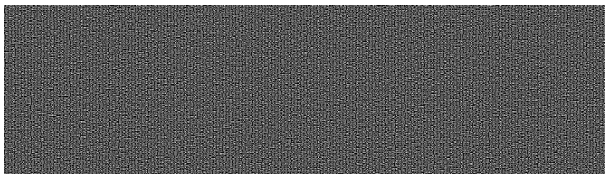
generated with the help of p1, p2, p3. Portion p1conntains upper one third portion of source image, Portion p2 contains Middle one third portion of source image and Portion p3 contains last one third portion of the source image. simply by combining these portion in order of p1appended by p2 and result of this appended by p3 source image can be recovered.source.image may portioned in more than three portion as in proposed method.

Source image(480*306)

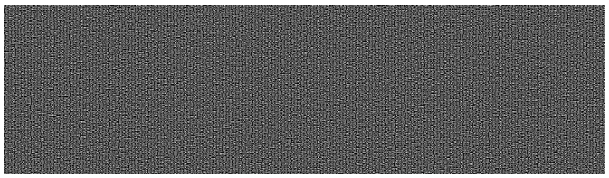
Fig 3



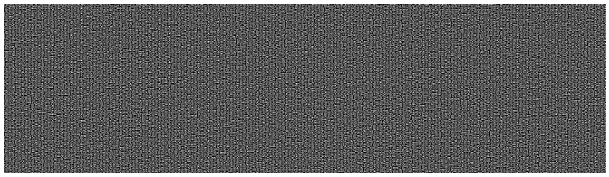
Share1 (960*204)



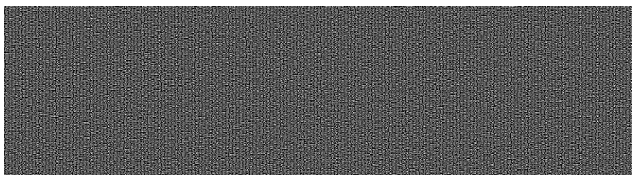
Share2 (960*204)



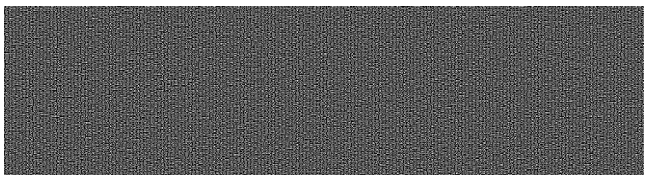
Share3 (960*204)



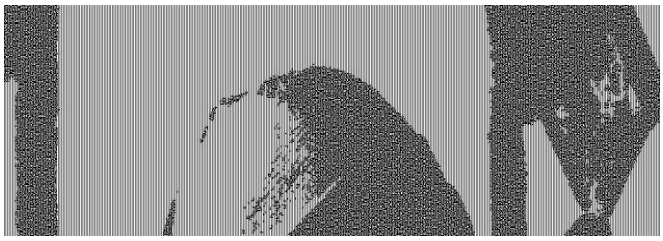
Share4 (960*204)



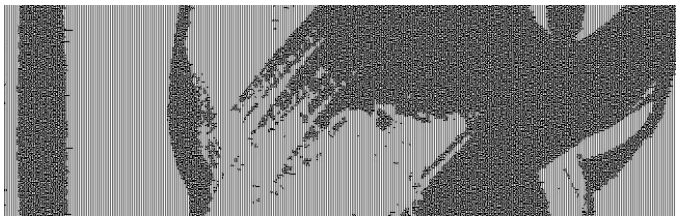
Share5 (960*204)



Share6 (960*204)



Portion p1(superimposition of Share1 and Share2)
(960*204)



Portion p2(superimposition of share3 and share4)

(960*204)

Portion p3 (superimposition of share5 and share6)
(960*204)

After Alignment of these three portion

Recovered Source image (order of images p1, p2 ,p3)(2880*612)

5 CONCLUSIONS

By applying the proposed method we can say that alignment is an important parameter of visual cryptography. If required shares are not superimposed as per required alignment then the source image cannot be recovered still source image is inside the shares. As in given proposed solution if all 6 shares are available but source image cannot be obtained by superimposition of all 6 shares. If these shares are superimposed and align in predefined manner than source image can be recovered. This method provide higher security on the basis of alignment in comparison of existing visual cryptographic schemes, because they are based on superimposition of all or required shares. Proposed method is very useful for large size images.

6 REFERENCES

[1]. M.Naor and A.Samir Visual Cryptography-Advances in cryptology Eurocrypt 1994,1.-12

[2]. M.Naor and A.Samir Visual Cryptography-in a D..Sentish editor,Advances in Cryptology volume 950,pages1-12,springer verlag,1995

[3] C.N. Yang, Visual cryptography: An introduction to visual secret sharing schemes, Department of Computer Scienceand Information Engineering National Dong Hwa UniversityShoufeng , Hualien 974, TAIWAN, access on June 07

[4] S. Cimato and C.N. Yang. Visual cryptography and secret image sharing. CRC Press, Taylor & Francis, 2011.

[5] F. Liu, C.K.Wu, and X.J. Lin. The alignment problem of visual cryptography schemes. In Designs, Codes and Cryptography, volume 50, pages 215-227, 2009

[6] A. Shamir. How to share a secret. In Communications of the ACM, volume 22 (11), pages 612-613, 1979.

[7] C. Blundo, A. De Santis, and D.R. Stinson. On the contrast in visual cryptography schemes. In Journal of Cryptology, volume 12(4), pages 261-289, 1999.

[8] Jim Cai, A Short Survey On Visual Cryptography Schemes, 2004, http://www.cs.toronto.edu/~jcai/paper.pdf

[9] Li Bai , A Reliable (k,n) Image Secret Sharing Scheme by,IEEE,2006

[10] F. Liu1, C.K. Wu1, X.J. Lin, Colour visual cryptography schemes, IET Information Security, July 2008

[11] Adi Shamir, How to Share a Secret, Communications of the ACM, Vol. 22, no. 11, pp. 612-613, Nov. 1979

[12] M. Naor and A. Shamir "Visual cryptography:Improving the contrast via the cover base" *IACR Eprint archive*, 1996.

[13] A. Ross and A. A. Othman, "Visual Cryptography for Biometric privacy", *IEEE Transaction on Information Forensics and Security*, vol. 6, no. 1, Mar.2011.