Analysis and Design of Multi Share Secret Message Sharing using Visual Cryptography

Anjali Varshney
CSE, Suresh Gyan Vihar University
Jaipur, Rajasthan, India

Dinesh Goyal
CSE, Suresh Gyan Vihar University
Jaipur, Rajasthan, India

ABSTRACT
Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human visual system. It is secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, the original image is revealed. In last decade Visual Cryptography has evolved as an entity which divides the data into different shares and then embedding is done. This technique is also is less secured. In this paper we propose an encryption algorithm, which is applied on the different shares of the images. Before embedding the image into the cover image, shares are also encrypted for which the size of share images and the recovered image is the same as for the original secret image. Pixel expansion and the quality of the reconstructed secret image has been a major issue of visual secret sharing (VSS) schemes. The proposed scheme maintains the perfect security and the size of the original image.

Keywords
TIFF, secret sharing, Visual Cryptography.

1. INRODUCTION
In the present trend of the world, the majority of people, from one end to the other all over the world to transfer data, technology has advanced so much that prefer using the Internet is the primary medium. With the rapid progress of network technology, multimedia data is transmitted over the Internet comfortably. However, one of the main problems with sending data over the internet is the "Security Threats".

In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography and digital watermarking. Cryptography is a method to conceal information by encrypting it to "cipher texts" and transmitting it to the intended receiver using an unknown key.

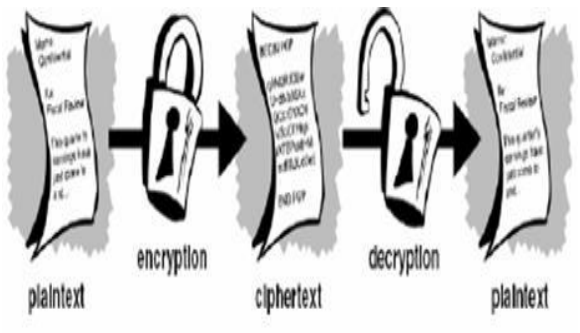

Figure1. Cryptography Scheme

Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats. Digital watermarking is a technique of hiding a message related to digital signal (i.e. image, audio, and video). Digital watermarking is a message that is hidden by a digital signal.

2. VISUAL CRYPTOGRAPHY
Visual cryptography is a cryptographic process which enables visual information (pictures, text, etc.) to be protected in such a way that the decryption could be done by individuals Visual encryption is a special encryption technique to hide the information of the image in a manner that can be interpreted by human vision system. Visual Cryptography offers information safety using easy algorithm. It is a method of encrypting a secret image into shares and the stacking of adequate quantity of shares reveals the secret image. Shares of the secret image are binary images usually represented in transparencies.

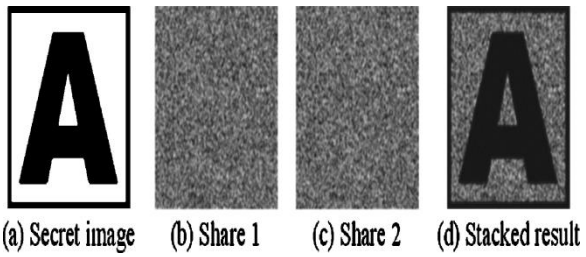

Figure2: Visual Cryptography

In the visual cryptography recovery of the secret can be done by superimposing the share images, hence there is no need of any special software and hardware to decode the image. As shown in figure (2). The secret message can be reconstructed by overlapping the share 1 and share2. The benefit of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS).

3. RELATED WORK
Visual cryptography was first proposed by Noar and Shamir in 1994, applied the Human visual system to decrypt the secret image without any computational and cryptographic algorithms. They proposed a scheme which involved breaking up the image into n shares so that only someone with all n shares could decrypt the secret image by superimposing the shares. They assume that the image is composed of black and white pixels, and each pixel is encrypted separately.

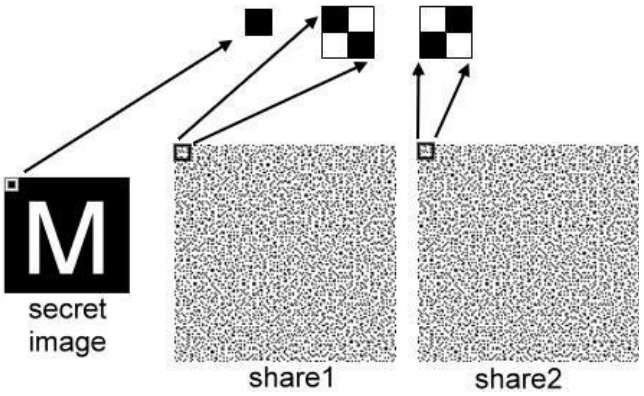

Figure3: Noar and Shamir Scheme

To encode a secret employing a (2,2) VC scheme, the original image is divided into two shares such that each pixel is replaced with a non-overlapping block of two or four sub-pixels in the original image. Anyone, having some shares will not be able to decode the original image. In this scheme the black pixels can be reconstructed perfectly but the white pixels cannot.

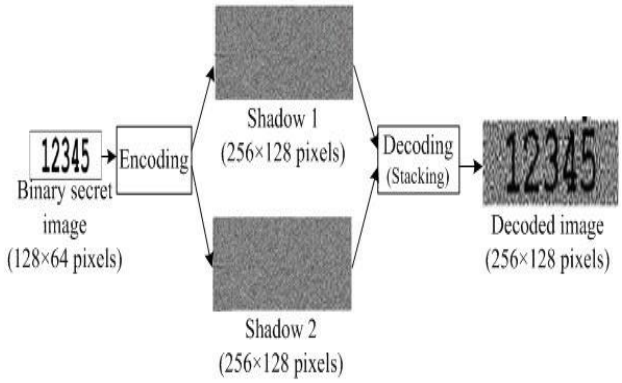

Figure4: How to hide a secret message

The visual cryptography schemes were applied to only black and white images until the year 1997. Verheul and Van Tilborg [17] proposed the first colored visual cryptography scheme. A colored secret image uses the concept of arcs to construct a colored visual cryptography scheme. One pixel is transformed into m sub pixels, and each sub pixel is divided into c color regions in c-colorful visual cryptography scheme. There is only one color region colored, and all the color regions are black in each sub pixel. The color of one pixel depends on the correlation the between stacked sub-pixels. The pixel expansion m is c× 3 for a colored visual cryptography scheme with c colors. The pixel expansion to c × 2 of Verheul and Van Tilborg is improved by Yang and Laih. But in both of the schemes, the shares generated were meaningless.

Chang and Tsai [19] implemented color visual cryptography scheme for sharing a secret color image and also to generate the meaningful share to transmit secret color image. In the color visual cryptography for a secret color image there are two significant color images are selected as cover images which are the same size as the secret color image.

The Color Visual Cryptography is a visual sharing process, wherever the original color picture is converted in to three color components red, natural and blue. These three components become halftone images and when overlapping these gives, three color components, which show meaningful visual information.

Pixel expansion and the quality of the reconstructed secret image has been a major issue of visual secret sharing (VSS) schemes. The proposed scheme maintains the perfect security and the size of the original image.

4. PROPOSED WORK

There are many visual cryptography schemes have been developed. All of the schemes divide the message image into two shares. The proposed scheme increases the security of secret message by providing the encrypted shares. In the proposed scheme first we convert the RGB image into grayscale image and then the grayscale image (containing the secure data) is splitted into four shares by using visual cryptography to provide better security. Figure 1 show the message image. Figure 2 show the grayscale image equivalent to message image. A Random Matrix is created of the size of share and the shares are encrypted with this random matrix, which is like as a security key for client to server. The information hiding includes both information embedding algorithms and information extraction algorithms. Embedding is an information hiding process, while extraction is the restoration process of secret information. Therefore extraction operation is the inverse operation of embedding operation.

There are 7-tuples defined in proposed visual cryptography scheme:

1. ‘S’ denotes the secret image (Which has to be protected).
2. ‘S1’, ‘S2’, ‘S3’ and S4’denotes the four different Secret shares of Secret Data.
3. ‘ES1’, ‘ES2’, ‘ES3’ and ‘ES4’ denotes the encrypted shares generated encryption algorithm.
4. ‘CE’ denotes the composite image of encrypted shares.
5. ‘C’ denotes the cover image in which the secret image is to be embedded.
6. ‘E’ denotes the embedded image generated from embedding algorithm.

The following algorithm is used in proposed scheme.

Step 1: Read Input Secure Data ‘S’ and convert it into gray scale image.
Step 2: Create 4 different shares of secret image by taking out bit-I of each pixel and save to share-i.
Step 3: Repeat this process for 4 shares.
Step 4: Generate a random number matrix in MATLAB.
Step 5: Shares are encrypted by performing X-OR operation of shares with random matrix.
Step 6: Find the composition of encrypted shares.
Step 7: Read Input a Cover image where the size of secret image and cover image should be the same.
Step 8: Embedded the composited image of encrypted shares with cover image.
Extract the original image:
Step 9: Extract the Random matrix which is like a security key.
Step 10: Again performing the X-OR operation of encrypted shares with extracted random matrix.
Step 11: Find the original secret message.

5. COMPUTING PEAK SIGNAL-TO-NOISE RATIO (PSNR)

The ratio between the maximum possible power of the signal and the power of corrupting noise that affects the reliability of watermark illustration is known as phase peak signal-to-noise ratio (PSNR). It is represented in terms of logarithmic decibel scale due to wide range of signals.

For measuring performance of algorithm we need to check The Peak Single to Noise Ratio (PSNR). PSNR is a common measure of the quality of Embedded Image.

Calculating PSNR using following formula:

$$PSNR = 10log_{10}((255)^2/MSE)db$$

The higher the pixel value the better the quality of the reconstructed image.

6. SIMULATIONS AND RESULTS

For calculation of Peak Signal to Noise Ratio (PSNR) for the analysis and simulation algorithms, we have used MATLAB software.

The information hiding includes both information embedding algorithms and information extraction algorithms. Embedding is an information hiding process, while extraction is the restoration process of secret information. Therefore extraction operation is the inverse operation of embedding operation. As the better performance of the proposed visual cryptography scheme, we use the Secret Data as shown in Figure (5) and in figure (6) show the gray scale image of this secret data.

Figure5: Secret image (S)

Figure6: Gray Scale Image

After converting RGB image into gray scale image we split the secret image into 4 shares by taking out bit i of each pixel and save to share i. we use the 4 MSB's of each pixel to create the shares. Figure (7) shows the shares of secret image. When the shares are created, a random matrix is generated in MATLAB which is like as key for host. All the shares are encrypted by performing the X-OR operation with Random matrix. Figure (8) shows the encrypted shares. Figure (9) shows the composite image of encrypted shares which is to be embedded into cover image. In a data hiding procedure, the host image must not be degraded too much, otherwise the quality of the embedded image or stego-image will not be acceptable, and the embedded data easily detected.

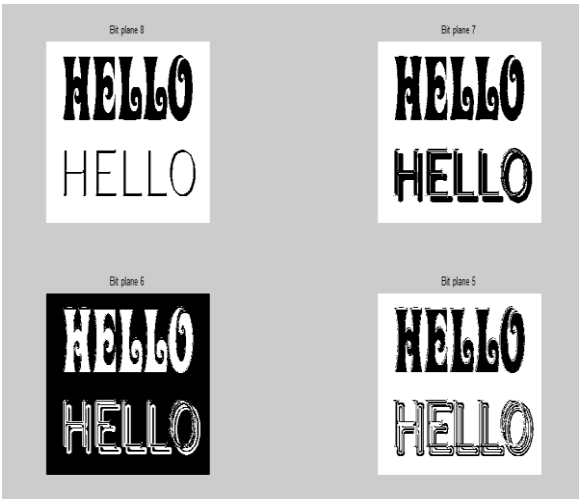

Figure7: Shares of secret Image (S_1, S_2, S_3, S_4)

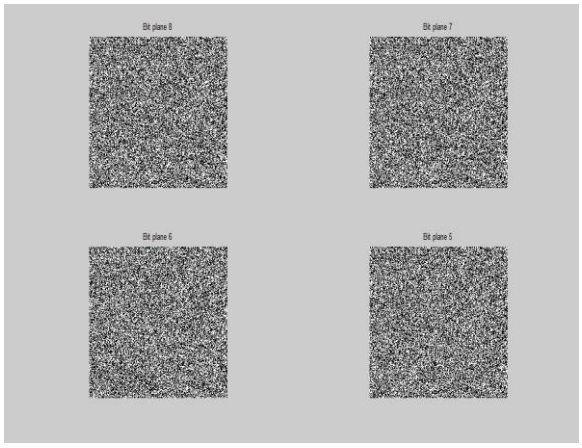

Figure8: Encrypted shares (ES_1, ES_2, ES_3, ES_4)

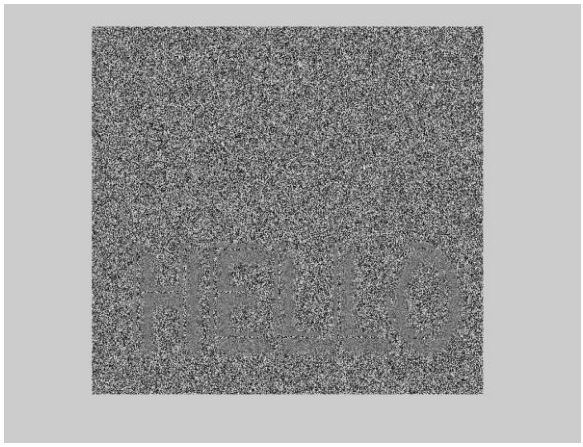

Figure9: Composite image of encrypted shares (CE)

6.1 Embedding Process

In the embedding process, we embed the random matrix with the LSB bit and 4th share is embedded with the 2nd LSB bit of Red color of cover image. Same process is done for share 3, 2 and one. Only two LSB of each color of cover image is used to embed the secret image.

Figure 10 shows the cover image without embedding the message.

Figure10: cover image (C)

Human eye cannot easily find this share in cover object. At the recipient side we apply the extraction process. We easily find the secret data using overlapping these shares. Figure 11 shows the cover image after embedding the secret image**.**

Figure11: Embedded image (E)

6.2 Extraction Process

In extraction we first extract the random matrix and all the shares which are embedded into the cover image. After extracting the encrypted shares, these can be decrypted by performing the X-OR operation with random matrix which is extract from the cover image. Figure 12 shows the decoded message after decryption process performing on receiver side.

Figure12: Decoded Image

After decoding the message we calculate the PSNR (Peak signal to Notion Ratio) to check the image quality. We find the PSNR for decoded message is 38.18 db. When PSNR is higher than 30, recomposed image has a very good quality and the eye could hardly tell the difference between the original and the recomposed image. We got resultant PSNR is greater than 38.18 db which shows our proposed scheme is good and it provides robustness also. So the proposed visual cryptography schema is good to transfer the secret data over communication channel.

7. CONCLUSION

Security has gained lot of importance as information technology is widely used. Visual cryptography scheme promotes some level of security. The proposed scheme

increases the security of secret message by providing the encrypted shares.
The decoded secret image quality is improved. In our scheme the results are better then and the size of the retrieve image is the same as the original. The original secret image is divided into shares in such a way that after decryption operation of qualified shares, we reveal the secret image.

Moreover, the computational complexity of our proposed scheme is very low, so it is suitable for real-time applications.

From the results it can be inferred that the new algorithm has merits in terms of configuration requirement, optimal running time, ease of use and a better PSNR value & reduced communication overhead.

The proposed scheme has shown less pixel expansion which is desirable and good for the final retrieval of the secret image.

8. FUTURE WORK

Visual Cryptography has wide area of application in today's world. Future works will provide highest level of security and better performance.

Further extend this work to use this technique by creating 8 shares of secret image. Also consider that secret image can be hidden behind any audio or video. Future work will be on multiple image visual cryptography i.e. multiple secret images can be hidden behind a single image.

9. REFERENCES

[1] M. Naor, A. Shamir, in: A. De Santis (Ed.), Visual Cryptography, Advances in Cryptology: Eurpocrypt'94, Lecture Notes in Computer Science, Vol. 950, Springer, Berlin, 1995, pp. 1–12.

[2] H.-C.Hsu, T.-S. Chen,Y.-H.Lin, "The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing", in Proceedings of the 2004 IEEE International Conferenceon Networking, Sensing & Control, Taipei, Taiwan, pp.996–1001, March2004.

[3] H.-C.Wu, C.-C.Chang, "Sharing Visual Multi-Secrets Using Circle Shares",Comput. Stand. Interfaces 134 (28), pp.123–135,(2005).

[4] Chin-Chen Chang, Jun-Chou Chuang, Pei-YuLin, "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conferenceon Paralleland Distributed Systems (ICPADS'05), 2005.

[5] Liguo Fang, Bin Yu, "Research On Pixel Expansion Of (2,n) Visual Thres hold Scheme", 1st International Symposiumon Pervasive Computing and Applications, pp.856-860, IEEE.

[6] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[7] Gajanand Sharma, Amit Gupta, Dinesh Goyal, "Analysis & Design of Visual Cryptography Using Moving Image", Volume 3 No. 12, Nov -Dec 2013, ISSN 2223-4985.

[8] "A Comprehensive Study on Various Visual cryptography Schemes with an Application", Madhuri Ghuge, Prof.Kanchan Doke, Volume 4, Issue 2, February 2014, ISSN 2250-2459, ISO 9001:2008.

[9] Wen-Pinn Fang, "Visual Cryptography In Reversible Style", IEEE Proceedingon the Third International Conference on Intelligent Information Hidingand Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C,2007.

[10] Jen-Bang Feng, Hsien-ChuWu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, "Visual Secret Sharing For Multiple Secrets", Pattern Recognition 41, pp.3572–3581, 2008.

[11] Mustafa Ulutas, Rıfat Yazıcı, Vasif V.Nabiyev, Güzin Ulutas, (2,2)- "Secret Sharing Scheme With Improved Share Randomness",978-1-4244-2881-6/08,IEEE,2008.

[12] Juan Zhou, Shijie Jia, "Design and Implementation of Image Hiding System Based on LSB", Computer Technology and Development, vol. 17 (05), 2007, pp. 114-116, doi: cnki: ISSN: 1673-629X.0.2007-05-034.

[13] S.J.Shyu, S.Y.Huanga, Y.K.Lee, R.Z.Wang, and K.Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol.40, Issue 12, pp.3633-3651,2007.