International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Encrypting Multiple Images Using Visual Secret Sharing Scheme

Isha M. Padiya[1], G. D. Dalvi[2]

[1]Amravati University, P.R.Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Maharashtra, India

[2]Professor, Amravati University, P.R.Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Maharashtra, India

Abstract: ***Visual Cryptography is an encryption technique where a secret image is cryptographically encoded into n meaningless share images. A basic model for visual cryptography for natural images was proposed by Naor and Shamir. Security has gained a lot of importance as information technology is widely used. Cryptography refers to the study of mathematical techniques and related aspects of Information Security like data confidentiality, data Integrity, and of data authentication. Visual cryptography is a process where a secret image is encrypted into shares which refuse to divulge information about the original secret image. Its strength is a fact that the decryption of the secret image is through human visual system without computation. This paper provides a formulation of encryption for multiple secret images, which is a generalization of the existing ones, and also a general method of constructing visual secret sharing schemes encrypting multiple secret images.***

Keywords: Visual Secret Sharing (VSS), Visual Cryptography (VC), Information-theoretic security, multiple secret images, image processing.

1. Introduction

VISUAL cryptography (VC), which was proposed by Naor and Shamir, allows the encryption of secret information in the image form [1]. With the network is more and more popular, the hackers utilize leak of the Internet to steal information that they want. Therefore, secure data transmitting becomes very important. In the recent years, generally using the traditional cryptology to avoid the data to be altered, but it needs complex computation to decode. In order to reduce the computation and furthermore secure the data, Naor and Shamir [1] proposed a new cryptology called visual cryptography in 1994. Without huge calculation, it can restore encrypted messages by stacking two shares via human visual system to identify. The first visual cryptography scheme is used for the black-and-white image in disorder to embed the confidential message. These disordered images are called "shares" that one of them may regard as the cipher text and the other treats as the key. Hackers cannot decrypt the secret message from one share. As shown in fig.1.Later on this theory, visual cryptography can extend as (k, n) – threshold visual secret sharing scheme that divides n transparencies into secret information. When be decoded, the owner must have k or more shares to stack. In 1998, Chen and Wu proposed a new visual cryptography scheme. It improves the drawback of the conventional visual cryptography that two share images only can embed.

In a k-out-of-n scheme of VC, a secret binary image is cryptographically encoded into n shares of random binary patterns. The n shares are Xeroxed onto n transparencies, respectively, and distributed among n participants, one for each participant.

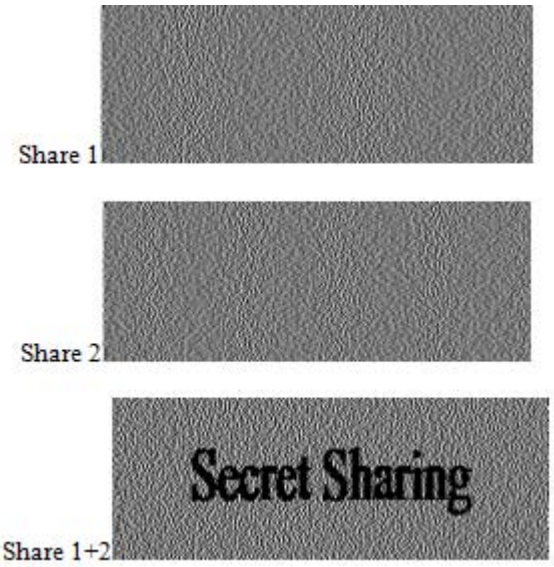

Figure1: Example of visual Cryptography

No participant knows the share given to another participant. Any k or more participants can visually reveal the secret image by superimposing any k transparencies together. The secret cannot be decoded by any k-1 or fewer participants [4].There are many algorithms to encrypt the image in another image, but a few of them have been in visual cryptography for colour image. In this paper, the different approach have been produced for the visual cryptography for colour image, the proposed algorithm splits a secret image into two shares based on three primitive colour components.

2. Visual Cryptography Model

A printed page of cipher text and a printed transparency (which serve as a secret key) . The original clear text is revealed by placing the transparency with the key over the page with the cipher, even though each one of them is indistinguishable from random noise. The model for visual

secret sharing is as follows in fig.2. There is a secret picture to be shared among n participants. The picture is divided into n transparencies (shares) such that if any m transparencies are placed together, the picture becomes visible. If fewer than m transparencies are placed together, nothing can be seen. Such a scheme is constructed by viewing the secret picture as a set of black and white pixels and handling each pixel separately [5].

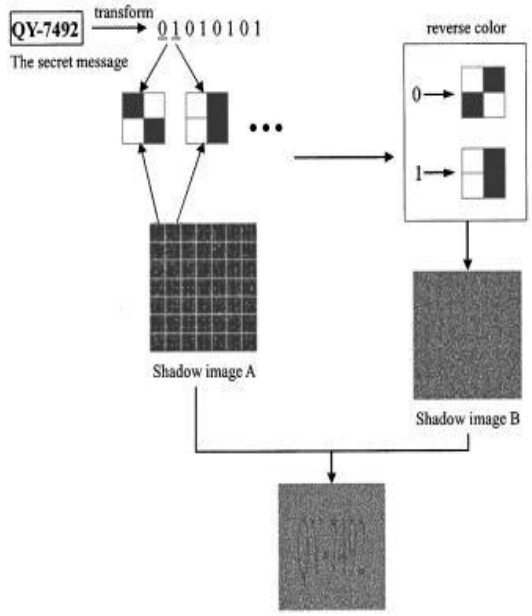

Figure 2: Visual cryptography system

In visual cryptography system the pixels of the image to be encrypted can be applied to the image in different manner. There is a set of n participants (image), and the secret image is divided and encoded into n shadow images called shares. Each participant is encrypted by one share, k out of n participants are needed to combine shares and see secret image, sometime k-1 of shares can not reveal information about secret image. The technology makes use of the human vision system to perform the OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human's mind [6].

3. Previous Scheme

A.Black And White Visual Cryptography Scheme

The visual cryptography scheme is used for encrypting the information. Visual cryptography is a one of the technique of encryption which is used to hide the information in an image; decryption can be done by human visual system. By using only this type of cryptography, no one is able reuse the data. The image which we can recover after decryption will not be same as original image so it cannot be reused. There are number of visual cryptography schemes in existence. Some of them are described below.

1) Sharing Single Secret Image*:* In this type of visual cryptography scheme, the secret image is divided into exactly two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with remote voting system that uses 2 out of 2 secret sharing schemes for authentication purpose. To reveal the original image, these two shares are required to be stacked together. Naor and Shamir's proposed encoding scheme to share a binary image into two shares i.e. Share1 and Share2. If pixel is white one of the above two rows of table from fig 2 is chosen to generate Share1 and Share2, likewise If pixel is black one of the below two rows table of fig 2 is chosen to generate Share1 and Share2. Here each share of pixel p is encoded into two white and two black pixels. Each share alone gives no hint about the pixel p. That is share is not provide any information whether it is white or black. Secret image is shown only when both shares of images are overlaid or superimposed. Wen-Pinn Fang suggested non pixel expansion scheme in which the pixel expansion was minimal. These all schemes have their own disadvantages

2) Sharing Multiple Secret Images*:* Wu and Chen [10] were first researchers to present the visual cryptography schemes to share two secret images in two shares. He hidden two secret binary images into two random shares, that is A and B, such that the first secret can be seen by stacking the two shares, denoted by A⊗ B, and the second secret can be obtained by first rotating AΘ anti -clockwise. They designed the rotation angle Θ to be 90◦. However, it is easy to obtain that Θ can be 180◦ or 270◦. To overcome the angle restriction of Wu and Chen's scheme [10].Wu and Chang also refined the idea of Wu and Chen [10] by encoding shares to be circles so that the restrictions to the rotating angles (Θ = 90◦, 180◦ or 270◦) can be removed.

S J Shyu were first researchers to advise the multiple secrets sharing in visual cryptography. This scheme encodes a set of n≥2 secrets into two circle shares. In this the n secret image can be obtained one by one by loading the first share and the rotated second shares with n different rotation angles. For encoding purpose unlimited shapes of image and to remove the limitation of transparencies to be circular, Fang [4] offered reversible visual cryptography scheme. In this scheme two secret images which are encoded into two shares; one secret image appears with just stacking two shares and the other secret image appears with stack two shares after reversing one of them. Jen-Bang Feng [8] developed a visual secret sharing scheme for hiding multiple secret images into two shares. This scheme analyses the secret pixels and the corresponding share blocks to construct a stacking relationship graph. In this the vertices denote the share blocks and the edges denote two blocks stacked together at the desired decryption angle. By using this graph and the pre-defined visual pattern set, two shares are generated. To provide more randomness for generating the shares Mustafa Ulutas advised secret sharing scheme based on the rotation of shares. In this scheme shares are of rectangular shape and they are created in a fully random manner. Stacking of the two shares reconstructs the first secret. Rotating the first share by 90° counter clock wise and stacking it with the second share reconstructs the second secret. Tzung-Her Chen proposed the multiple image encryption schemes by rotating random grids, without using any pixel expansion and codebook redesign. To encode four secrets into two shares and recovering the reconstructed images without distortions

Zhengxin Fu intended a rotation visual cryptography scheme. Rotational visual cryptography scheme construction was based on correlative matrices set and random permutation, which can be used to encode four secret images into two shares. Jonathan Weir suggested sharing multiple secrets using visual cryptography. A master key is generated for all the secret images; correspondingly, secret images are shared using the master key and multiple shares are obtained. This kind of scheme allows dividing a secret into K number of shares. Then the secret can be open from any N number of Shares among K. The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption. The application of this scheme is usually found with banking system. In the joint accounts, three shares are created. One is reserved with bank's server, second is given to the one customer for the joint account and third share is delivered to the second customer. Hence both customers are able to access the account [9]

All the above schemes can be used only to share the black and white secret images, but it is need of time that schemes should also support color images. To meet this demand we are going to review on the shares of the color images

B. Colour Visual Cryptography Schemes

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colour visual cryptography scheme was developed by Verheul and Van Tilborg. Colour secret images can be shared with the concept of arcs to construct a colour VCS. In colour VCS one pixel is converted into m sub pixels, and each sub pixel is further divided into c colour regions. In each sub pixel, there is exactly one colour region is colour, and other colour regions are black. The colour of one pixel depends on the interrelations between the stacked sub pixels. For a coloured visual cryptography scheme with c colures, the pixel expansion m is c× 3. Yang and Laih improved the pixel expansion to c × 2 of Verheul and Van Tilborg. But in both of these schemes share generated were random. To share true-colour images Lukac and Plataniotis developed bit-level based scheme by operating directly on S-bit planes of a secret image.

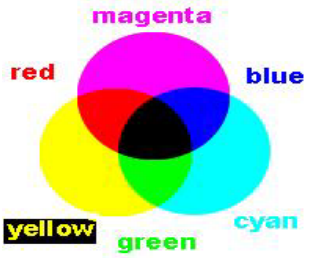

Figure 3: Color scheme

1) To hide a colour secret image into multiple colour images it is desired that the generated camouflage images contain less noise. For this purpose R. Youmaran et al invented an improved visual cryptography scheme for hiding a colour image into multiple colour cover images. This scheme provides improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals. By considering colour image transmission over bandwidth constraint channels a cost effective visual cryptography scheme was invented by Mohsen Heidarinejad et al. This scheme offers a perfect reconstruction while producing shares with size smaller than the size of input image using maximum separable distance. This scheme provides pixel expansion less than one. Haibo Zhang et al presented a multi-pixel encoding which can encode a variable number of pixels for each run to improve the speed of encoding. F. Liu [6] developed a colour visual cryptography scheme under the visual cryptography model of Naor and Shamir with no pixel expansion. In this scheme the pixel expansion is not increasing the number of colours of a recovered secret image is increased.

2) Visual Cryptography technique is used to protect image-based secret information. In this scheme we have proposed a technique called random sequence to divide an image into n number of shares. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimizes but the distorted shares may arise suspicion to the hacker's mind that some secret information is passed. The original image can be encrypted using a key to provide more security to this scheme. The key may be a text or a small image. Steganography can be used by enveloping the secret shares within apparently innocent covers of digital picture. This technique is more effective in providing security from illicit attacks.

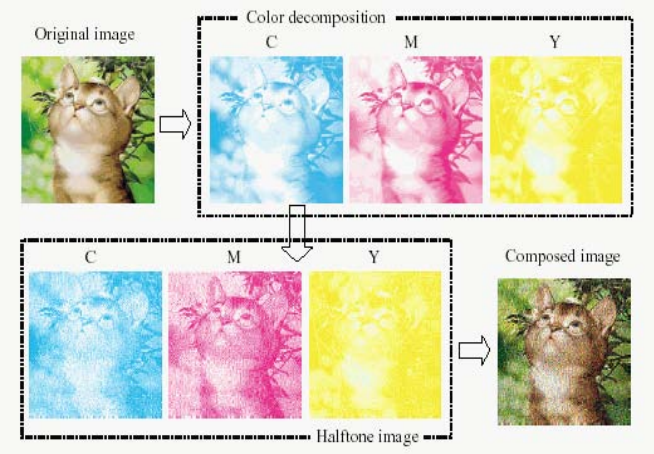

Figure 4: Color Visual Cryptography

3) In this proposed idea comes from the fact that VSS schemes need no computation in decryption and the generic idea behind the proposed system is to introduce security to a weakly secure visual secret sharing scheme. That is, it is possible to assume in VSS schemes that we do not have (or it is a bother to use) computers in decryption. In such a scenario, it may be difficult to analyse every share exhaustively without computers, for instance, we would not investigate combinations and/or statistical data of pixels in shares. Based on this observation, we can relax the unconditional security notion of (k ,n) -threshold VSS schemes to a weaker notion in such a way that it is secure if the image obtained by stacking k-1 or fewer shares seems to be a random dot image. We say that such VSS schemes are weakly secure VSS schemes or simply WS-VSS schemes hereafter. On the other hand, we abbreviate the

unconditionally secure VSS scheme as US-VSS schemes in this paper. We note here that, in several previous studies on VSS schemes for black–white binary secret images, the weak security notion discussed above was implicitly used without sufficient security mechanisms in their constructions of US-VSS schemes.

Hence, it is important to discuss the security of WS-VSS schemes not only in terms of minimizing the pixel expansion but also to evaluate the security of these previous studies in VSS schemes. Motivated by the above background, we formally define a WS-VSS scheme and give its security analysis.

4. Proposed Algorithm

Step1: Secret color image.

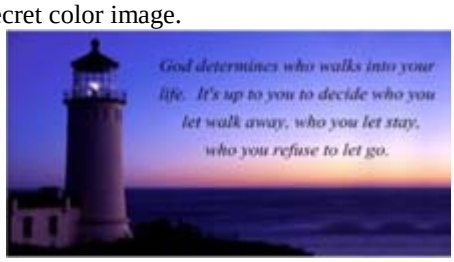

Figure 5: Secret Colour Image

Step2: The secret colour image as shown in Fig.3 is decomposed into three planes namely, red, green, blue, RGB. Fig.4 shows the three primitive colour components of secret colour image, where each image has 256 levels of the corresponding primitive colour, and each pixel represented by 24 bits.

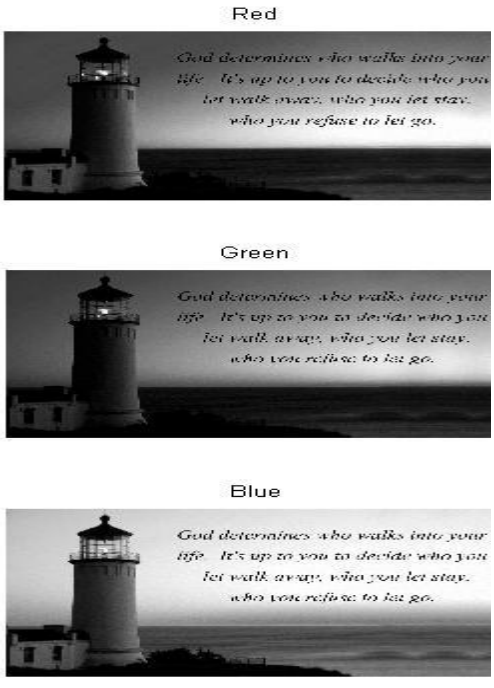

Figure 6: Primitive colour (R, G, and B) component

Step3: Encrypt the colour space

Step4: Half tone image

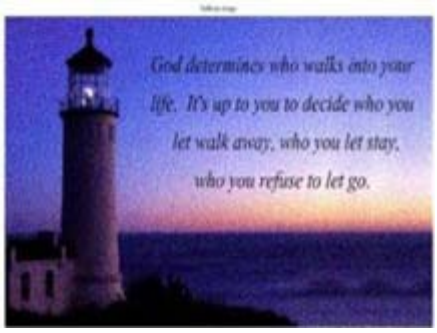

Figure 7: Halftone image

Step5: Two shares will be generated by the following method.
Method:
1. Read the pixel value with respect to ii (number of rows of secret image) and jj (number of columns of secret image).
sij = I(ii,jj);
2. Pixel reversal.
sij1 = 255-sij;
3. Read each pixel and convert to shares.
4. Reduce sij.
5. Pixel reversal.
6. Take difference of two random generator with original pixel.
7. Pixel reversal.

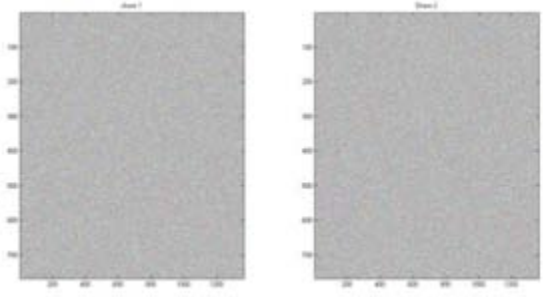

Figure 8: Share1 and Share 2

Step 6: After mixing share1 and share 2 with three planes of RGB we obtain decrypted image.

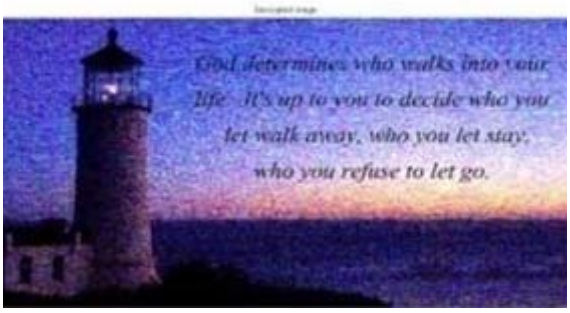

Figure 9: Decrypted image

Step7: Size of the decrypted image is same as secret image.

5. Conclusion

Visual cryptography exploits human eyes to decrypt secret image with no computation required. As we are divide the input into multiple visual encrypted parts. The given input image can be divided into secret sharing parts which can be used in future for Encryption. We would be using genetic

algorithm for implementation of this Encryption technique. Paper suggests VSS, but we would be developing as it is a better and more robust algorithm for image encryption. This paper exploits the techniques of Halftone technology. The proposed scheme revealed good security due its randomness.

6. Acknowledgment

We thank immensely our management for extending their support in providing us infrastructure and allowing us to utilize them in the successful completion of our research paper.

References

[1] Adi Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
[2] Moni Naor and Adi Shamir, “Visual cryptography,” in Proceedings of Advances in Cryptology – Eurocrypt ’94, Perugia, Italy, 1994, vol. 950 of Lecture Notes in Computer Science, pp. 1–12, Springer-Verlag.
[3] Pankaja Patil, Bharati Pannyagol, “Visual Cryptography For Color Images Using Error Diffusion And Pixel Synchronization”, International Journal of Latest Trends in Engineering and Technology (IJLTET)
[4] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson, “Extended capabilities for visual cryptography,” Theoretical Computer Science, vol. 250, no. 1–2, pp. 143–161, 2001.
[5] Mitsugu Iwamoto and Hirosuke Yamamoto, “A construction method of visual secret sharing schemes for plural secret images,” IEICE Trans. Fundamentals, vol. E86-A, no. 10, pp. 2577–2588, 2003.
[6] Manami Sasaki and Yodai Watanabe, Formulation Of Visual Secret Sharing Schemes
[7] Encrypting Multiple Images, 2014 IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP)
[8] Thomas M. Cover and Joy A. Thomas, Elements of Information Theory, Wiley-Interscience, 2nd edition, 2006.
[9] Douglas Robert Stinson, Cryptography: Theory and Practice, Chapman & Hall, CRC, 3rd edition, 2005.
[10] Verheuland H. V. Tilborg, ”Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes. ”Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.