INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ENCRYPTING MULTIPLE IMAGES USING VISUAL SECRET SHARING SCHEME

MISS ISHA M. PADIYA[1], PROF. G. D. DADVI[2]

1. ME Student, Amravati University, P. R. Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Maharashtra, India.
2. Assist. Prof. Amravati University, P. R. Pote (Patil) Welfare & Education Trust's college of Engineering & Management, Maharashtra, India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

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. 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

Corresponding Author: MISS. ISHA M. PADIYA

Access Online On:

www.ijpret.com

How to Cite This Article:

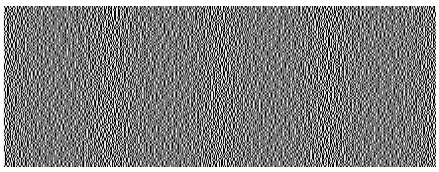
Isha M. Padiya, IJPRET, 2015; Volume 3 (9): 422-430

PAPER-QR CODE

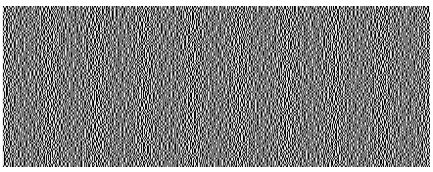
INTRODUCTION

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.



Share 1



Share 2

Share 1+2

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.

1. 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].

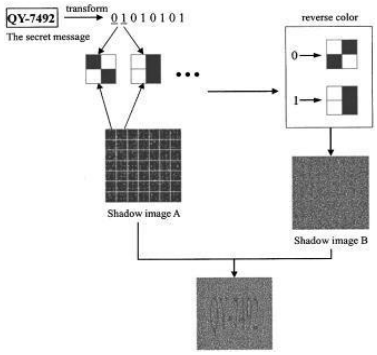


Figure 2: Visual cryptography system

2. 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 A Θ 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.

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.

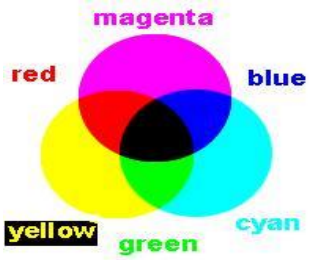


Figure 3: Color scheme

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.

3. Visual Secret Scheme

An algorithm in cryptography created Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore sometimes the *threshold scheme* is used where any k of the parts are sufficient to reconstruct the original secret.

Mathematical definition

The goal is to divide secret S (e.g., a safe combination) into n pieces of data $S_1, \ldots, S_n$ in such a way that:

1. Knowledge of any k or more S_i pieces makes S easily computable.
2. Knowledge of any $k-1$ or fewer S_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).This scheme is called (k, n) threshold scheme. If $k = n$ then all participants are required to reconstruct the secret.

Suppose we want to use a (k, n) threshold scheme to share our secret S, without loss of generality assumed to be an element in a finite field F of size P where $0 < k \leq n < P; S < P$ and P is a prime number.

Choose at random $k-1$ positive integers $a_1, \cdots, a_{k-1}$ with $a_i < P$, and let $a_0 = S$. Build the polynomial. $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$ Let us construct any n points out of it, for instance set $i = 1, \cdots, n$ to retrieve $(i, f(i))$. Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

4. Proposed Algorithm

Step1: Secret color image.

Figure 4: Secret Colour Image

Step2: The secret colour image as shown in Fig.4 is decomposed into three planes namely, red, green, blue, RGB.

Step3: Encrypt the colour space

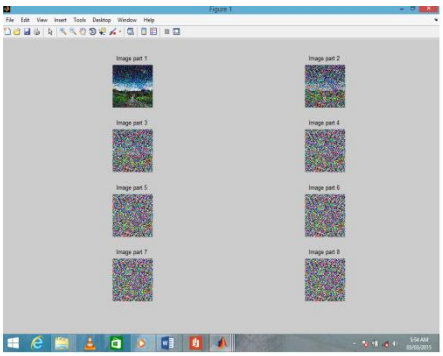


Figure 5: Share1 to Share 6

Step 4: After mixing any share 3 with three planes of RGB we obtain decrypted image.

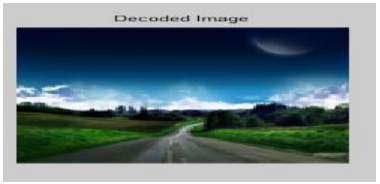


Figure 6: Decrypted image

Step 5: Comparison of original image and decrypted image.

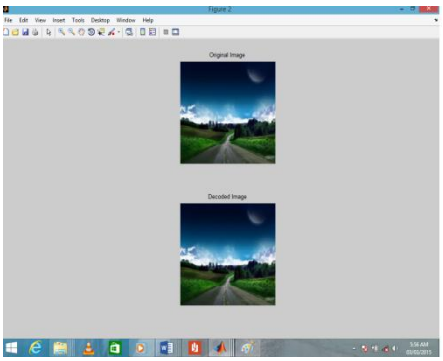


Figure 7: Comparison

Step 6: 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.

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 ComputerScience, 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.