XOR OPERATED VISUAL CRYPTOGRAPHY

Ranbir Sinha[1], Dr. Manish Shrivastava[2]

Abstract: Visual Cryptography is a method for protecting image-based secrets that has a computation-free decoding process. In this paper, we describe a method which can be used to share an image with at least 256 colours into two meaningful cover images. We use a pseudo random number generator and XOR Operator to make cover images pretend to be innocent and do not express any hidden clue about the secret image which is to be shared. Because of the use of pseudo random number generator and the private key, even if the cover images are captured by the hackers, it is much harder to reveal the secret image. The image can be in any standard format. In this paper, symmetric key encryption technique is used. The experimental results support the view of the algorithm and the algorithm is much safer, practical and effective.

Keywords: Visual Cryptography, Secret Image Sharing, XOR Operation, Colour Image, Information Hiding, Image Processing, Private Key.

1. INTRODUCTION

Visual Cryptography [1] is defined as the encryption of text, pictures, etc. in such a way that they can be decoded by the human visual system instead of computational steps. The combination of computer and communication technology makes the development of digital media grow up fast. The rapid and prosperous development and common usage of the internet makes more and more digital data to be transmitted and exchanged via internet. As the internet has advanced with the advancing age, much more information is transmitted over the web conveniently and rapidly. This information can be confidential and private. Since the multimedia data are very easy to spread, duplicate, capture and modify, the convenience of sharing digital data over the internet produces the misappropriation and illegal problems against the intellectual property rights. Though the exchange of information over the web has evolved rapidly, the security aspects have not been evolved at the same rate. Therefore, Security is the crucial problem in the transmission process. Therefore, Visual Cryptography is to build a system such that the confidential messages can be encrypted such that the malicious person is not able to decode easily.

Recently, more and more intellectual property protection schemes have been proposed. Among all, encryption is still the fundamental method to protect the important data files for the purpose of copyright protection, integrity, checking and captioning. But the computation time for encryption and decryption are quite lengthy and the noise-like encrypted results may tempt the interceptor to break it. Therefore, researchers developed the technique of information hiding to conceal the secret image into a cover image. The result is the so called stego image. The secret image can then be delivered out with the help of stego image. The extra information hidden in the stego image is not immediately apparent which enhances the security

of the secret information being transmitted. Even if the stego image is captured by the illegal users, it still has a good chance not to give rise to the suspicion that some secret information is kept hidden inside.

Firstly a plain image and a private key are inserted into cryptographic system. The encryption algorithm produces a cipher image which is sent into receiver through a communication medium. When the cipher image reaches the destination, the receiver enters the private key and the original image is decrypted.

2. BACKGROUND

Many image encryption algorithms have been proposed till now. There are two major categories of image encryption algorithms. They are: -

- Non-Chaos Selective Methods
- Chaos Based Selective or Non Selective Methods

Many of these algorithms are format specific and apply to a specific class of images.

Naor and Shamir [1] introduced a perfectly secure method called visual cryptography for protecting the secret images. Compared with the other traditional encryption/decryption processes the visual cryptographic scheme possesses the advantages of needing only human visual perception to decrypt the secret images, without the need of any complex mathematical operations.

The basic model of visual cryptography consists of “splitting” the image or watermark into two transparencies (shares). Each share looks like random noise, without any clue to disclose the outlines of the secret image. However, the secret image can be revealed simply by superimposing the two shares. Due to this simplicity the model can be used by anyone, even without the knowledge of cryptography and without performing any complex computations.

Chang et.al [2] proposed a visual cryptography-based technique for sharing a secret colour image. Although Chang’s Approach can handle colour image, the number of distinct colours in the secret image is limited. It is quite restricted especially in multiuser environment.

Lin [3] proposed a new colour visual cryptography based scheme to solve limited colour problem by giving different interpretation for the bit pattern used in Chang’s Scheme.

Ateniese et.al [4] proposed a visual cryptography technique using an ordinary image as the colour image, to extend the capability of the visual secret sharing mechanism. However, in Ateniese’s sharing method the secret image is limited to black and white.

Hou and Wu [5] extended Ateniese's visual cryptography model by applying the colour decomposition and the halftone techniques to decompose a secret colour image into three monochrome (cyan, magenta and yellow) halftone images, to finally produce coloured meaningful shadow images.

Hwang and Chang [6] modified Ateniese's visual cryptography model by extending each block from 2X2 sub pixels to 3X3 sub pixels.

Chang et.al [7] extended Hwang and Chang's Scheme to colour image.

The common drawback for [6, 7] is that the contrasts on shares and recovered image are all 2/9 which is worse than Ateniese's Result (1/4).

In this paper, a new information hiding scheme for digital images based on visual cryptography is proposed. We use XOR Operator to compute the binary code for the overlapped blocks in the stacked image. Our Scheme improves Lin's Drawbacks i.e. we use only one operator and does not need a mask share to guarantee the generation of the noise-like shares.

3. THE PROPOSED TECHNIQUE:

We have proposed a technique which will fit to every type of image with some or little modification. The following is an algorithm for 256 colour image. The same with some modification can be used for true colour image.

i.) 256 COLOUR IMAGE

In this paper, we expand each pixel of the image into 3X3 sub pixels block. For a 256 colour image we need only 8 bits (P1 – P8) to record the corresponding colour index in CIT. Thus the ninth sub pixel (P9) to store the palette data which we are going to transmit over the internet. Thus the data is given protection in the image instead of transmitting insecurely it over the web.

Let us consider an example to understand the viewpoint. When we want to dispatch a secret pixel to shares, firstly we count the number of 1s in the sub pixels P1 - P8. Suppose there are n 1s in P1 – P8, we randomly choose ceil ((n-P9)/2) locations of the 1s fill up 1 in share 1 and 0 in share 2 respectively. On the other hand, the remaining ceil ((n+P9)/2) locations of the 1s to fill up 0 in share 1 and 1 in share 2 respectively.

And in the rest of (n – 8) locations containing 0, randomly choose [5 – ceil ((n+P9)/2)] locations to fill up 1 in share 1 and share 2. And finally fill up 0 in the remaining locations. By following the above mentioned procedure we can hide every pixel of the secret image into the shares.

For the value of P9 we put the colour bit (palette data) into the ninth position of the share 1. We use the ninth position of the share 2 to adjust the number of 1s in the corresponding block.

- If n is odd and the colour bit is 0 OR n is even and colour bit is 1, then the ninth position of share 2 is filled by a 1.

- If n is odd and the colour bit is 1 OR n is even and the colour bit is 0, then the ninth position of share 2 is filled by a 0.

By following the procedure, every block has 4 white and 5 black sub pixels in it. This means regardless of colour of the secret image, the probability of them to appear 1 on each share is 5/9. Therefore, this gives no clue about the content of the secret image on the shares.

EXAMPLE: For a secret pixel with colour index 170 (binary value of 170 = 10101010) and the palette data to be stored at P9 is 0, there are 4 1s at the locations of P1, P3, P5 and P7. We first randomly choose ceil ((n-P9)/2) = 2 locations (say P1 & P3) in the share 1 to fill up 1 and the remaining 1s are put at P5 & P7 in share 2. For the rest 0 locations P2, P4, P6 & P8, we randomly choose [5 – ceil ((n+P9)/2)] = 3 locations (say P2, P4 & P6) to fill up 1 in both share 1 and share 2. In the rest unassigned locations in P1 – P9 0s are filled up.

As for the value of P9, we put colour bit in the ninth position of share 1 and a 0 in the ninth position of share 2. Since n is 4 and colour bit is 0, we put 0 in the P9 of share 1 and 0 in P9 of share 2. By doing so, every block has 4 white and 5 black sub pixels in it. It will not leak any secret information contained in the shares.

2. INFORMATION SHARING

The detailed information sharing algorithm is as follows: -

ALGORITHM VISUAL_ENCRYPTION

STEP 1: Obtain the binary code of the secret pixel and 1 bit of the palette data and arrange them in a matrix P1 – P9.

STEP 2: Count the number of 1s in P1 – P8.

STEP 3: Randomly Choose Ceil ((n-P9)/2) locations of the 1s to fill up 1 in share 1 and 0 in share 2. The remaining Ceil ((n+P9)/2) locations of the 1s fill up 0 in share 1 and 1 in share 2.

STEP 4: In the rest of (8 – n) 0 locations randomly choose [5 – Ceil ((n+P9)/2)] locations to fill up 1 in both share 1 and share 2. Fill up 0 in the rest (8 – n) - [5 – Ceil ((n+P9)/2)] locations in both share 1 and share 2.

STEP 5: If (n mod 2 = 1)
If (Colour bit = 1) Then P91=1 & P92=0
Else If (Colour bit=0) Then P91=0 & P92=1 Else

If (Colour bit=1) Then P91=1 & P92= 1
Else If (Colour bit=0) Then P91=0 & P92=0

STEP 6: For every 1s in the share 1 and share 2, fill the corresponding colour of the cover pixel at that location. For every 0s in both of the shares, just leave them as White.

STEP 7: Repeat Steps 1 – 6 until every pixel in the secret image is processed.

END ALGORITHM

3. INFORMATION RECOVERY

The detailed information recovery algorithm is as follows: -

ALGORITHM VISUAL_DECRYPTION

STEP 1: Divide the share 1 and share 2 into 3X3 blocks.

STEP 2: Take the ninth bit (P9) of each block from the share 1. If it is the colour of the cover image, we record it as 1. Otherwise, we record it as 0. When all the colour bits are collected, we can set up the palette table.

STEP 3: Take first 8 bits of each block from both shares. If it is the colour of the cover image, we record it as 1. Otherwise, we record it as 0. By doing so, we can get the binary code from the share 1 and the share 2.

STEP 4: Perform XOR Operation on the binary code. The result is the index number on the CIT. Check with the CIT; we can get the colour of the secret pixel at that location.

STEP 5: Repeat Steps 3 – 4 until every block in the shares is processed.

END ALGORITHM

IV. TRUE COLOUR IMAGE

In the case of the TRUE Colour Secret Image, we use the same algorithm to hide and recover secret image. We use 24 bits to record the R, G and B Values of that secret pixel.

This need can be accomplished by expanding every pixel into a 5X5 matrix. Since, there is no need to record the palette data, the bit no. 25 i.e. P25 could be abandoned or conceal additional data like digital watermark.

The same algorithms can then be applied on the 5X5 matrix with appropriate corrections in those algorithms.

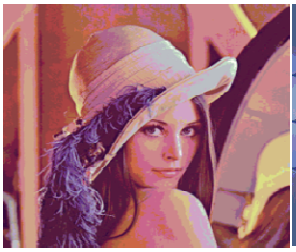

Fig. 1: Secret Image (256 Colours)

Fig. 2: Cover Image 1

Fig. 3: Cover Image 2

4. CONCLUSIONS

In this paper, we use information hiding technique to conceal secret images into two meaningful cover images. Every pixel is expanded into a 3X3 block. The binary index code of the secret pixel and 1 bit of the palette data are randomly dispatched to shares. The only criterion is to make the results of the XOR operation on the corresponding block equal to the binary index code of the secret pixel. Every block on the shares has 4 White and 5 Black Sub pixels in it. It means regardless of the colour of the secret image, the probability of them to appear 1 on each share is 5/9.

This gives no clue about the content of the secret image on the shares. This indistinguishable property assures the security of the secret image on the shares. In addition, for every 1s in the share 1 and share 2, we fill the corresponding colour of the cover pixel at that location. This makes shares meaningful. Our model can easily be extended from 256 Colour Image to the True Colour Image. We only need to expand the block size from 3X3 to 5X5.

5. REFERENCES

1. M. Naor and A. Shamir, "Visual Cryptography", Proceeding of Euro crypt 94 Lecture Notes in Computer Science, LNCS963,Berlin: Springer, 1994, pp1-11.
2. Chang, C. C., Tsai, C. S. and Chen, T. S., "A technique for sharing a secret colour image", in Proceedings of 9th National Conference of Information Security, Taichung, May 1999, pp. LXIII-LXXII.
3. Lin, F., "A New Approach on Colour Secret Image Sharing Technique", Master Thesis, Department of Information Management, National Central University, 2000.
4. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Extended Schemes for Visual Cryptography", Theoretical Computer Science, Vol. 250, 2001, pp. 143-161.
5. Y. C. Hou and J. H. Wu, "An Extended Visual Cryptography Scheme for Concealing Colour Images", in Proceedings of the 5th Conference on Information Management and Police Administrative Practice, Taoyuan, Taiwan, June 2001, pp. 62-69.
6. Hwang, R. J. and Chang, C. C., "Hiding a picture into two pictures", Optical Engineering, Vol. 40, 2001, pp. 342-351.
7. Chang, C. C., Tai, W. L. and Lin, C. C., "Hiding a secret colour image in two colour images", The Imaging Science Journal, Vol. 53, 2005, pp. 229-240.
8. Gizem, Aksahya & Ayese, Ozcan (2009) Communications & Networks, Network Books, ABC Publishers.

****

---

[1]Ranbir Sinha[1]
Department of Computer Science & Engineering
Institute of Technology
Guru Ghasidas Vishwavidyalaya, Bilaspur, C.G.
rsinha.u64@gmail.com
[2]Dr. Manish Shrivastava[2]
Department of Computer Science & Engineering
Institute of Technology
Guru Ghasidas Vishwavidyalaya, Bilaspur, C.G.
manbsp@gmail.com