Secure Image Encryption Based on Visual Cryptography

Cho Cho Aung, Khin Than Mya
University of Computer Studies, Yangon
cc.aung9@gmail.com

Abstract

Information security is a major issue today for any company or individual who conducts business electronically. It is of utmost important that mechanisms are set up to ensure information and data security. Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. In this paper we consider a new type of cryptographic scheme; encryption is used to securely transmit data in open networks. The increasing use of digital techniques for transmitting and storing images, integrity as well as the authenticity of image has become a major concern. Visual cryptography is a cryptographic technique which allows visual information to be encrypted. Visual cryptography can be seen as a one-time pad system. Then, it cannot be reused. This system presents a 2 out of 2 schemes based on visual cryptography of image encryption. Visual cryptography is a powerful technique which combines the notions of perfect ciphers and secret sharing in cryptography. Visual cryptography can decode concealed images without any cryptographic computation.

1. Introduction

The ability to share all kinds of information and resources is fundamental in today's global environment. The rapid growth of information technology for human to communication on the internet. Internet is public; anyone can easily read information and perform successful transmissions without protection. In order to avoid sensitive information being illegally read or modified, the information must be encrypted before transmission. At the same time a whole variety of security system using encryption methods have also been developed to prevent information from being accessed or used by unauthorized people [1].

In 1994, Naor and Shimar first presented a novel secret sharing scheme called visual cryptography that differs extremely from the traditional cryptography. It divides a black-white image into n shares. Among those shares, any k or more ones are stacked and then a discernable image appears; otherwise any less than k ones together can reveal nothing about the original secret. The advantages of this visual secret sharing (VSS) scheme are very clear in that those complex computations needed in traditional cryptography are redundant and the decryption even does not need any knowledge of cryptography or any help with computer; it only depends on the humankind's visual system [2].

This paper proposes a 2 out of 2 visual cryptography scheme. To encrypt a binary image, it is divided into an arbitrary-n of slides and slides are encrypted using an XOR process with a binary random key or keys.

2. Related Work

Many image-protection techniques are using visual cryptography (VC). H.Kuwakado and H.Tanaka have proposed a new visual secret sharing scheme such that the reconstructed image is the same size as the secret image; the contrast in this proposed scheme is done as the difference of the probabilities [3]. D. Bloisi et al. have presented a novel method for integrating in an uniform model cryptography and steganography. They have proven that he presented ISC algorithm is both an effective steganographic method as well as a theoretically unbreakable cryptographic one (ISC is an image based one-time pad.) [4]. W.Q. Yan et al. presented a new visual cryptography for print and scan applications. They have been solved the practical problem associated with the use of visual cryptography [5]. M.Nakajima and Y.Yamaguchi presented extended visual cryptography for natural images. The encryption based on extended visual cryptography method and the decryption is done directly by the human visual system with no special cryptographic calculations. It showed a method to improve the image quality of the output by enchancing ed by observing the actual results of this method [6]. In S.K. Chen presented a novel non-expanansible visual cryptography scheme that generates meaningful transparencies. It is the same size with the same size with the secret image [7]. In S.S. Lee et al. proposed a new visual cryptography method that applies a phase-assignment rule to every encrypted image. The binary image to be encrypted was divided into any number of n slides. Only one random key or (n-1) randomly generated keys and

the n-th random key from an XOR process between (n-1) random keys were prepared to encrypt these slides. For decryption, the phase masks were placed on interferometer paths and their interference pattern produced the same image as the original one and the original image and decrypted image have the same resolution [8].

3. Background Theory

In this background theory section shows the parts of cryptography and visual cryptography.

3.1 Cryptography

Cryptography or cryptology is the practice and study of hiding information. In data and telecommunications, cryptography is necessary when communicating over any entrusted medium, which includes just about any network, particularly the Internet. Cryptography is the study of mathematical techniques for all aspects of information security. Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Cryptography is used in application presented in technologically advanced societies. Cryptography referred almost exclusively to encryption, the process of converting the ordinary information (plaintext) into intelligible gibberish (cipher text). Decryption is the reverse, moving from unintelligible cipher text to plaintext.

3.2 Visual Cryptography

Visual cryptography is a special encryption method to hide information in images in such a way that it can be decrypted by the human visual system if the correct key image is applied. The technique was proposed by Naor and Shamir in 1994. Visual cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Either transparent images or layers are required to reveal the information. The easiest way to implement visual cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a one- time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears.

3.3 Visual Cryptography Scheme

The secret image consists of a collection of black and white pixels where each pixel is treated independently.

- Original image into n modified versions (referred as shares) such that each pixel in a share now subdivides into m black and white sub-pixels.
- To decode the image, the scheme simply pick a subset S of those n shares and Xerox each of them onto a transparency.

If S is a “qualified” subset, then stacking all these transparencies will allow visual recovery of the secret.

4. Algorithm of 2 out of 2 visual Cryptography scheme model

Pixel		Share1 Share 2	Superimpose Two Shares
	P=.5 P=.5		
	P=.5 P=.5		

The algorithm specifies how to encode a single pixel, and it would be applied for every pixel in the image to be shared.

Table 1. 2 out of 2 schemes

A pixel P is split into two sub pixels in each of the two shares.

- If P is white, then coin toss is used to randomly choose one of the first two rows in the table 1.
- If P is black, then a coin toss is used to randomly choose one of the last two rows in the table 1.

Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row in the table 1. Every pixel is encrypted using a new coin toss. We look at a pixel P in the first share. One of the two sub pixels in P is black and the other is whit. Each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white.

The first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image were encrypted using independent random coin flips, there is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme.

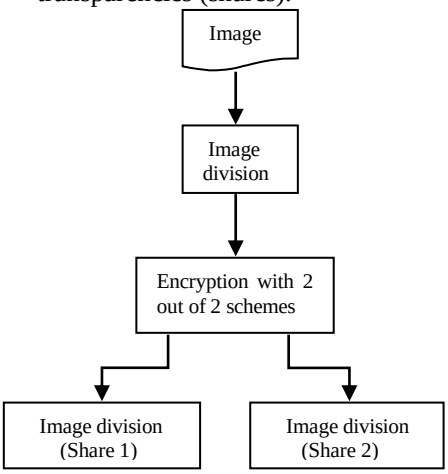
We superimpose the two shares; consider one pixel P in the image.

- If P is black, we get two black sub pixels when we superimpose the two shares;
- If P is white, we get one black sub pixel and one white sub pixel when we superimpose the two shares.

Thus, we could say that the reconstructed pixel (consisting of two sub pixels) has a grey level of 1 if P is black and a grey level ½ if P is white. There will be a 50% loss of contrast in the reconstructed image, but it should still be visible.

5. Propose System

This system is an implementation of encryption and decryption using visual cryptography schemes. For encryption of our proposed system, the first stage of the system is accepted image to encrypt by the user's desire. Second, the input image has divided into the two slides and transforms XOR process. Then, encrypt using 2 out of 2 visual cryptography schemes. Second step is the decryption process. Decryption process is the overlay the transparencies (shares).



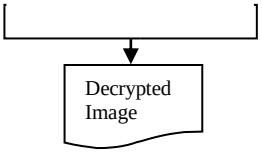


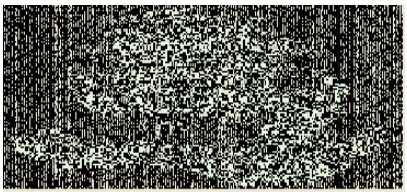
Figure 1. System Process Overview

6. Experimental Results

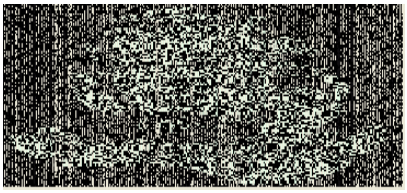
This system is implemented using C# programming language. This section shows the result of encryption and decryption process. This system can encrypt and decrypt for jpg, bmp, png and wmf files and different file sizes are used for testing the system.

(a) Original Image

Figure 2(a) is displaying original image. This image will be in encrypted with the 2 out of 2 visual cryptography scheme. Figure 2(b) and 2(c) are showing the two shares of original image after encryption process. Figure 2(d) is displaying the decrypted image with superimpose of two shares.



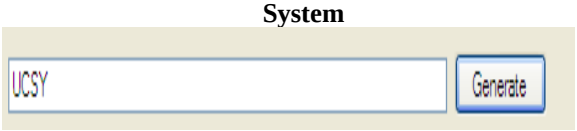
(b) Share 1



(c) Share 2

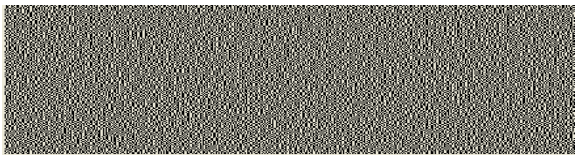
(d) Decrypted Image

Figure 2. Sample Image Encryption process of System

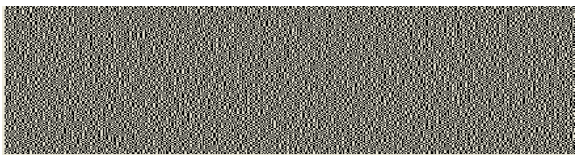


(a) Input text box

Figure 3(a) is displaying text box for input text. We get the text input as the bitmap file. In figure 3(b) and 3(c) are showing the two shares of input file. Figure (d) is showing the decrypt file.



(b) Share 1



(c) Share 2

(d) Decrypted text

Figure 3. Sample Text Encryption System

7. Conclusion

This system represents the method of encryption and decryption for image security using 2 out of 2 visual cryptography schemes. This system can encrypt the gray images and color image. When the proposed system was applied the image can decrypt without computation. Visual cryptography has proved that security can be attained with even simple encryption schemes.

8. Reference

[1] C. W. Chen and Y.D. Wu, "A Visual Information Encryption Based on Visual Cryptography and D-H Key Agreement Scheme" Source: Dept of Computer Science and Information Technology, National Taichung of Technology, Taiwan, R.O.C.

[2] H. Zhang, X. Wang, W. Cao and Y. Huang, "Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding" *Journal of Computer*, vol. 3, No. 12, December 2008.

[3] R. Ito, H. Kuwakado and H. Tanaka, "Image Size Invariant Visual Cryptography" *IEICE TRANS FUNDAMENTALS*, vol.E82-A, No.10, OCTOBER 1999.

[4] D. Bloisi and L. Iocchi, "Image Based Steganography and Cryptography" Source: Dipartimento di Informatica e Sistemistica, Sapienza, University of Rome, Italy.

[5] W.Q. Yan, D. Jin and M. S. Kankanhalli, " Visual Cryptography for Print and Scan Application" Source: School of National University of Singapore, Singapore 117543.

[6] M. Nakajima and Y. Yamaguchi, "Extended Visual Cryptography for Natural Images" Source: Dept of Graphic and Computer Sciences, University of Tokyo,3-8-1 Komaba, Meguro-ku, Tokyo 153-8902, Japan.

[7] S. K. Chen, "An NEVC scheme based on nature shares" Source: Dept of Computer and Information Engineering Yuan-Pei University, Taiwan.

[8] S.S Lee, J.C. Na,S.W. Sohn, C. Park, D.H. Seo and S.J. Kim, "Visual Cryptography Based on Interferometric Encryption Technique" *ETRI Journal*, vol-24, No-5, October . 2002.