International Journal of Infinite Innovations in Technology|ISSN:2278-9057
IJIIT|Volume-IV|Issue-I|2015-2016 July|Paper-04
Reg. No.:20150604|DOI:V4I1P04

Design of Random Image Slicer using Implementation on Steganography – A Survey

Tanvi Chavan[#1], Prof. Umesh Kulkarni[*2]

Department of Information technology
VIYALANKAR INSITUTE OF TECHNOLOGY, MUMBAI UNIVERSITY
Tanvi.chavan@vit.edu.in
Umesh.kulkarni@vit.edu.in

ABSTRACT

Nowadays Digital Communication is most essential part of organization as a many of applications are based on internet, so it is important to made in a secret way. Accordingly to protect confidentiality and data integrity of digital communication, security of information passed over an open channel has become a fundamental issue. Cryptography and Steganography are widely used techniques that manipulate information (messages) in order to enhance security over open channel. The main purpose behind cryptography is to make message concept unintelligible, while steganography aims to hide secret message. This paper shows basic concept of cryptography and steganography along with its method to enhance security over open communication channel.

Keywords: Visual Cryptography, PVC, steganography, shares, key.

I. INTRODUCTION

Cryptography and Steganography widely used techniques. Visual Cryptography technique converts data into an unreadable format so as to protect the information from unauthorized parties. This is thus used to maintain the privacy and security of the information transferred between the systems. The Steganography hides the message so it cannot be seen by. Even though both cryptography and steganography methods provide security, a study is made to combine both methods into one system for better confidentiality and security. Visual Cryptography (VC) was first introduced by Shamir and Noar at Eurocrypt'94 [1]. To encode a secret employing a (2, 2) VC Scheme, the original image is divided into 2 shares such that each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. Without any cryptographic computation. Particularly in a k-out-of-n visual secret sharing scheme (VSS), a secret image is cryptographically encoded into n shares. Each share resembles a random binary pattern. The n shares are then Xeroxed onto transparencies and distributed among n participants. The secret images can be visually revealed by stacking together any k or more transparencies of the shares and no cryptographic computation is needed. However, by inspecting less than k shares, one cannot gain any information about the secret image, even if infinite computational power is available. Steganography, literally means, "Covered Writing" which is derived from the Greek language. Steganography is the art and science of communicating in a way which hides the existence of the message so it cannot be seen. In contrast to Visual Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present.

II. RELATED WORK

Visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed.
Visual cryptography is introduced by first in 1994 Noar and Shamir [1]. Proposed a new cryptography paradigm, called visual cryptography (VC) or visual secret sharing (VSS), which attempts to recover a secret image via the human visual system by stacking two or more transparencies.where decoded image is double than that of the original secret image as pixel p expanded into two sub pixels. This is called pixel expansion, affecting the contrast of resulting image.
The (2, 2) VC scheme divides the secret image into two shares so that reconstruction of an image from a share is impossible. Each share is printed in transparencies. Table 1 reveals how decryption is performed by a two share stacking when the secret image is seen by the naked eye without any computation. A secret picture is to be shared among n participants. The picture is divided into n transparencies (shares) so that when m transparencies are placed together it is visible. When less than m transparencies are together, it remains invisible. This
Process is through viewing a secret picture as a black and white pixels set, where each pixel is handled individually.

Pixel	White	Black
Prob.	50 % 50%	50% 50%
Share 1		
Share 2		
Stack Share 1 & 2		

Table 1. Visual Cryptography Scheme

Young-Chang Hou and Zen-Yu Quan [3] proposed a progressive visual cryptography scheme with pixel-unexpanded shares to solve the main problems such as leak of secret information, pixel expansion, and bad quality of recovered images. Even though in this method has so many advantages, it generates noise-like shares. The generated shares are not meaningful, which are of more interest to hackers as they treat them as critical information in the transmission. Confidential images have no means to be secured when they are transmitted over the network.

Ch.Ratna.babu, M.Sridhar, Dr.B.Raveendra.Babu [8] proposed novel method of VC is presented for halftone images which represent the resultant image in the same size as the original secrete image. This method divide image into 2 shares and decryption is performed by human visual system. Hiding of the visual information based on pseudo randomization and pixel reversal.

In the proposed algorithm, pre-processing elements were added to change dark/high level of gray image into a lighter one (called pre-processed/halftone image). This must be undertaken prior to inputting the secret image into the algorithm.

Pixel values are changed to white (255) based on its position. Odd and even pixel value combinations are used in the matrix as follows:

Method 1: If i=j=odd and i=j=even pixel (i, j) = 255

Method 2: If i=odd & j=even OR i=even & j=odd pixel (i, j) = 255

Such pre-processing converts the secret image into a lighter one in contrast before handing it over to the algorithm for processing.

Adi Shamir, [4] provided perfect ways to share information. Nevertheless, all these schemes needed computer to solve those complicated math in order to decrypt the secret image other than simply using the human eyes.

Jithi P V, Anitha T Nair[7] proposed a watermarking scheme which overcomes the drawbacks Young-Chang Hou and Zen-Yu Quan's[3] PVC method. In this proposed method, a digital watermarking technique is used to generate meaningful shares. The secret gray scale image shares are watermarked with different cover images and are transmitted. At the receiving side the cover images are extracted from the shares and stacked one by one which reveals the secret image progressively.

InKoo Kang, Gonzalo R. Arce and Heung-Kyu Lee [2] developed an encryption method to construct color EVC scheme with VIP synchronization and error diffusion for visual quality improvement. Some methods for color visual cryptography are not satisfactory in terms of producing either meaningless shares or meaningful shares with low visual quality, leading to suspicion of encryption. This scheme introduces the concept of visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality.

Mehdi Hussain and Mureed Hussain [6] define steganography and various technique of steganography. Depending on the type of the cover object there are many suitable steganography techniques which are followed in order to obtain security. Generally steganography is known as "invisible" communication. Steganography means to conceal messages existence in another medium. Today's steganography systems use multimedia objects like image, audio, video etc as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information. Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object. After hiding process cover object and stego-object are similar. So, steganography and cryptography are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis

Drawback:

1. It is for black and white images.
2. Need more storage capacity as shares are four times the original image.
3. The secrete image is encrypted into 2 shares so that decryption can be perform by human visual system.
4. It is time consuming as single pixel encoding at each run.

III. THE PROPOSED SYSTEM

This research work is motivated by the following facts; as we know; visual cryptography and steganography have been known for many years. We can encrypt data, but it will be exposed while transferring. On other hand, we can hide data into a common object, but if someone extracts it, he/she can get the information easily. Therefore, my idea is to apply both of them, so in case one gets the embedded stuff, he/she will face an encrypted data.

In proposed work we design random image slicer for secrete color images that uses visual cryptography for secrete image sharing with image steganography. That divides images into n no of shares. By increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively. Even though no one can obtain any hidden information from a single share. This type of visual cryptography technique is insecure as the shares generated are meaningless (random

looking) images and have more interest of hackers as they treat them as critical information in the transmission. So that this random looking share is enveloped into some meaningful images so that interest of hackers can be reduced.

This method provides a more efficient way to hide image in different meaningful shares providing high security and recovered image with high contrast.

In proposed method the recovered image and original image are of the same size there is no pixel expansion effort.

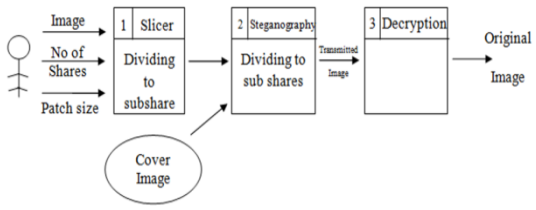

Figure 1.Proposed system

Algorithm	Pixel Expansion	Security	Quality
Naor Shamir(basic (2x2)(for gray scale images)	Double	Increase	Poor
(k,n) VC scheme.(for gray scale images)	Double	Increase	Poor
Color Extended Visual Cryptography Using Error Diffusion	No	Increase	Poor
Progressive Visual Cryptography with Unexpanded Shares.(for gray scale images)	No	Average	Average
Halftone Visual Cryptography. (for gray scale images)	Double	Poor	Poor
Progressive Visual Cryptography With Watermarking For Meaningful Shares. (for gray scale images)	No	Good	Good
Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security. (for gray scale images)	No	Poor	Average
Proposed technique. (for color images)	No Expansion	Increase	Good

Table 2.Comparison of algorithms

Advantages:

1. It is for color images.
2. The secrete image is encrypted into n no of shares so that decryption can impossible by human visual system.
3. Visual cryptography is combining with steganography to provide more security to secrete images.

IV. SCOPE & APPLICATIONS

This type of progressive visual cryptography method are used to encrypt the visual information such as printed text, handwritten notes, pictures, documents, military maps.

This can also be used in Biometric system, remote electronic voting, and bank customer identification.

V. CONCLUSION

Different methods are used to protect information from unwanted parties like Visual Cryptography, Watermarking PVC, and Steganography.

All these methods are excellent at their own place but neither technology alone is perfect. So in order to add multiple layer of security, multiple authors have used a combination of these technologies. By using Visual Cryptography the author's intent to reduce the computational time required by their system.

A less complex system is required, as the decryption process the shares have to be stacked one on top of another to generate the secrete image. By using the method of unexpandable shares the authors have increased the contrast and hence image quality of the received images has been increased. The memory requirement of the system has been reduced as pixels of the image have not been expanded. It is a possibility that hackers may try to decode the transmitted image which is in the form of shares. As a result the shares generate suspicion in the mind of hackers that it might contain some information. A

few authors have proposed Steganography to overcome this, as the Steganography the shares are hidden in a cover image so that hackers do not generate interest in the transmitted shares and try to decode it.
There is no method for color images, so all authors have proposed scheme for gray scale images.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. Adv. Cryptol.: EUROCRYPT, vol. 950. 1995, pp. 1–12.

[2] InKoo Kang, Gonzalo R. Arce, "Color Extended Visual Cryptography Using Error Diffusion", and Heung-Kyu Lee, 1057-7149/ 2010 IEEE.

[3] Young-Chang Hou and Zen-Yu Quan"Progressive Visual Cryptography with Unexpanded Shares", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 21, No. 11, November 2011

[4] Adi Shamir, How to Share a Secret, published in ACM, Laboratory for Computer science, Massachusetts Institute of Technology, 1979.

5] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, Half tone Visual Cryptography, IEEE Transaction on image processing, vol.15, no.8, 2006.

[6] Mehdi Hussain and Mureed Hussain,"A survey of image stegnogaraphy technique" International Journal of Advanced Science and Technology Vol. 54, May, 2013

[

[7]Jithi P V, Anitha T Nair, "Progressive Visual Cryptography with watermarking for meaningful shares" by 978-1-4673-5090-7/13/ 2013 IEEE.

[8]Ch.Ratna.babu,M.Sridhar,Dr.B.Raveendra.Babu,"Information Hiding in gray scale Images using Pseudo-Randomized Visual Cryptography Algorithm for visual Information Security" IEEEInternational conference on information systems and computer networks,March 2013