Visual Cryptography and Steganography Methods - Review

Kavita M. Tambe.
PG Scholar: Electronics and Telecommunication
Alamuri Ratnamala Institute of Engineering & Technology, Mumbai
e-mail: ktambe87@gmail.com

Ramling D. Patane
Associate Professor :Electronics and Telecommunication
Terna Engineering College
Nerul , Navi Mumbai
e-mail:rrpatane@yahoo.com

Abstract—In today's information era information hiding becomes very much important as people transmits the information as innocent as credit card to online stores and as dangerous as terrorist plot to hijackers. The art of information hiding receive attention of the researchers. This paper provides a review of two methods – Visual Cryptography and Steganography for secure communication via a common communication channel.

Keywords- *Visual Cryptography ;Steganography; Halftone; Recursive Threshold; Progressive visual cryptography*

*****

I. INTRODUCTION

As there is rise in use of Internet and development in computers in different vicinity of life. Safety of data becomes most important factor in information technology and communication. Information comes in various forms and requires secure communication .For providing secure communication in terms of exchange of information many different methods such as Cryptography, steganography; coding, etc have been developed. Sometime it is not enough to keep the message secret , it may also required to maintain confidentiality and authenticity of the message .Security , confidentiality and authenticity of communication ranges from bank transactions , online payment , computer forensic etc. In recent years steganography combine with visual cryptography have received attention of researchers.

Steganography is related to transfer a secret message while hiding its existence. The word steganography is derived from the Greek words steganos, meaning 'covered', and graphein, meaning 'to write'. Whereas Cryptography deals with a process called as Encryption. The word cryptography derived from the Greek words kryptós, means "hidden, secret"; and graphein, and stands for writing" or study, respectively.

The main objective of Steganography is to keep the information secrete in the other cover media so that other person will not detect the existence of the information and Cryptography deals with the study of hiding information. In steganography only sender and receiver know the presence of message but in cryptography the encrypted message is visible to the world. Steganography removes the unnecessary interest towards the secrete message. Cryptography aims to protect content of message while steganography provides various methods that can be use for hiding the message as well as the content .Therefore a combination of both Steganography and cryptography can be use to achieve better Security and confidentiality. [1]

II. BASIC OVERVIEW OF STEGANOGRAPHY

Steganography is an art of transferring message in such a way that the existence of message is concealed. Following terms deals with the steganography system [3]:

- Cover Media: In order to hide the presence of secret data the message is embedded in this medium.
- Stego: The media through which the data is hidden.
- Secret Data: The data which is to be hidden.
- Steganalysis: It is the process by which the secret data is to be extracted.

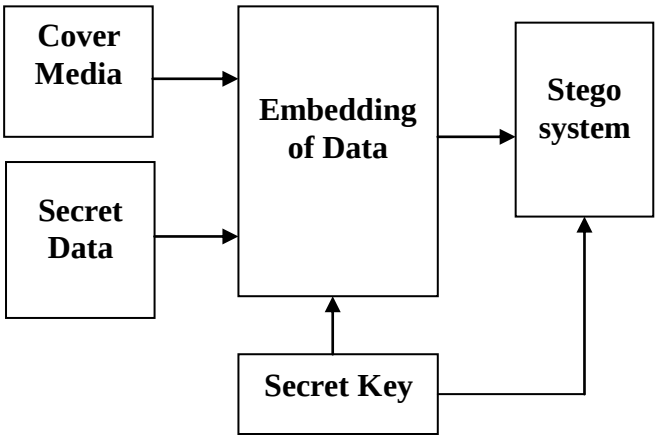

Figure 1. Basic Overview of Steganography.

Steganography can utilize various medium as carriers of the message. These mediums may include text, like character marking, invisible ink, using pin pictures, type-writer correction, images, and audio, video signals. In actual practice three main types of steganographic protocols are used .They are Pure Steganography, Secrete Key Steganography and Public key steganography. The steganographic system which does not requires exchange of cipher is called as pure steganography. This system is less secure because in this system sender and receiver assumes that only they (Sender and receiver) are aware about the secrete message. Where as in case of Secret key steganography, a secret key is required to be exchange before communication so that only the parties who aware about the secret key can extract the message. Because of the exchange of the secrete key the system becomes unsusceptible to the interference from third party. The concept of Public key steganography is derived from Public key cryptography. In this system the parties which want to communicate with each other uses Public Key and Private Key. During encoding process sender uses public key and only private key can be used for the process of deciphering the secret message. [5] [6]

On the basis of the media used for hiding the data , steganography can be differentiated as : Text Steganography, Image Steganography , Audio Steganography ,Video Steganography and Network Steganography .

A. *Text Steganography*

In this method text is used as a media for hiding the data [3].It involves changing the formatting of the text, changing the words within the text in order to generate a sequence of random character readable text [7]. Hiding of data in to text becomes very challenging because text files contains small amount of redundant data [5] [7]. Encoding secret message in to the text results in to low embedding capacity also the text has less noise therefore this method is less secure. Text based Steganography is broadly classified in to following types:

- Format Based Method
- Random and Statistical Method
- Linguistics Method

B. *Image Steganography*

In today's digital world secret messages get embedded in to the digital image which is called as Image Steganography where cover object used is Image. Because of the limited power of the Human vision system this method is most commonly used [5].

According to Duncan Sellars [4], image can be explains as "To a computer, an image is an array of numbers that represents light intensities at various points or pixels. These pixels make up the images raster data. Image steganography typically uses 8-bit and a 24 bit pixel image files [5] .8 bit image are small in size (in KB) but during encoding it provides only 256 colors. 8- Bit images uses gray scale color palette for example .GIF. 24-bit images offer large size, more flexibility and provide more than 16 million colors so that it becomes tough to identify the secret message. The data hiding capacity of the 24- bit image is larger than that of 8- bit image. Large size of the 24- bit image can consider as its drawback because large size makes it more suspect than small size 8-bit images. Therefore to overcome this problem Digital image compression method is used. There are two types of Digital image compression method namely Lossy and Lossless. In lossy compression method image size is get compressed by removing excess image data and it calculates close approximation to the original image. This method is mostly used by 24-bit images.
Most of the steganographic users use lossless image compression technique as it keeps the whole digital image without loss. Following parameters are required to be considering for Image Steganography [12] [13]:

- High Capacity and security: The data hiding capacity must be high so that maximum amount of data can be hiding in the image. A high quality steganographic system should be secure from all types of attacks.
- Perceptual Transparency: It is nothing but the Imperceptibility and it should be as high as possible.
- Robustness
- Temper Resistance: It refers to existing of the embedded data even when the third party tries attempt to modifies it in the Stego image.
- Computation Complexity: It involves computation cost required for embedding and extraction of hidden data and it should be as low as possible.

Image steganography uses different techniques for encoding the image and these are spatial domain, frequency domain, Distortion techniques, Masking and Filtering.

C. *Audio Steganography*

When sound signal is used to embed the secrete data then the technique is known as Audio steganography. The sound files can be in the form of WAV, Au and MP3. This method is most challenging as Human Auditory System (HAS) has dynamic range that it can listen over. The HAS perceives sound over the range of power greater than 109:1 and frequency greater than 103:1. The weakness in the HAS is sound differentiation and this must be exploited for encoding the secrete message in audio. Before selecting any encoding technique two factors are required to be consider .The first factor is audio format. Sample Quantization, Temporal sampling Rate and Perceptual Sampling are the three main digital audio formats.WAV and AIFF uses sample quantization which is 16- bit linear sampling architecture .Temporal sampling uses selectable frequency for sampling audio. The last audio format that is perceptual sampling in which statistics of the audio is get changes by encoding only the part of listeners perceives and therefore maintain the sound but changes the signal. In today's world of internet this format is used popularly. The second factor is the transmission medium through which data can be sending from sender to receiver. There are four possible transmission mediums:

- Digital End to End: From one machine to another without any modification.
- Increased/Decreased resampling: In this sampling rate is get modify but the nature will remain digital.
- Analog and resample: Nature of the signal is changed to analog and resample at different rate.
- Over the air: Radio frequencies are used for transmission of the signal.

Low bit encoding, Phase Coding and Spread Spectrum are the different methods used for audio steganography.

D. *Video Steganography*

Video is nothing but the combination of pictures. In this method video is used as a carrier for hiding any information [14] [15]. Used of video as carrier improves the capacity and also enhanced the security aspects. There are various methods used for video steganography such as Least Significant Bit method (LBS), Spread Spectrum, Discrete Cosine Transform (DCT), vector embedding method. Mostly Discrete cosine transform (DCT) changes the value for example 8.667 get alter to 9 and this is used to hide information in each of the image in the video and also not noticeable to the human eyes. H.264, MP4, ICMP, AVI or other video formats are used by video steganography.

E. *Netwok Steganography*

This steganography uses network protocols for hiding data .This is possible by using secrete channels and by using fields in the protocol header s as these fields are irrelevant and unused. The network steganography methods may be classify on the basis of protocol functions associated with the OSI RM layers and on the basis of types of modification of protocol data units.

III. BASIC OVERVIEW OF VISUAL CRYPTOGRAPHY

Visual Cryptography (VC) is a method of encrypting a secret image into shares such that stacking an adequate number of shares reveals the secret image. A very simple and totally new way of secret sharing is introduced by Naor and Shamir in 1994 [2] which not include any cryptographic computations – called as Visual Cryptography Scheme (VCS). VCS is a special encryption technique used to hide the information in image as the name suggest it can be decrypted by simple human vision.

VCS in very simple form uses two transparent images. One image contains random pixels where as the other one contains secrete information. It is not at all possible to reveal the secret information from any one of the image. Both the transparent images are required for revealing the information. When two transparencies are stacked together, human eye can decrypts the information. This allows anyone to use the system without having any knowledge of cryptography, this consider as an advantage of VCS over other cryptographic techniques. VCS is easy for implementation, use and consider as very secure. Initially the VCS were implemented for black and white images or messages which are nothing but the collection of black and white pixels. But the decryption process in this is lossy and because of this loss the contrast of the image gets affected. Contrast is consider as one of the most important parameter in VCS as it determines the clarity of the secrete revealed by human visual system. Therefore the entire VCS can be summarizes as follows [4]:

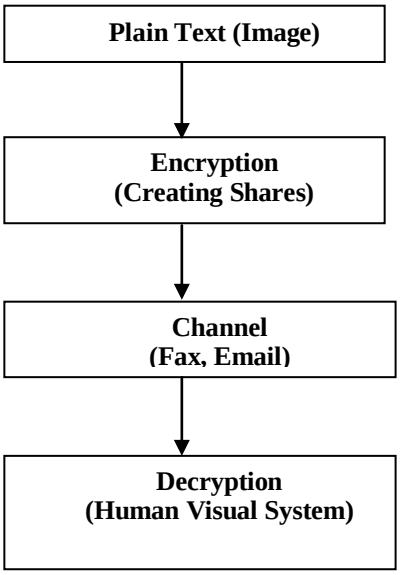

Figure 2. Basic Overview of Visual Cryptography .

A. *(2 , 2) Visual Cryptographic Scheme*

In this method original image is divided into 2 shares and shown in figure 3 below. Every secrete pixel in the original image is converted into 2 or 4 sub pixel. Only one share will not able to reveal any secret information. Both the shares are required to be stack on each other to reveal secret image. This is similar to the logical OR operation between the shares. From the figure 4 sub pixels are generated from pixel of secret image in such a way that 2 sub pixels are black and 2 sub pixels are white. The selection of black and white pixel is random and having probability of 0.5. During superimposing if 2 white pixels are overlaps then resultant pixel will be white and if black pixel in one share overlaps with either white or black pixel in another share then the resultant pixel will be black[16]. Figure 3 shows resulting sub pixel when the sub pixel of both the shares in the 3rd and 4th columns are place over each other.

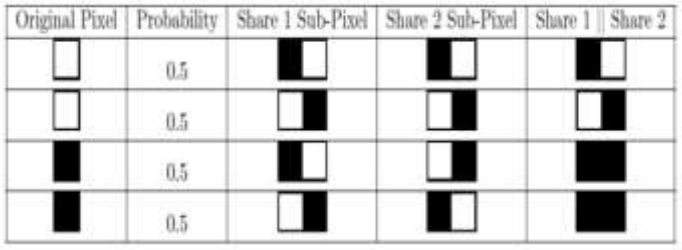

Figure 3. (2,2) Visual Cryptography Scheme.

B. *(k, n) Visual Cryptography Scheme*

In basic method original image is divided into n shares and all n shares are equally important. Any K shares out of n shares can reveal the secret information .Because of this security of the system gets reduced. To overcome this issue G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extend the basic model into general access structure. In this general access structure the n shares are get divided into two subsets - Qualified and Forbidden depending on the importance of the share. From qualified subset any k shares can be used to reveal the secret information whereas the number of shares is less than k or equal to k from forbidden subset cannot decrypt the secret information.

C. *Halftone visual cryptography*

Halftone is reprographic method. In this method secret binary pixel is encoded into array of Q1 X Q2 sub pixel. This array is called as halftone cell. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

D. *Recursive Threshold visual cryptography*

This method is invented to eliminate the inefficiency of the (k, n) visual cryptographic method .In this method smaller secret in the shares gets hide in the shares of the larger secrets with doubling the secret size at every step. Network load is get reduced when this technique is used in network applications.

E. *Visual Cryptography Scheme for Color images*

Till year 1997 visual cryptography were applicable only to the black and white images and not suitable for color images. Verheul and Van Tilborg proposed first color visual cryptography scheme [17]. In this method one pixel is distributed in to m sub pixels, and each sub pixel is divided into c color regions. Out of c color regions one color region is colored while other color regions are black. There are three approaches:

- In the first approach colors in the secret image can be directly printed on the shares similar to the basic model of visual cryptography. It uses larger pixel expansion method because of which quality of the decoded color image gets degraded.
- Second approach uses three color channels. For additive model it uses Red, Green and Blue, whereas subtractive model uses cyan, magenta and yellow. It converts the color image into black and white image on the three color channel. This approach reduces the pixel expansion but also reduces the quality of the image.

- In third approach bit level encryption of secret image is done and binary representation of color of pixel is used.

F. Multiple secret sharing Technique

Wu and Chen invented the method for multiple secret sharing. It involves sharing of two secret images in two shares. In this method two secret binary images can be concealed in to two random shares for eg. A and B in such a way that first secret can be achieve by stacking two shares and can be denoted by B whereas second secrete can be obtained by rotating A by 90^0 in anti-clock wise direction. The angle of rotation can be 90^0 , 180^0 or 270^0 .

G. Extended Visual Cryptography Scheme

In traditional visual cryptography the randomly generated patterns of pixel looks like noise and catch the attention of the hacker's .Therefore to overcome his problem, alike. Nakajima, M. and Yamaguchi, Y., developed Extended visual cryptography scheme (EVS). In this technique a meaningful shares gets generated rather than generating a random shares.

H. Progressive Visual Cryptography Scheme

The limitation of (k, n) visual cryptography can be overcome by using this method, developed by D. Jin, W. Q. Yan, and M. S. Kankanhalli .In this method obtaining more than one share can also be used for recovering the secrete image .In this method quality of the image depends on the number received shares, more number of received shares improves the image quality.

I. Region Incrementing Visual Cryptography Scheme

Previous research of visual cryptography uses whole image as a single secret and same encoding rule gets applied for all pixels. But it may possible that different regions in one image may have different secrecy levels. In that case it is not possible to apply same rule of encoding to all the pixels. Therefore Ran-Zan wang developed a method called as Region Incrementing Visual Cryptography Scheme which provides multiple privacy levels in single image by using different encoding rules.

APPLICATION AREAS AND FUTURE SCOPE

In real life it is essential to provide security to the shared digital information. This paper provides various techniques of visual cryptography and steganography. Both the techniques can be used for applications such as Web based application , computer Forensic , for transmission of financial documents , for online payment , for secure satellite based communication . Steganography and visual cryptography they both have some part of similarity in concept but have its own individual existences in security of information ,but combining features of visual cryptography and steganography provides double layer security There is much more scope of research in both the field.

REFERENCES

[1] http://www.differencebetween.com/difference-between-cryptography-and-vs-steganography

[2] F. A. P. Petitcolas, R. 1. Anderson and M. G. Kuhn, "Information hiding-A survey," Proc. IEEE, vol. 87, pp.1062-1078,1999.

[3] Rakhi , Suresh Wawande , "A Review on Steganography Methods," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , Vol. 2, Issue 10, October 2013.

[4] Dimple Kapoor,Swati Keshari,Saurabh Kumar Gaur, "An Overview of Visual Cryptography," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014 ISSN: 2277 128X.

[5] Bret Dunbar "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment," SANS Institute 2002.

[6] C.P.Sumathi, T.Santanam and G.Umamaheswari , "A Study of Various Steganographic Techniques Used for Information Hiding," International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[7] Monika Agarwal, "Text Steganographic Approaches: A Comparison," International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013.

[8] L. Y. POR, B. Delina, "Information Hiding: A New Approach in Text Steganography," 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, April 6-8, 2008.

[9] Swati Gupta and Deepti Gupta,"Text -Steganography: Review Study & Comparative Analysis,"Swati Gupta et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, 2060-20622060.

[10] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin & M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method," Global Journal of Computer Science and Technology Graphics & Vision Volume 12 Issue 15 Version 1.0 Year 2012.

[11] NamitaTiwari , Dr. Madhu Sandilya & Dr. Meenu Chawla, "Spatial Domain Image Steganography based on Security and Randomization," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014

[12] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques," International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[13] Gandharba Swain, Saroj Kumar Lenka, "Classification of Image SteganographyTechniques in Spatial Domain: A Study," International Journal of Computer Science & Engineering Technology (IJCSET) ,Vol. 5 No. 03 Mar 2014.

[14] Gupta S. and Gujral G., "Enhanced least bit algorithm for image Steganography" IJCEM international journal of computational engineering & management, vol.15 issue4, July 2012

[15] Manpreet Kaur, Er. Amandeep Kaur, "Improved Security Mechanisam of text in Video by using

[16] Steganographic Technique: A Review", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 5, May 2014 ISSN: 2277 128X.

[17] Suhas B. Bhagate, P.J.Kulkarni, "AN OVERVIEW OF VARIOUS VISUAL CRYPTOGRAPHY SCHEMES," International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013, ISSN (Online) : 2278-1021.

[18] E. 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.

[19] M. H. S. Shahreza, and M. S. Shahreza, "A new approach to Persian/Arabic text steganography," In Proceedings of 5th IEEE/ACIS Int. Conf. on Computer and Information Science and 1st IEEE/ACIS Int. Workshop on Component-Based Software Engineering, Software Architecture and Reuse, 2006, pp. 310-315.

[20] M. H. S. Shahreza, and M. S. Shahreza, "A new synonym text steganography," Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, 2006, pp. 1524-1526.

[21] S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O. Gorman, "Document marking and identification using both line and word shifting," INFOCOM'95 Proceedings of the Fourteenth Annual Joint Conf. of the IEEE Computer and Communication Societies, 1995, pp. 853-860.