A Review on Data Hiding using Steganography & Visual Cryptography

[1]Ms. Megha B. Goel, [2]Mr. M. S. Chaudhari, [3]Mrs. Shweta A. Gode
[1]PG Student, [2]HOD & Asst. Professor, [3]Asst. Professor
Dept. of CSE, Priyadarshini Bhagwati College of Engineering, Nagpur, India
[1]megha.bgoel@gmail.com, [2]manojchaudhary2@gmail.com , [3]shweta_amt80@rediffmail.com

Abstract— **Steganography is the art & science of hiding data in the images. From thousands of year, our ancestors have invented various ways to pass information in hidden form from one place to another place. For eg. Papyrus scroll, cryptex, invisible ink, tattooing, pencil marks on handwritten characters etc. Cryptography is a technique which converts the data or simple text into an unreadable form. Visual cryptography schemes hide the secret image into two or more images which are called shares. It is different from the traditional cryptography, because for decrypting the secret image, it does not need any complex computation. The secret image can be decrypted or recovered when all the shares are stacked together. The advantage of visual cryptography is that if any one captures a share then single share would not reveal anything about the data. In this paper, we discuss about various visual cryptographic schemes based on share generated is meaningful or meaningless, type of secret images (either binary or color) and number of secret images (either single or multiple) encrypted by the various visual cryptography scheme. Also this paper proposed a new way for hiding data in images by combining steganography & visual cryptography.**

***Index Terms*—Steganography, Cryptography, Visual cryptography, Shares**

I. INTRODUCTION

Because of the rapid advancement in network technology large amount of data is transmitted through the network. For eg. various confidential data such as military maps, images taken from the satellite etc. are transmitted through the network. So the security of the data becomes necessary because hackers can steal this confidential information. So for providing security to these data basically there are two techniques

a) Cryptography
b) Steganography

a)Cryptography

Cryptography is a technique which converts the data into an unreadable form. There are two process of cryptography

1) Encryption
2) Decryption

Encryption is the process in which the plain text is converted into cipher text. Decryption is the process in which cipher text is converted into plain text. For encryption we use the encryption algorithm at the sender side & for decryption we use the decryption algorithm at the receiver side.

b) Steganography

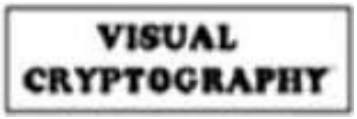
Steganography is the art & science of hiding messages, image or file within another message, image or file. So steganography is an effort to conceal the existence of the hidden information. The difference between cryptography & steganography is that cryptography conceals the content of the message not the existence of the message. In steganography, the possible cover mediums are images, audio, video, text which will hold the hidden information. Together the cover medium and the hidden message create a stego-carrier. While hiding information, some applications require a key which is an additional secret information, for eg., password. This process may be represented as:

cover medium + embedded message + key = stego-medium

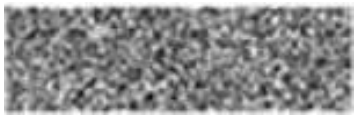
The advantage of steganography is that it can be used to secretly transmit messages & it does not attract the attention of the hackers while plain encrypted message, no matter how unbreakable attract the attention of hacker.

Visual Cryptography

In 1994 Naor & Shamir [1] proposed a new cryptography area called visual cryptography where the decryption is done by the human visual system. Hence, there is no need of any complex cryptographic function for decryption. In Visual cryptography, the secret image is hidden into two or more images which are called shares or cover images. To recover the original image all shares are stacked together.



Original Image



Share 1

Share 2

Decoded Image

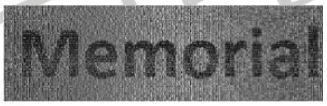
Fig -1: Working of (2, 2) Visual Cryptography scheme

In 1996, Ateniese, Blundo, & Stinson [2] proposed extended visual cryptography schemes in which shares contain not only the secret information but are also meaningful images.

Secret Image

First Cover Image

Second Cover Image



Share1

Share2

Recovered Secret Image

Fig -2: Example of (2, 2) EVC Scheme

Visual cryptography can be used in many applications like transmitting financial documents, banking applications, remote electronic voting applications, authentication & validation. More recent applications are in the field of biometrics such as face privacy, iris authentication & fingerprint scanning.

II. RELATED WORK

Steganography

From thousands of year our ancestors are using steganography. For eg., the sender hide messages within wax tablets, on messenger's body, on paper written in invisible inks, on envelopes covered by the stamp etc. Modern steganography hides the secret image into images, audio, video, text. Steganographic techniques are classified according to the cover medium used as shown in the fig below:

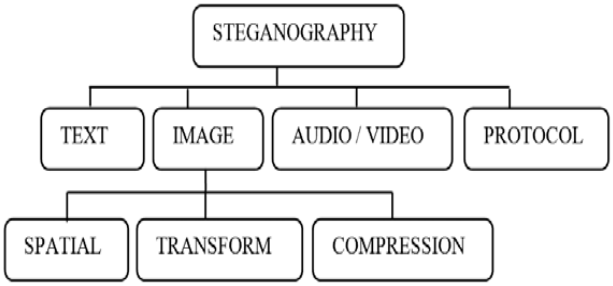


Fig-3: Classification of Steganographic Techniques

Visual Cryptography

In 1994[1], Naor & Shamir, proposed visual cryptography scheme. In this secret image is divided into exactly two shares & both shares are required for the decryption process. In this, the shares generated are meaningless and is used for black & white images only.

In 1996[2], Ateniese, Blundo & Stinson proposed extended visual cryptography schemes that contain meaningful share images. The (2,2) EVC scheme proposed in this required expansion of one pixel in the original image to 4 sub pixels which can then be selected to produce the required images for each share.

Until the year 1997, visual cryptography schemes were applied to only black & white images. First coloured visual cryptography scheme was developed by Verheul & Tilborg[3]. The disadvantage of this scheme is that they use meaningless shares to hide the secret image & the quality of the recovered plain text is bad.

In 2002, Nakajima & Y. Yamaguchi [4], proposed a system which take a 3 pictures as an input & generates two images which correspond to two of the 3 input pictures. The third picture is recovered by stacking the two output images together.

While the previous researches mainly focus on binary images such as text images this paper uses the EVC scheme suitable for natural images such as photography.

In 2003, Hou [5] proposed another color VC scheme. Based on the halftone technique & color decomposition, it decomposes the secret image into three colors C, M & Y. By manipulating the three colors values, the color pixels in the secret image can be represented.

In 2008, H. chu wu, Hao-cheng wang & Rui-wen yu [6], proposes a color visual cryptography scheme which generate meaningful shares. These meaningful shares will not attaract the attention of hackers. The proposed scheme uses thehalftone technique, cover coding tables & secret coding table to generate two meaningful shares. The secret image can be recovered simply by stacking the two meaningful shares together.

In 2010, Q. Chen, X. Lv, M. Zhang, Y. Chu [7], proposed an extended visual cryptography scheme with multiple secrets hidden. Meaningful shares are generated by using the principle of contrast & multiple secret images may be hidden by changing the overlapping angle of the shares. This scheme can also apply to color image. The scheme is easy & effective & shares also have sufficient security level.

In 2012, M. Kamath, A. Parab, A. Salyankar, S. Dholay[8], proposes a new visual scheme for color images. The proposed scheme makes use of Jarvis error filter, a key table & specialized tables for coding.

Sr. No.	Authors	Year	Image Format	Type of share generated	No. of secret Images
1.	Naor & Shamir	1994	Binary	Random	1
2.	G. Ateniese, C. Blundo, Stinson	1996	Binary	Meaningful	1
3.	E. R. Verheul & H.C.A. van Tilborg	1997	Color	Random	1
4.	M. Nakajima, Y. Yamaguchi	2002	Color	Meaningful	1
5.	Y. C. Hou	2003	Color	Meaningful	1
6.	Hsien-chu Wu, Hao-Cheng Wang & Rui-Wen Yu	2008	Color	Meaningful	1
7.	Q. Chen, X. Lv, M. Zhang, Y. Chu	2010	Color	Meaningful	Multiple
8	M. Kamath, A. Parab, A. Salyankar & S. Dholay	2012	Color	Meaningful	1

Table 1: Comparison of visual cryptography schemes on the basis of no. of secret images, image format.

III. PROPOSED WORK

The proposed scheme suggests the novel approach for data hiding using steganography & visual cryptography. There are 5 modules in the proposed scheme

1. Data Hiding
2. Halftone transformation
3. Encoding & Generation of shares
4. Stacking of shares
5. Data Extraction

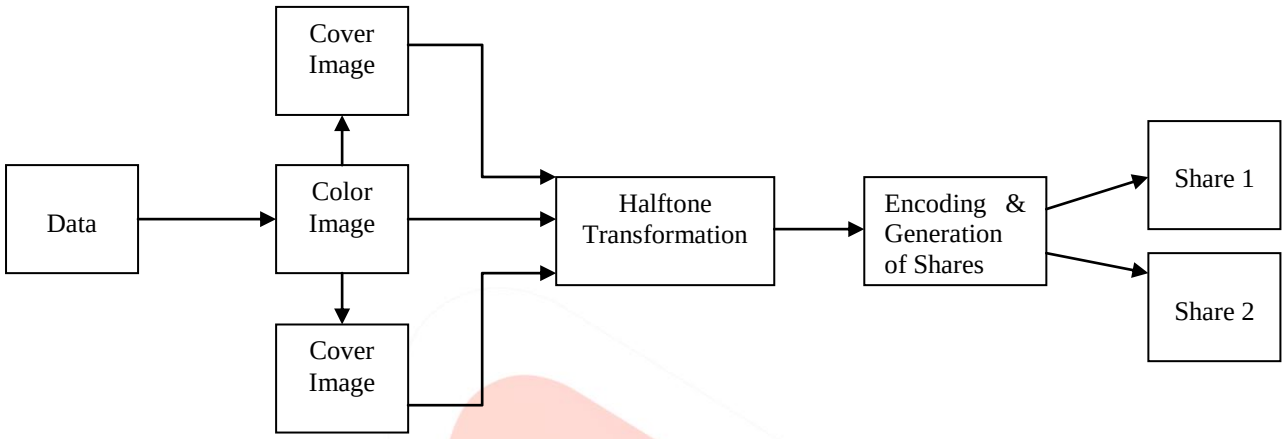


Fig – 4: Encryption Process

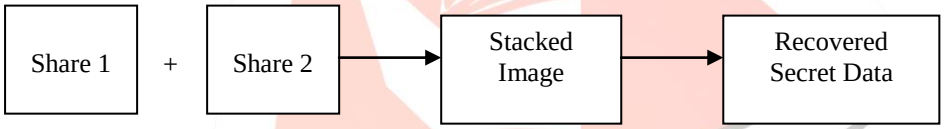


Fig – 5: Decryption Process

In the first module data is hide in the image using the modified version of the LSB algorithm. Some modern steganographic algorithm inserts the text characters directly in the LSBs of the image pixel's. Usually 24-bit or 8-bit files are used to store digital images. 24-bit images provide more space for data hiding. The color information is retrieved from three primary colors: red, green & blue. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. So in 24-bit images each pixel can represent 16,777,216 color values. The lower two bits of these color values are used to hide the data, but this change is so little that is undetectable for the human visual system. This method is known as Least Significant Bit insertion. Following fig shows the process.

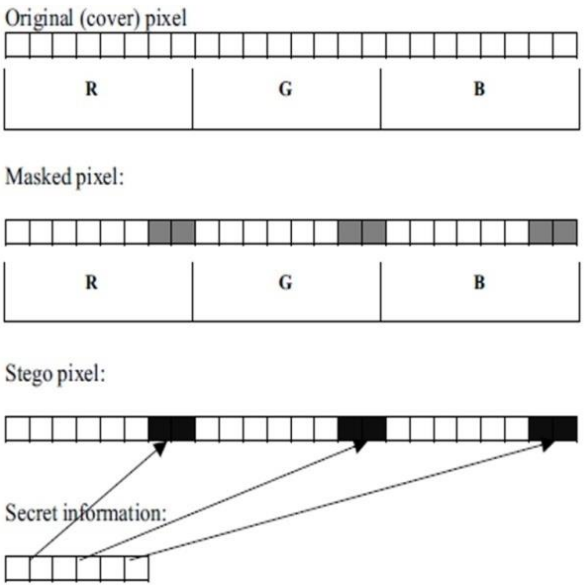


Fig 4: Basic LSB Scheme

But there are two main drawbacks of these algorithms

1. Passing text in the form of message digest is considered to be a separate packet & can easily be dropped as it is not included as a physical property of the host media.
2. Collaborating the LSBs from the pixels of encrypted image is absolutely easy.

So the proposed scheme uses the modified version of the LSB algorithm. At the encryption side the input text that is to be hide will be converted to a byte stream corresponding ASCII values of the characters present in the text. A hash function will be applied on the said byte stream to produce a pseudo byte stream. Subsequently the LSBs of R, G, B bytes of the pixels of color image will be retrieved and individual bits of pseudo byte stream will be embedded into those LSBs. Moreover if hacker tries to collaborate the LSBs of image pixels he will get a wrong text because the LSBs of the encrypted image contain the bits of pseudo byte stream and until and unless the hash function is known, no one can convert the pseudo byte stream to original text byte stream.

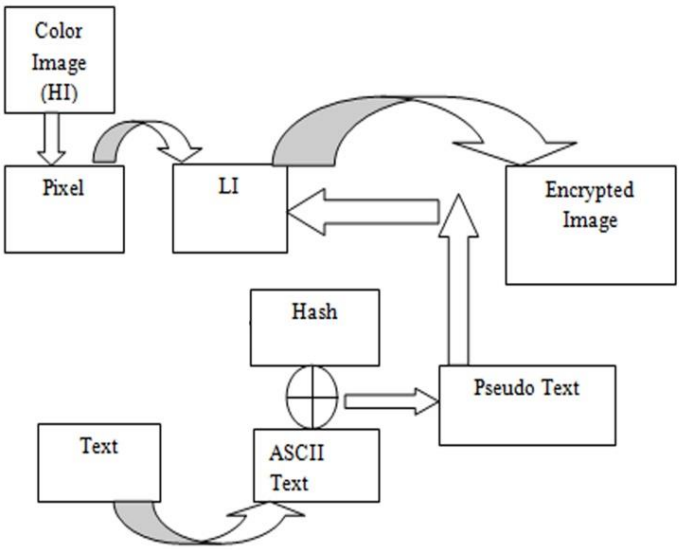


Fig 5: Schematic Diagram for Embedding Text

In the second module, the image in which the data is hidden & two cover images are transformed into an halftone image. Each input image is decomposed into three constituent planes red, green and blue. Then the halftone technique is applied to each of these planes. By combining these three halftoned planes, a color halftone image is generated.

In the third module, based on the three images, that is, the image in which the data is hidden & two cover images, shares are generated.

In the fourth module, stacking of shares will be done. This process will give the image in which the data is hidden.

In the fifth module data extraction will be done. In the module, decryption algorithm will be applied on the image in which the data is hidden this will give the original data.

IV. CONCLUSION

In this paper various visual cryptography schemes are studied on various criteria: number of secret images, image format & type of share generated. Also this paper proposed a new way for hiding data in images using steganography & visual cryptography. First data is hided in color image using steganographic technique then shares are created of this color image using visual cryptography & these shares are transmitted to the receiver. The advantage of visual cryptography is that if any one captures a share then single share would not reveal anything about the data.

REFERENCES

[1] M. Naor & A. Shamir, "Visual Cryptography", advances in cryptology- Eurocrypt'94.Lecture notes in computer science,1-12,1994.

[2] G. Ateniese, C. Blundo, A. Santis & D. R. Stinson, "Extended capabilities for visual cryptography", ACM Theor. Comput. Sci., Vol.250,pp. 143-161,2001.

[3] E. R. Verheul & H.C.A. van Tilborg, "Construction & properties of k out of n visual secret sharing schemes", Designs, codes & cryptography, vol.11, no. 2, pp.179-196, 1997.

[4] M. Nakajima, Y. Yamaguchi, "Extended visual cryptography for natural images", in Proc. WSCG Conf. 2002, pp303-412.

[5] Y. C. Hou, "Visual cryptography for color images", Pattern Recognition, vol. 17773, pp.1-11, 2003.

[6] Hsien-chu Wu, Hao-Cheng Wang & Rui-Wen Yu, "Color visual cryptography scheme using meaningful shares", 8th International conference on intelligent systems design & applications, IEEE computer society, 2008.

[7] Q. Chen, X. Lv, M. Zhang, Y. Chu, "An extended color visual cryptography scheme with multiple secrets hidden", 2010 International conference on computational & information sciences, IEEE computer society, 2010.

[8] M. Kamath, A. Parab, A. Salyankar & S. Dholay, "Extended visual cryptography for color images using coding tables", International conference on communication, Information & computing technology(ICCICT), Oct. 19-20, 2012, Mumbai, India.

[9] P.S. Revenkar, A. Anjum, W. Z. Gandhare, "Survey of visual cryptography schemes", International Journal of security & its applications, vol.4, No. 2, April-2010.

[10] Soumik Das, Pradosh Bandyopadhyay, Proj Alai Chaudhuri, Dr. Monalisa Banerjee, "A Secured Key-based Digital Text Passing System through Color Image Pixels", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[11] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition 37 (2004) 469 – 474.

[12] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[13] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012.

[14] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18.