www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 7 July, 2014 Page No. 7214-7317

A Novel Approach for Data Hiding by integrating Steganography & Extended Visual Cryptography

Megha Goel[1], Mr. M. Chaudhari[2]

[1]PG Student, Dept. of Computer Science & Engg.,RTMNU, Nagpur, India
[1]megha.bgoel@gmail.com

[2]ASST. Prof. & HOD, Dept. of Computer Science & Engg.,RTMNU, Nagpur, India
[2] manojchaudhary2@gmail.com

Abstract: ***This paper proposes a novel approach for transmitting secret data securely by integrating steganographic method & visual cryptography. Steganography is the art & science of hiding data in the images. In the older age, our ancestors had also used the steganography. For eg., they use invisible ink, tattooing etc. for hiding secret information. In the digital age, secret data is hidden within the image, file, audio, video, text etc. Cryptography is the art & science of converting plain text or data into an unreadable form which is called as cipher text. The advantage of steganography over cryptography is that in cryptography everybody knows about the existence of the message but in steganography only the sender & the receiver knows about the existence of the message so it does not attract unwanted attention. Although there has been an extensive research in the past related to cryptography & steganography but neither of them provide enough security. So the proposed system combines steganography & visual cryptography for hiding data.***

Keywords: Cryptography, Steganography, Visual Cryptography, Shares, Halftone Transformation.

1. Introduction

Now a day the transmission of secret information through computer network has increased rapidly. So the security concerns of secret information have also grown proportionally. Cryptography & Steganography are the traditional method of providing security to the secret information.

In 1994 Naor & Shamir[1] proposed a new method called as visual cryptography for providing security to the secret information. Visual cryptography encrypts visual information such as pictures, printed text etc. in a perfectly secure way which can be decrypted by the human visual system. Visual cryptography encrypts a secret image into two or more cover images & then generates shares. Now these shares are transmitted to the intended receiver. The secret image can be recovered by stacking all the shares together.

In 1996, ateniese, blundo & stinson proposed extended visual cryptography schemes. The difference between visual cryptography & extended visual cryptography is that extended visual cryptography contains meaningful shares while visual cryptography contains random noise like shares.

This means that in extended visual cryptography each share carries some meaningful images rather than random dots.

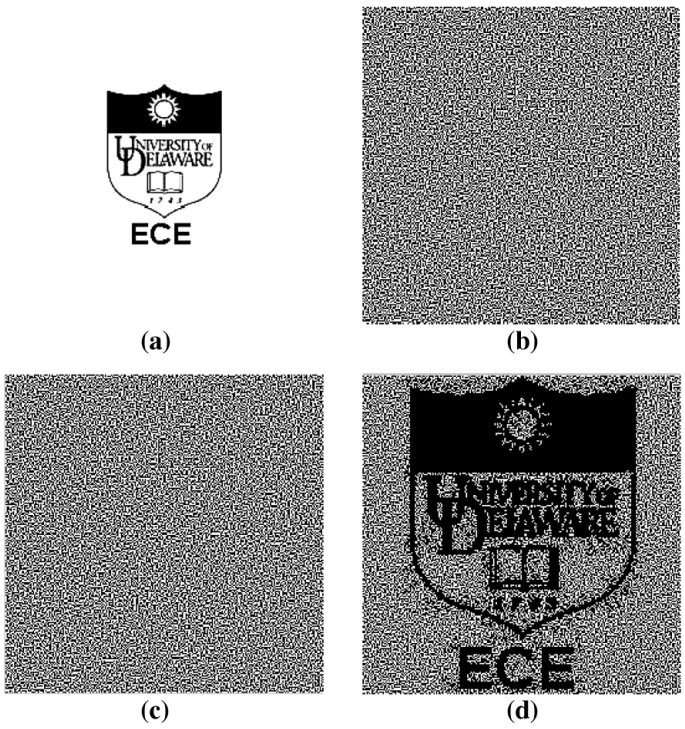


Figure 1: Example of basic visual cryptography. (a) Binary secret image. (b)share 1. (c) share 2. (d) Recovered secret message

2. Literature Survey

Naor & Shamir[1] proposed visual cryptography scheme in 1994. This is the basic scheme of visual cryptography in which the secret image is divided into two shares. The shares generated are meaningless. When the two shares are stacked together, it produces the original secret image. This scheme is only for black & white images.

Ateniese, Blundo & Stinson [2] proposed extended visual cryptography in 1996. This scheme contains meaningful shares.

Up to 1997, Visual cryptography schemes were applied to only black & white images.

Verheul & Tilborg [3], proposed first colored visual cryptography scheme. But this scheme produces meaningless share.

Nakajima & Y. Yamaguchi [4], proposed the extended visual cryptography scheme for natural images in 2002. This scheme also improves the quality of the recovered secret image.

Hou[5], in 2003, proposed another color VC scheme. This scheme uses halftone technique & color decomposition method. Halftone is a technique which converts gray level image to binary image. Color decomposition, decomposes the secret image into three colors C, M & Y.

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 the halftone 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.

Q. Chen, X. Lv, M. Zhang, Y. Chu [7], this scheme hide multiple secret images. This scheme generate meaningful images & can be applied to color images.

3. Proposed system

The proposed system presents a novel approach for transmitting secret data securely by integrating steganographic method & visual cryptography. The basic techniques for providing security to the data are cryptography & steganography. But neither of them alone provides enough security to the secret information over an untrusted communication channel & so hackers can attack the secret data. So the proposed system will provide better security than the above one.

There are two main procedures in the proposed scheme

A)Encryption

B)Decryption

Encryption process is divided into following modules

1) Data hiding

2) Halftone transformation

3) Generation of shares

Decryption is divided into following modules

1) Stacking of shares

2) Data extraction

A) Encryption

Following are the description of the encryption modules

1) Data Hiding

This module is based on the steganography. In this data is hided in one color image. This is the very basic concept of steganography. Many steganographic systems are available that pass data with digital media in the form of message digest. There is some steganographic algorithm that inserts the secret data directly in the LSB's of the image. But there are two main drawbacks of these methods.

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 framework overcomes both of the above drawbacks. Following is the working of the proposed framework.

Here, the secret data is first converted to a byte stream which is made up by the ASCII value of the characters present in the secret data. Then a 32 bit key & a hash function is applied on this byte stream & it will generate a pseudo byte stream. Now the LSB's of RGB bytes of the color image is retrieved & individual bits of this pseudorandom byte stream is embedded into those LSB's.

Following is the algorithm for embedding text into the color image.

Input: Color host image (HI), Text String (S)

Output: Text encrypted image (EI).

Stepl: H_I= getpixel_info (H1)

Step2: L_I = LSB_to_zero (HI)

Step3: A_T = ASCII_chopper (S)

Step4: H_{ASH} = Hash_func (K, L_I)

StepS: P_T = Pseudo_generator (A_T, H_{ASH})

Step6: EI= replace (L_I , P_T)

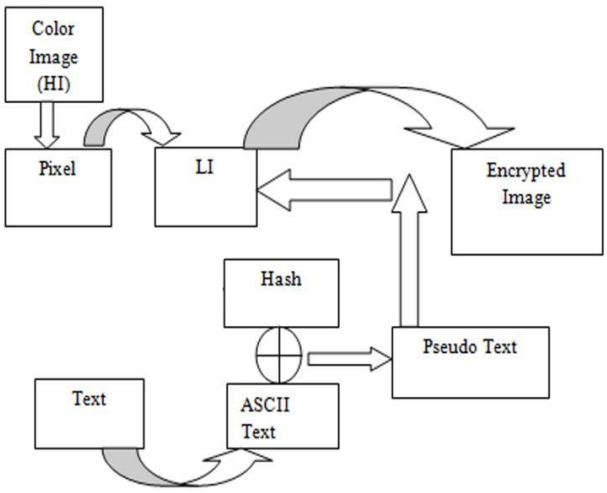


Figure 2: Diagram for embedding text

2) Halftone Transformation

In halftone Transformation the image in which the data is hided is decomposed into 3 constituent planes red, green & blue. Then the halftone technique is applied to translate the image into halftone image. Following figure shows the process:

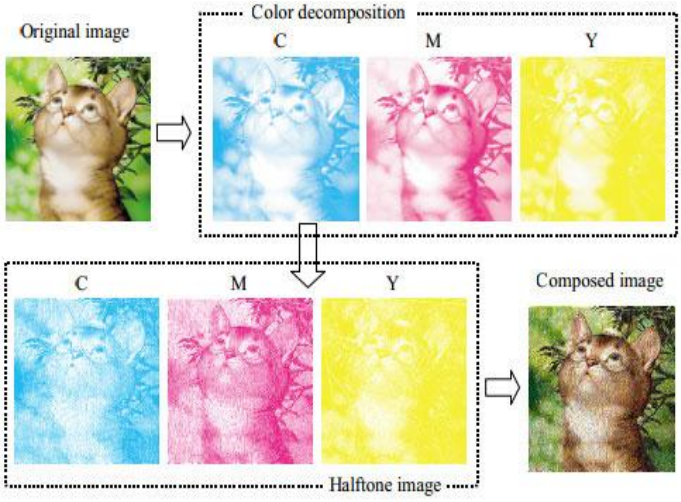


Figure 3: Halftoning Process

3) Generation of Shares

To generate meaningful color shares this paper uses the VIP synchronization & error diffusion method. VIPs are the pixels on the shares which represent color values of the original secret images, & thus make the encrypted shares meaningful. So, in this method, each subpixel carries visual information as well as message information to produce meaningful shares.

Example 1 ((2, 2)-Color EVC Matrices Derivation):
Consider the basis matrices S0 and S1 and of (2, 2)-VC scheme with m=4,λ=1
m -> total number of sub-pixel in each share of matrices
λ -> VIP pixel show color information

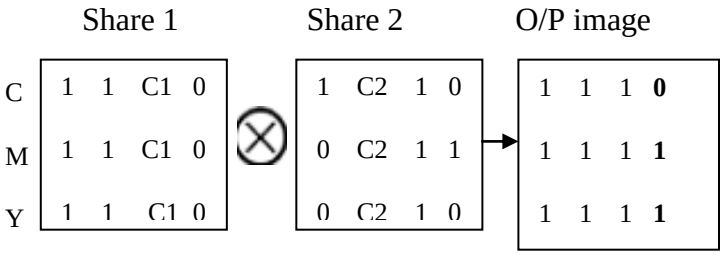
$$S1=\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad S0=\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

The first row in each of the matrices S1 & S0 are (1100) and (1100). We begin by inserting the C1's in the first row of each matrix as (1 1 C1 0) and (1 1 C1 0) the 0s at third position in each row is replaced with C1.

$$S1^{C1C2}=\begin{bmatrix} 1 & 1 & C1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad S0^{C1C2}=\begin{bmatrix} 1 & 1 & C1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

For the second rows, the condition of S0 & S1 is 0 not found then Switch the second and the third bits of s1. The condition S0 &S1 is 0 found at third position and replace them with C2 resulting in (0 C2 1 1) for $S1^{C1C2}$ and (1 C2 1 0) for $S0^{C1C2}$ as:

$$S1^{C1C2}=\begin{bmatrix} 1 & 1 & C1 & 0 \\ 0 & C2 & 1 & 1 \end{bmatrix} \quad S0^{C1C2}=\begin{bmatrix} 1 & 1 & C1 & 0 \\ 1 & C2 & 1 & 0 \end{bmatrix}$$



A) Decryption
Following are the description of the decryption modules

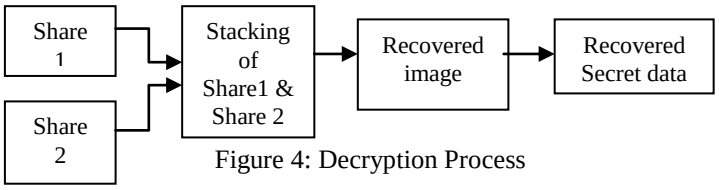


Figure 4: Decryption Process

1) Stacking of Shares

In this process, two shares are stacked together to reconstruct the secret image.

2) Data Extraction

After stacking the shares, we get recovered cover image. On this recovered image, apply decryption algorithm to extract the secret data.

Algorithm for Extracting Text:

[EXTRACT_TEXT]

Input: Text encrypted image (EI)

Output: Extracting Text (S)

Stepl:P_{T1} = retrieve (EI)

Step2:L_{I1} = LSB_to_zero (EI)

Step3:H_{ASH} = Hash _ func (K, L_{I1})

Step4:A_{T1}= ASCII_generator (H_{ASH}, P_{T1})

Step: S_1= Text_generator (A_{T1})

4. Conclusion

So, this paper proposes a novel approach for hiding data in color images by integrating steganography & extended visual cryptography. For share generation this paper uses the VIP synchronization. VIP synchronization retains the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes.

5. 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.