SECURED DATA HIDING BY USING EXTENDED VISUAL CRYPTOGRAPHY

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

[1]*PG Student, Computer Science & Engineering, PBCOE, Maharashtra, India*
[2]*HOD & Asst. Professor, Computer Science & Engineering, PBCOE, Maharashtra, India*

Abstract

Due to the rapid advancement of the internet large amount of data is transmitted over the internet. Some of the transmitted information is very important like password, confidential file, security codes etc. so it is very important to provide security to these data. In computer technology there are two ways to provide security to the data they are cryptography & steganography. Although, in the past, there has been various research related to cryptography & steganography but neither of them provide enough & strong security. So this paper proposes a novel approach for data hiding by combining steganography & extended visual cryptography. Visual cryptography was invented by Moni Naor & Adi Shamir in 1994. Visual cryptography hide secret image within one or more images & then generate shares. For share generation this paper uses Visual Information Pixel (VIP) & error diffusion technique.

***Keywords:** Steganography, Visual Cryptography, Share Generation, VIP, Extended Visual cryptography, Cryptography*

--***--

1. INTRODUCTION

1.1 Visual Cryptography

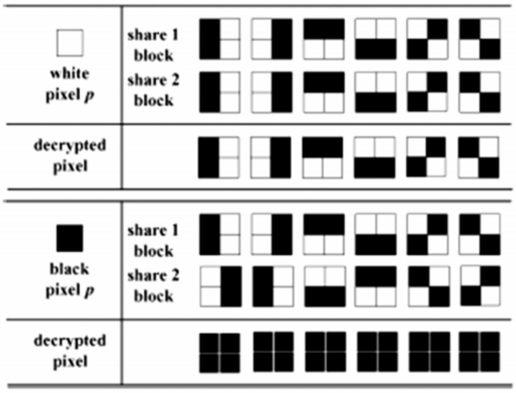
Visual cryptography is a secret sharing scheme proposed by Naor & Shamir [1] in 1994. In Visual cryptography secret images are divided into *n* number of shares & separately shares reveal no information about the secret image. Each share looks like a collection of random pixels & appear meaningless. These shares are distributed to *k* participants & recovery of the secret image is done by superimposing these shares. For decryption in traditional cryptography, require a key, but in visual cryptography it is done by the human visual system. In other words, visual cryptography does not require any software or complex computation technique for decryption. The summary of Naor and Shamir's schemes is
(1) The secret data is separated into *n* shares.
(2) Any *k* or more than *k* shares can recover the secret.
(3) Any *k-1* or fewer than *k* shares cannot recover the secret data.

1.2 Basic Model of Visual Cryptography

Following is the process of share generation. Each pixel p from the secret image is encoded into m black and white subpixels in each share. If pixel p is white or black one of the six columns from the Table 1 is randomly selected. Regardless of the value of p it is replaced by a set of 4 subpixels two of them black & two white. Now the subpixel in the share gives no clue about the original pixel p of the secret image.

Fig. 1 shows the basic 2-out-of-2 scheme of visual cryptography. Here the secret image is divided into two shares which look like a random collection of black & white pixels. These shares are distributed to two participants. Now separately these shares will not reveal anything about the secret image. After stacking the share 1 & share 2, secret image can be recovered.

Table 1: Construction of (2, 2) Visual Cryptography Scheme (VCS)



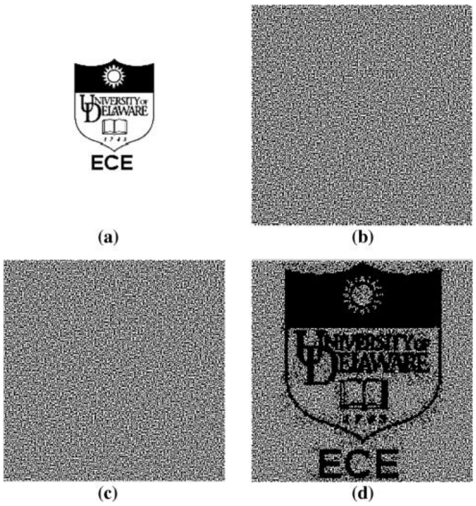


Fig 1: Example of 2-out-of-2 scheme. (a) Binary secret image. (b) Encrypted share 1. (c) Encrypted share 2. (d) Decrypted secret message.

1.3 Basic Schemes of Visual Cryptography

1. (2,2) VCS – This is the simplest & less secured scheme of visual cryptography. In this scheme secret image is encoded into 2 shares & also distrubuted to only two participants. For decryption two shares are overlaid. This scheme can be implemented by encoding each pixel of the secret image into either 2 subpixels or 4 subpixels as shown in the figure 2.
2. *(n,n) VCS* – This scheme encode the secret image into *n* number of shares. For decryption it also require all of the *n* shares. If we stack less than *n* shares than it will not reveal anything about the secret image.
3. *(k,n) VCS* – This scheme encrypt the secret image into *n* number of shares & distribute theses shares to *n* participants. For decryption it require *k* number of shares i.e. *k<n* & *k-1* shares will not provide any information.

1.4 Extended Visual Cryptography

Ateniese, Blundo & Stinson [2] proposed Extended Visual Cryptography. In EVC, shares contain secret information but these shares are meaningful share. In EVC, each share is some meaningful image rather than random collection of black & white pixels.

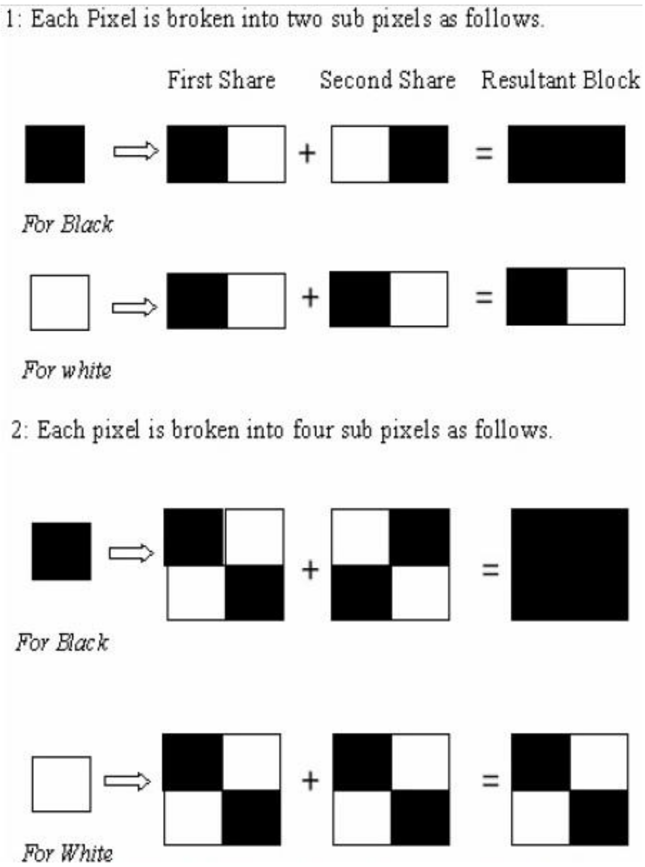
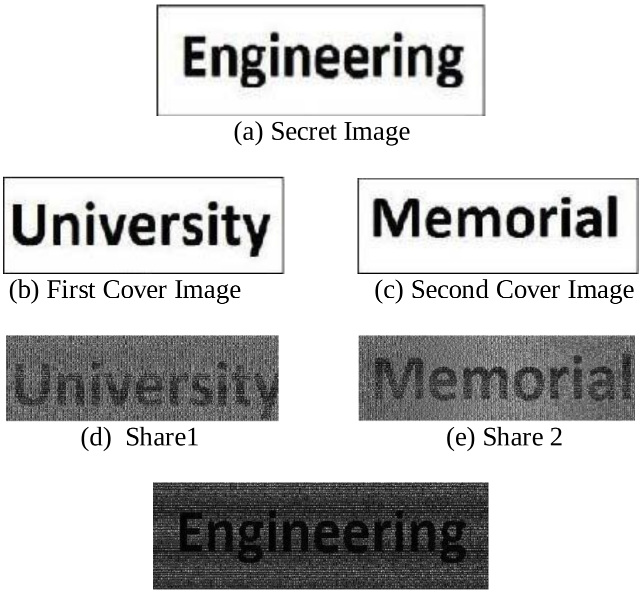

1: Each Pixel is broken into two sub pixels as follows.
First Share
Second Share
Resultant Block
For Black
For white
2: Each pixel is broken into four sub pixels as follows.
For Black
For White

Fig 2



(a) Secret Image

(b) First Cover Image

(c) Second Cover Image

(d) Share1

(e) Share 2

(f) Recovered Secret Image

Fig 3: Example of (2, 2) EVC Scheme

1.5 Steganography

Steganography is the art & science of passing information or hiding information in such a manner that the existence of information is known to the intended recipient only. The word steganography derived from Greek means “Covered Writing”.

Steganography uses various methods for hiding data. Previously our ancestors also used this method for secret communication. The media they were using are invisible inks, microdots, etc. today steganography uses test, images & soud media for hiding data.

There are number of ways to hide information in images. The most popular one are Least Significant Bit(LSB) Substitution, Masking & Filtering Technique.

2. RELATED WORK

Visual Cryptography is proposed by Naor & Shamir [1] in 1994. In Visual Cryptography, secret image is encoded into two or more images called as shares. These shares are similar to random noise like images. (2,2) is the masic model of visual cryptography.

Ateniese, Blundo & Stinson[2] in 1996 proposed Extended Visual cryptography which contain meaningful share images.

Upto 1997, Visual Cryptography schemes developed for black & white images only. Verheul & Tilborg[3] developed the first colored Visual Cryptography Scheme. But in this scheme share generated is meaningless.

Chang & Tsai [5] develop a color visual cryptography scheme & also generate meaningful share. In this scheme, secret color image is encoded in two color image called as cover images. This scheme uses predefined color Index Table. The disadvantage of this scheme is that it requires more storage space to store color index table. This disadvantage is overcome by Chin-Chen Chang et al. [6]. Nakajima & Yamaguchi [7] proposed Extended Visual Cryptography for natural images. This scheme produces meaningful binary shares.

Hou[8] proposed the visual cryptography scheme for gray level images. This scheme is based on the halftone technique & color decomposition method.

3. PROPOSED WORK

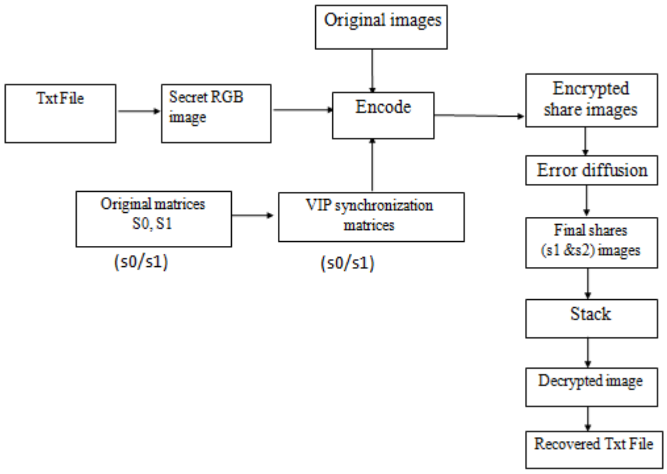


Fig 4: Framework of the proposed system

3.1 Data Hiding

This is the first module & it based on the steganography. In this secret data is hided in one color image using text embedding algorithm.

Following is the working of the algorithm.

- First retrive the pixel info i.e the R,G,B values of the pixel.
- Then convert the secret data into their ASCII equivalents, this forms a byte stream.
- Apply Hash function on that byte stream which will produce a pseudo byte stream
- This pseudo byte stream is hided in the LSB's of the image.

3.2 Generation of Shares

This paper uses VIP synchronization & error diffusion technique for share generation. VIP synchronization, this method, keep possession of pixels having visual information of original images & error diffusion technique is used to produce share of good quality.

3.3 Data Extraction

In data Extraction module, apply the text extracting algorithm on the recovered secret image.
Following is the working of the algorithm.
1) First retrive the pixel info i.e the R,G,B values of the pixel, this is the pseudo byte stream.
2) Then perform XOR operation between pseudo byte stream & Hash function to generate ASCII characters.
3) Then convert the ASCII byte stream to text string.

4. SIMULATED RESULTS

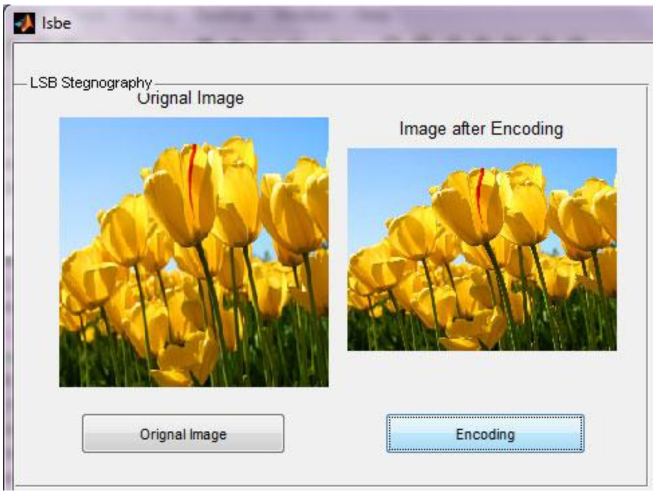
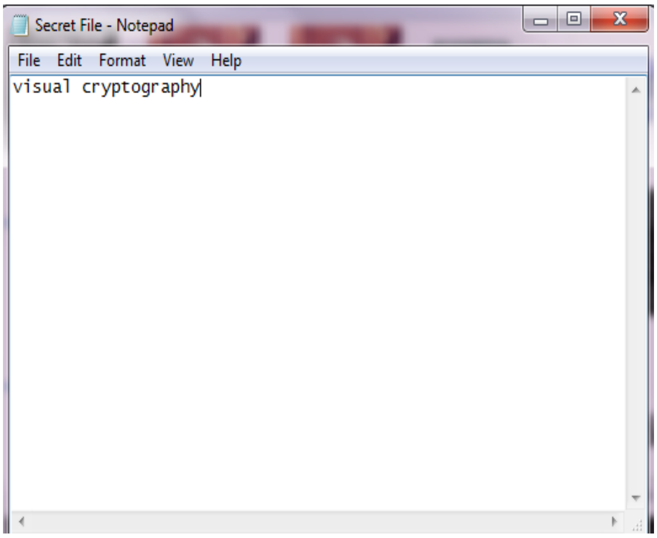


Fig.5 Data Hiding Screen



visual cryptography

Fig.6 Secret File

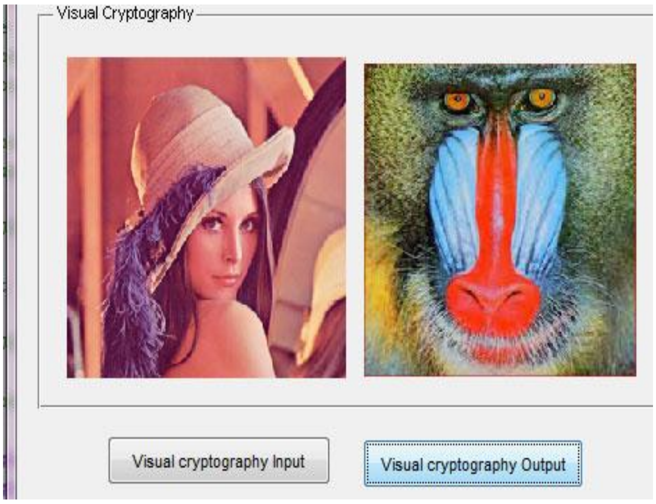


Fig 7 Selection of cover images

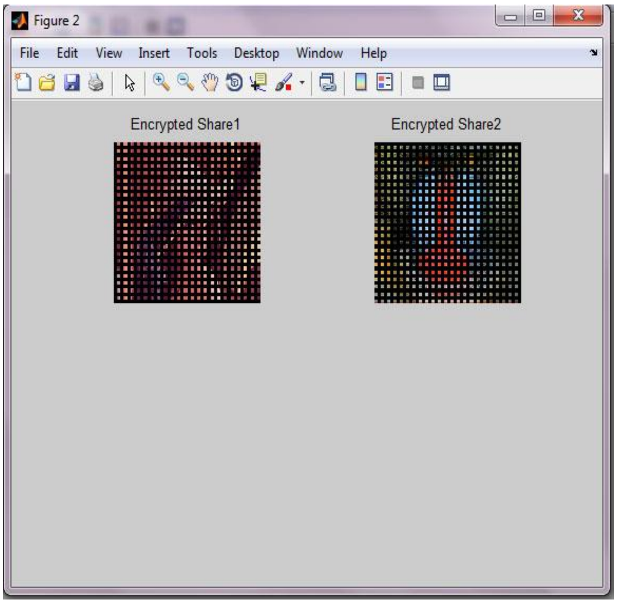


Fig 8 Generation of Shares

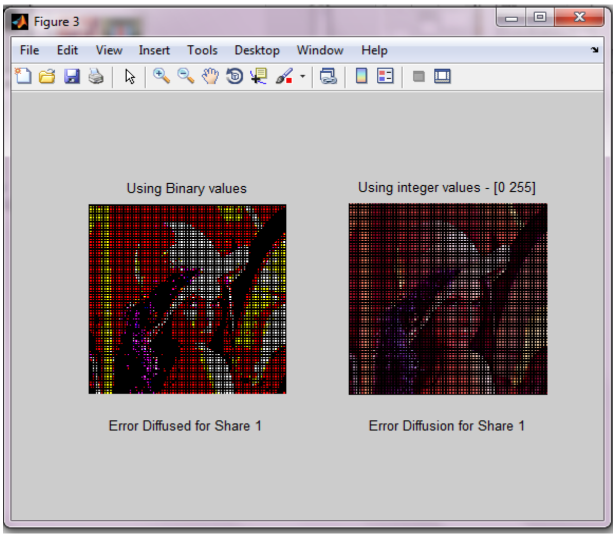


Figure 3
File Edit View Insert Tools Desktop Window Help
Using Binary values
Using integer values - [0 255]
Error Diffused for Share 1
Error Diffusion for Share 1

Fig: 9 Error diffused for share 1

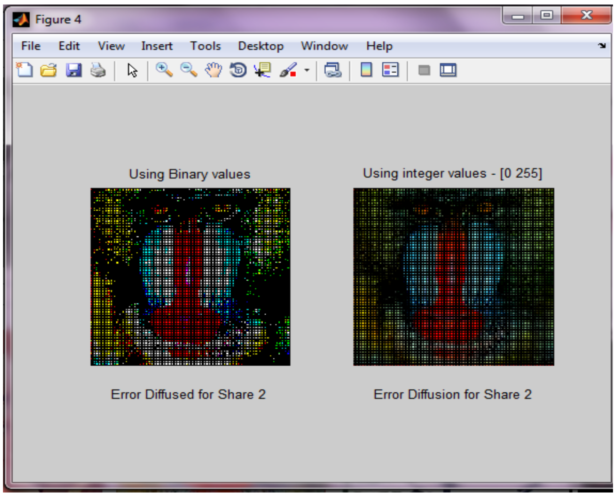
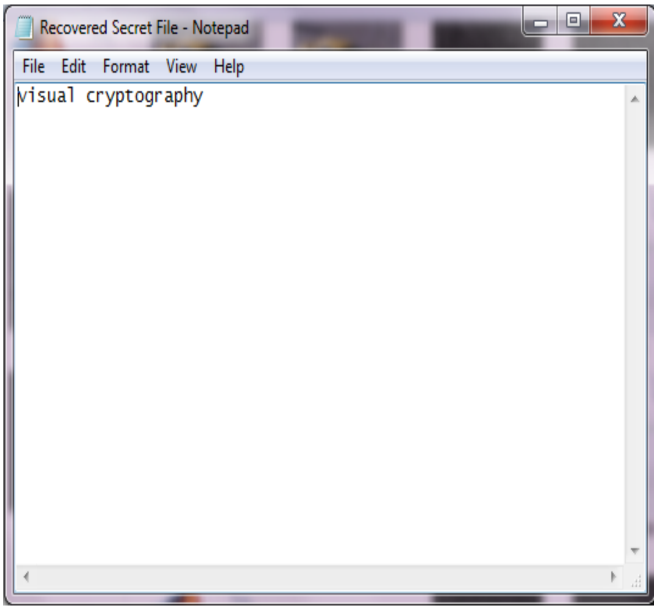


Figure 4
File Edit View Insert Tools Desktop Window Help
Using Binary values
Using integer values - [0 255]
Error Diffused for Share 2
Error Diffusion for Share 2

Fig: 10 Error diffused for share 2



visual cryptography

Fig: 11 Recovered Secret File

5. ANALYSIS OF THE RESULT

Following table shows the MSE & PSNR for the share1 & share 2.

Table 2 Result analysis of meaningful shares & their PSNR

Sr. No.	Color shares image	PSNR	MSE
1	Lena	30.6898 dB	55.4758
2	Baboon	31.1892 dB	49.4488
3	Pepper	30.6303 dB	56.242

6. CONCLUSION

This paper presents a novel approach for hiding data in color images by integrating steganography & extended visual cryptography. In Visual cryptography secret images are divided into n number of shares

For hiding data in color images, this paper uses text embedding algorithm & then for share generation which is a visual cryptography part, uses VIP synchronization & error diffusion technique. VIP synchronization, this method, keep possession of place of pixels having visual information of original images & error diffusion technique is used to produce share of good quality.

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]. C. Yang and C. Laih, "New Colored Visual Secret Sharing Schemes". Designs, Codes and cryptography, 20, pp. 325–335, 2000.

[5]. C. Chang, C. Tsai, and T. Chen. "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000.

[6]. Chin-Chen Chang , Tai-Xing Yu , "Sharing A Secret Gray Image In Multiple Images", Proceedings of the First International Symposium on Cyber Worlds (CW.02), 2002.

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

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

[9]. R.Youmaran, A. Adler, A. Miri , "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343, 2006.

[10]. Z. Zhou, Gonzalo R. Arce & Giovanni Di Crescenzo, Halftone Visual Cryptography, IEEE Transactions on image processing, vol. 18, no. 8, Aug. 2006

[11]. 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.

[12]. Z. M. Wang, Gonzalo R. Arce & Giovanni Di Crescenzo, Halftone Visual Cryptography via error diffusion, IEEE Transactions Inf. Forensics Security, vol.4, no. 3, pp. 383-396, Sep.2009.

[13]. 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.

[14]. John Blesswin, Rema, Jenifer Joselin, "Recovering secret image in visual cryptography" IEEE, 2011.

[15]. 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.

[16]. 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.

[17]. 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

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

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

[20]. 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.

[21]. 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.

[22]. N. Askari, N.H. Heys & C. R. Moloney, "An extended visual cryptography schemes without pixel expansion for halftone images", 2013, 26th IEEE Canadian conference of electrical & computer engineering.

[23]. Jin, D., Yan and Kankanhalli, M.S., Progressive color visual cryptography. J. Electron. Imaging. v14.