International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

A Novel Steganography Technique Using Visual Cryptography And Color Image Encryption

Nishit M.Vankawala[1],Komal M. Lineswala[2]

[1]*E.C. (ICT) Department, CGPIT Uka Tarsadia University, nishitvankawala@gmail.com*
[2]*E.C. (ICT) Department, CGPIT Uka Tarsadia University, komallineswala@gmail.com*

Abstract—In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. However, one of the main problems with sending data over the internet is the "security threat" it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration by employing techniques like cryptography and steganography. Both these techniques individually provide some security of data but neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks. Visual steganography is one of the most secure forms of steganography available today. However embedding data into image changes its color frequencies in a predictable way. To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format.

Keywords-Visual Cryptography; ciphers; Steganography; pixel transposition and shuffling

I. INTRODUCTION

Any information security algorithm is designed to satisfy three main objectives: confidentiality, data integrity and authentication. As cryptography and steganography complement each other, it is recommended to use these two techniques together for a higher level of security. Cryptography and steganography achieve separate goals. Cryptography conceals only the meaning or contents of a secret message from an eavesdropper. However, steganography conceals even the existence of this message.

Furthermore, steganography provides more confidentiality and information security than cryptography since it conceals the mere existence of secret message rather than only protecting the message contents[11].Therefore, one of the major weaknesses of cryptosystems is that even though the message has been encrypted, it still exists. A cryptographic system is considered broken if an attacker can read the secret message. However, a steganographic system is considered broken if an attacker can detect the existence or read the contents of the hidden message[12].

Visual Cryptography uses two transparent images in which first image contains random pixels and the second image contains the secret information [13]. The main advantage of this technique is that secret information cannot be retrieved without another image. Either transparent images or layers are required to reveal the information.

II. IMPLEMENTATION

2.1. Color Image Encryption

This algorithm is based on pixel transposition and shuffling. The shuffling of the image will be done by solely displacing the RGB pixels and also interchanging the RGB pixel values. At the end total image size before encryption will be the same as the total image size after encryption.
The images used will have their RGB colors extracted and their RGB values transposed and shuffled to obtain ciphered images. The ciphering of the images for this research will be done by using the RGB pixel values of the images only. In this method, there were no changes of the bit values of the images used and there was no pixel expansion at the end of the encryption and the decryption process [10].

Steps of Encryption process are as follows:

1. Resize color image into 126*126.
2. Decompose 126*126 into R, G and B planes and then convert into row vectors by reshaping these planes.
3. Combine row vectors to form matrix.
4. Again reshaping the matrix into one row vector (say t1).
5. Find length (T1) of t1.
6. Now divide t1 into three sections.
7. Then convert 3 1-D arrays into three matrixes (126*126) which is our encrypted images.

Steps for Decryption Algorithm are:

1. Reshape the obtained encrypted plane into 1-D array.
2. Divide 1-D array into three equal parts.
3. Convert each part into matrix to form original image.
4. Combine three planes to form original image.

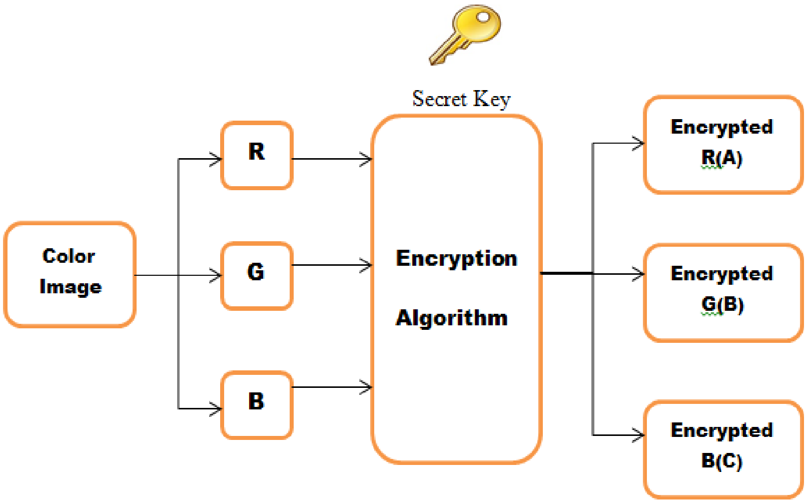


Figure 1. Block diagram implementation of color encryption

2.2. Visual Cryptography

In this paper (2, 2) VC Scheme is used as key in which the original image is divided into two shares such that each pixel in the original image is replaced with a non-overlapping block of two or four sub-pixels as shown in Fig. 2.

2.3. Novel Steganography Technique

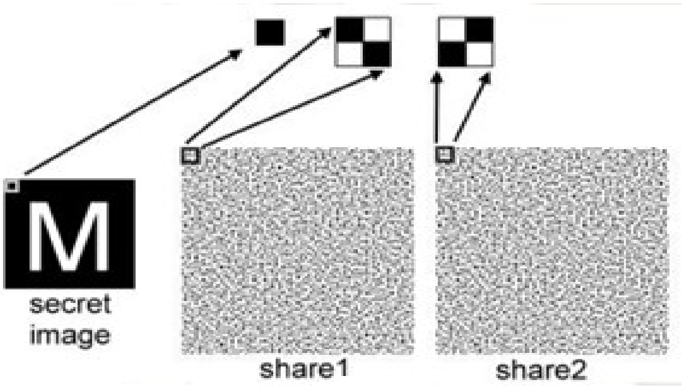


Figure 2. Visual cryptography

A new technique of hiding stego image into cover image is proposed in which pixel values of every encrypted planes of ciphered image is normalized and added to the pixel values of cover image. And at receiving side, the pixel values of cover image is subtracted from the original pixel values of cover image and thus pixel values obtained are de-normalized so as to obtain pixel values of ciphered image. The advantage of using this process is that addition of pixel values does not change significance of values as only decimal part of value changes, hence resolution of image is not affected. Steps of applied Steganography are:

1. Decompose Cover image into R, G and B.
2. Hide encrypted R and G planes into R plane of cover image.
3. Similarly encrypted B plane into G plane of cover image.
4. The two shares obtained from Visual Cryptography are embedded into decomposed cover image B.
5. Then embedded R, G and B are reconstructed to form Stego image.

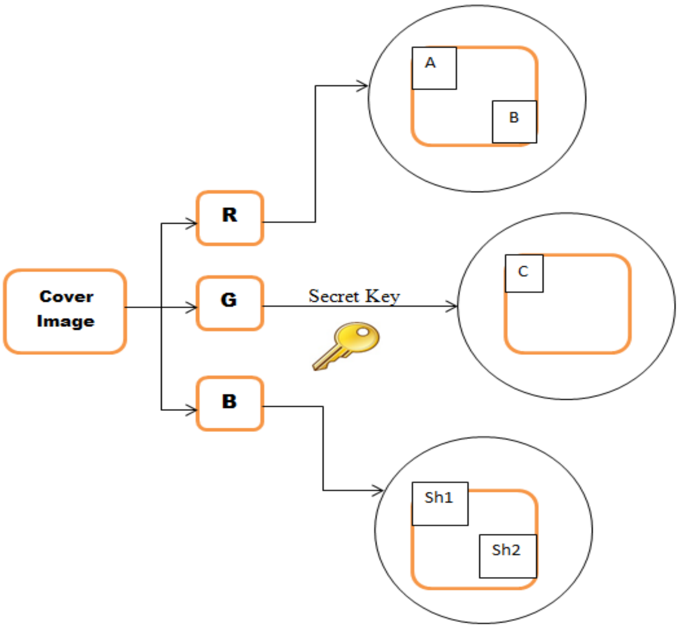


Figure 3. block diagram of formation of stego-image

Steps to obtain encrypted images from Stego Image:

1. Stego Image is first decomposed.
2. Then recover back the hidden encrypted images from decomposed images.
3. Apply Decryption Algorithm to recovered image to obtain original secret message.

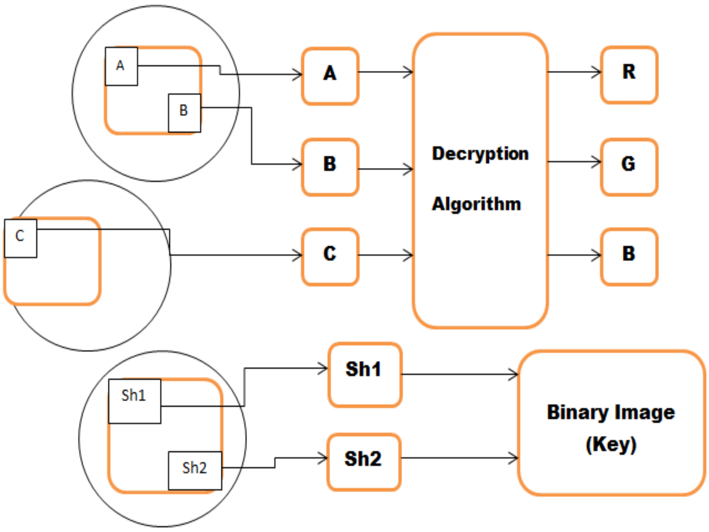


Figure 4. Decryption of stego-image

III. RESULTS

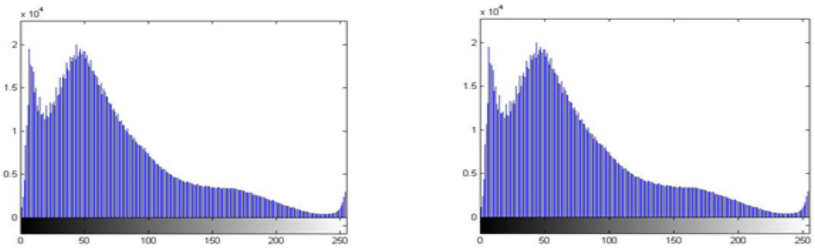
Table 1. Comparison between MSE and SNR

Size And Resolution		Observed Result	
Cover Image	**Hidden File (KB)**	**MSE**	**PSNR**
2.19 MB (2048 x 1536)	169 (1280 x 1024)	1.60 e-22	169.8098
	526 (1600 x 1200)	4.823 e-23	175.0357
	56.2 (600 x 750)	3.4557 e-23	176.4838
	102 (1000 x 1000)	1.280 e-22	170.7733
800 KB (1680 x 1050)	169 (1280 x 1024)	7.4183 e-21	153.1662
	526 (1600 x 1200)	1.646 e-21	159.7045
	56.2 (600 x 750)	4.8907 e-21	154.9755
	102 (1000 x 1000)	4.9103 e-21	154.9581

Comparing the above results with LSB, the most popular technique of Steganography concludes that MSE and PSNR values are far better (MSE is e^-22 in comparison to e^-10 and PSNR is ~170 in comparison to ~97) and provide three levels of security i.e. steganography, VC and key applied during encryption phase.

CONCLUSION

The proposed approach in this paper uses a new steganographic approach which provides two levels of security that is during encryption phase using key and during embedding process using VC as a key. The proposed approach provides higher security and can protect the message from stegoattacks. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the legitimate password.



Histogram of Cover Image

Histogram of Stego Image

Figure 6. Comparison of histogram of cover and stego image

V. FUTURE SCOPE

The security obtained using this approach is good but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption and implement this steganography technique in frequency domain where security can be increased further. Also, Visual

Steganography can be implemented for color images and can be used for sharing information rather using it for security purpose as in this case.

REFERENCES

[1] J. R. Smith and B. O. Comisky, "Modulation and information hiding in images," in Information Hiding, First International Workshop, Lecture Notes in Computer Science, R. Anderson, Ed. Berlin, Germany: Springer-Verlag, 1996, vol. 1174, pp. 207–226.

[2] Krenn, J.R., "S*teganography and Steganalysis",* IEEE communication magazine 2004.

[3] N. F. Johnson and S. Jajodia, *"Steganography: Seeing the Unseen",*IEEE Computer, Feb. 1998,pp. 26-34.

[4] X. Zhang , and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity", IEEE Signal Processing Letters, vol. 12, Issue 1, Jan. 2005, pp.67-70.

[5] H.C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc. Vision, Image and Signal Processing, vol. 152, Oct. 2005, pp. 611 -615.

[6] A.Sarkar, K. Solanki, and B.S. Manjunath, *"Further Study on YASS:Steganography Based on Randomized Embedding to Resist BlindSteganalysis"*, in Proc. SPIE - Security, Steganography, and Watermarking Of Multimedia Contents X, SanJose, California ,vol. 6819, pp.681917-681917-11, Jan.2008.

[7] Li Zhi,Sui Ai Fen and Yang Yi Xian,*"A LSB Steganography DetectionAlgorithm",* The 14m IEEE 2003International Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings.

[8] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar," A novel technique for image steganography based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.

[9] Kester, Q. Aphetsi, Koumadi, Koudjo M , "*Cryptographietechnique for image encryption based on the RGB pixeldisplacement*," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.74-77, 25-27 Oct. 2012

[10] R. Mathews, A. Goel, P. Saxena& V. P. Mishra, "*Image Encryption Based on Explosive Inter pixelDisplacement of the RGB Attributes of a PIXEL*", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol 1 WCECS 2011, October 19-21, 2011, San Francisco,USA

[11] A. Kahate, "*Cryptography and network security",* 2nd ed. McGraw-Hill 2008.

[12] J.R Kahn, "S*teganography and Steganalysis",*IEEE communication magazine 2004.

[13] J. Verma, Dr.V.Khemchandani," *A Visual Cryptographic Technique to Secure Image Shares*", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1, Jan-Feb 2012, pp.1121-1125.