Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 8, August - 2015

Secure The Secret Information In An Image Using K-MM In Steganography

Amanjot Kaur[1]
Student M.Tech IT
CEC, Landran,Mohali
Mohali, 140307, India
jotk387@gmail.com

Dr. Bikrampal Kaur[2]
Prof. IT Department
CEC Landran, Mohali
Mohali, 140307, India
cecm.infotech.bpk@gmail.com

***Abstract*—Steganography can be defined as the art to perform invisible communication. Steganography usually deals with method of hiding any content in data to be communicated so that it can remain confidential. The prime purpose of steganography is to provide confidentiality in communication. In image steganography, secrecy is achieved by embedding data image and generating a stego-image. There are different types of steganography techniques each have its pros and cons. In this paper, secret data is secured by using k-Modulus Method.**

Keywords—Steganography, k-Modulus Method, PSNR, MSE, BER.

I. INTRODUCTION

In this age of technology, need of communication is increasing with considerable pace. Evolution of internet brought vast changes to methods of communication but initially internet was designed on the basis of trust. With the passage of time when internet became public need of privacy and confidential communication has increased. The whole scenario of less secure transmission and necessity of privacy gave birth to steganography[1]. Steganography is art to communicate in such way that it can hide the existence of element of communication [2]. Various files can be used as platform to conduct steganography for example JPEG files, audio files. A text can be embedded to JPEG file which will be hidden even this will not change its original size. Social engineering is providing a great platform to conduct steganography these days [3].

II. LITERATURE REVIEW

This section discussed about the literature review. This dissertation figured the different researches given by different researchers.

In 2013, Firas A Jasim[7], to hide text inside grey scale images created a practical steganographic implementation. Using Five Modulus Method the secret message is hidden in cover image. For each of the images, Peak Signal-to-Noise Ratio(PSNR) is captured. The stego image has high PSNR value, based on the PSNR value of each image.

In 2013, Mamta Juneja[8] a new LSB(Least Significant Bit) based edge embedding technique using hybrid edge detection filter to improve the capacity and PSNR. This method ensures the higher PSNR value and high embedding capacity. Also this method provides security against various attacks e.g. visual analysis, histogram analysis, chi-square and RS analysis.

In 2013, Rama Kant Singh et al. [9] proposed a steganography technique; the Saliency based steganography technique has advantage of lesser perceptual degradation compare to other techniques. The secure data may be kept in background or foreground as required. This technique provides both advantages, non-prominent area selected for steganography as well as less affect in segmentation boundaries.

In 2013, Firas A. Jassim[10] proposed a novel method to use two cover images as host images with one secret(stego) image. The main aim of this technique is to increase the security at the receiver end when sending each host image alone in different times. The first phase starts with sending the first cover image alone with special stego key. The second phase sends the other cover image with different stego key. The performance metrics have proven that the reconstructed secret image has high PSNR value with very small MSE.

III. PRELIMINARIES

The method used to hide the information in image is the k-Modulus Method.

k- Modulus Method

Initially, k-Modulus Method (k-MM) was initially suggested by [11]. In fact, it was originated as a technique for image transformation to hide information in it that can serves as a *good* host. It is renowned that simple difference between the original image and the transformed image do not affect the human visual system (HVS). In practice, the lossy JPEG compression is one of the best examples that can be best describing this fact. There are some differences in resulted image from JPEG compression from the original bitmap image. But these differences are ignored since it does not have an effect on the final visual image quality [12]. Undeniably, k-MM and JPEG compression are both sharing the same principle of producing slight differences.

The k-MM embarks with converting the entire image pixels into multiples of positive integer $k > 0$. According to [11], the best accessible result that can

be achieved is at $2 \leq k \leq 10$. In case of $k = 5$, the complete image pixels are converted into multiples of 5, i.e. 0, 5, 10. . . 255. In case of $k = 10$, the same procedure can be applied and the new transformed values are 0, 10, 20,. . . 250. In terms of value of PSNR, the 5-MM outputs higher PSNR than 10-MM. Actually, this is because the disimilarities from the original image are smaller in 5-MM than 10-MM.

IV. PROPOSED ALGORITHM

There are different algorithm steps used to secure the information.

1. Read the original colored image.
2. Extract the three different layers that are Red layer (R layer), Green layer (G layer) and Blue layer (B layer).
3. Apply 10-MM on G and B layer of the original image.
4. Hide secret message into secret image, this is hiding stage 1 and this is called stego secret image.
5. Apply 5-MM on stego secret image.
6. Hide this stego secret image into G and B layer of the original image, this is hiding stage 2 and the image after embedding is called stego image.

Block diagram

The block diagram of the algorithm is shown in Figure 1:

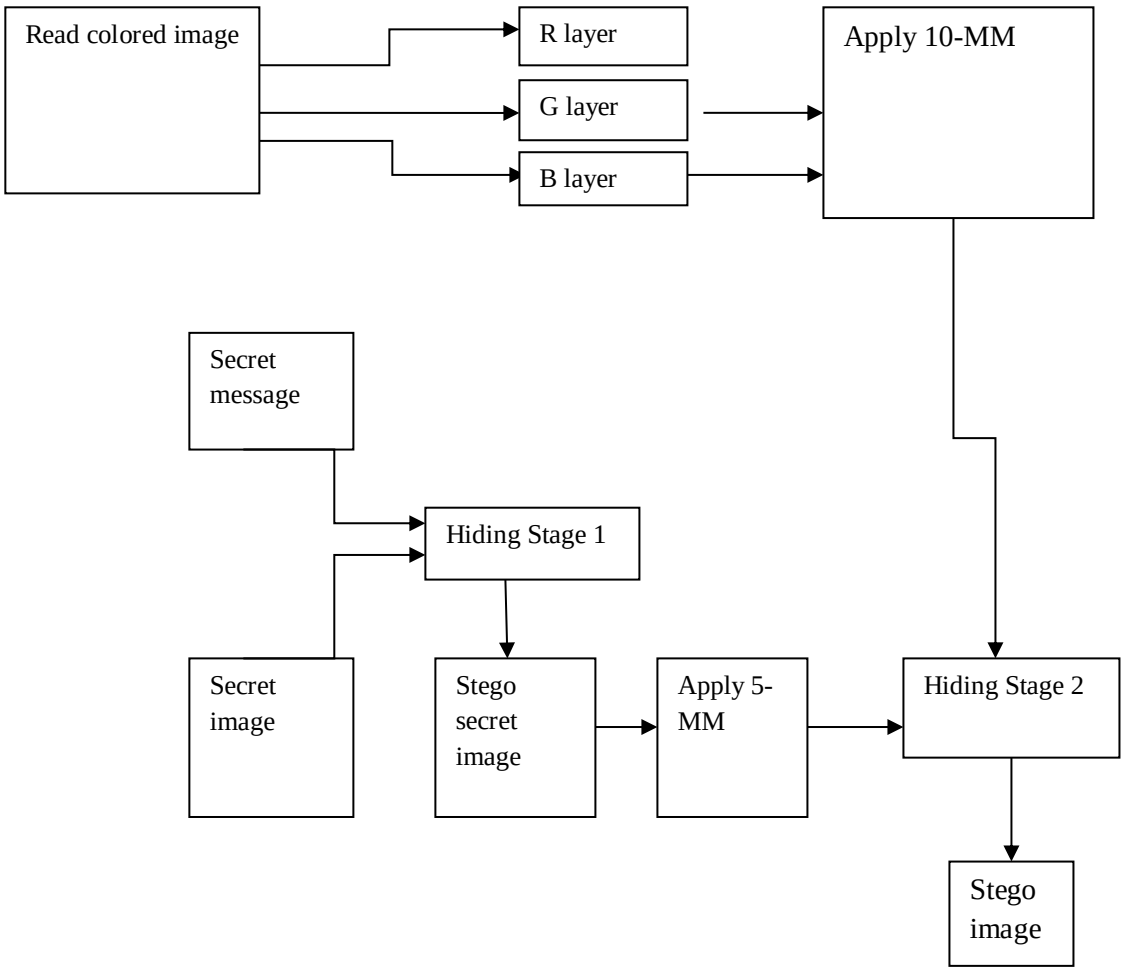

Figure 1: Block diagram of proposed algorithm.

V. RESULTS

MATLAB software and Image and Video Processing toolbox is required to precede the research. In the following Table 1, there are three images. In first image, there is original image that is cover image. In second image, there is the image after applying k-MM. In the third image, there is stego image in which secret information is hidden. The results of three images are shown below.

Table 1: k-Modulus Method Transform (Original Image, k-MM Transform, Stego Image)

Sr.no.	Original Image	MM Transform	Stego Image
1.			
2.			
3.			

In the following Table 2, the results of the above k-MM are shown. In this table, there are three parameters that is PSNR, BER, MSE are used. The secret data is 256 KB for all the three images. In the first image, the secret message of length 23 bytes are embedded in secret image of size 256 KB that is the stego secret image. Then apply 5-MM on stego secret image and this image is hide into the G and B layer of the original image of size 512 *512 on which the 10-MM is apply. The values of PSNR, BER and MSE for this image are 8.7972, 0.0205 and 0.8577 respectively. In the second image, the message length of secret data is 36 bytes are embedded in same size secret image. Same technique is used for second image and the value of parameters PSNR, BER and MSE are 49.5330, 0.0202 and 0.7241 respectively. In the third image, the secret message of length 51 bytes are hidden in the same size secret image that is 256 KB. The values of three parameters PSNR, BER, MSE are 53.2849, 0.0188 and 0.3052 respectively.

Table 2: Results of proposed algorithm

Data	PSNR	BER	MSE
256KB	48.7972	0.0205	0.8577
256KB	49.5330	0.0202	0.7241
256KB	53.2849	0.0188	0.3052

VI. CONCLUSION

This paper proposed a novel embedding approach based on k-Modulus Method for colored images. From experimental results it is clear that the proposed technique obtained high PSNR along with good image fidelity for various images which conform k-Modulus Method based image steganography can obtain better security.

References:

[1] R. Chandramouli and N. D. Memon, "Steganography Capacity: A Steganalysis Perspective", SPIE Security Watermarking Multimedia Contents, vol.5020, 2003, pp. 173-177.

[2] Krenn. R.,"Steganography and Steganalysis," Internet Publication, January 2004. Stuti Goel, Arun Rana, Manpreet Kaur,"A Review of Comparison Techniques of Image Steganography," Global Journal of Computer Science and Technology Graphics & Vision, vol. 13, no. 4, 2013, pp. 9-14.

[3] Francesco Quierolo, "Steganography in images".

[4] Johnson, N. F. And Jajodia, S. (1998), "Exploring Steganography: Seeing the unseen", Computer, vol. 31, no. 2, 1998, pp. 26-34.

[5] Neils Provos, Peter Honeyman, Hide and Seek: Introduction To Steganography(2003).

[6] N.F. Johnson, S. C .Katezenbeisser , "A Survey of Steganographic Techniques" in Information Techniques for Steganography and Digital Watermarking, S. C. Katezenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75.

[7] Firas A. Jassim, "A Novel Steganography Algorithm for hiding text in image using Five Modulus Method", International Journal of Computer Applications, vol.72, no.17, June 2013.

[8] Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique," J Inf Process Syst, vol. 9, no. 4, Sept 2013.

[9] Rama Kant and Brejesh Lall, "Saliency Map Based Image Steganography," 28th International Conference on Image and Vision Computing New Zealand, 27 Nov 2013.

[10] Firas A. Jassim, "A Novel Steganography Algorithm to hide a Grayscale BMP Image in Two Grayscale BMP Images for Dual Secrecy", 2nd National Conference on Information Assurance (NCIA), vol.4, no.8,11 Dec 2013.

[11] F. A. Jassim, "k-modulus method for image transformation," International Journal of Advanced Computer Science and Applications, vol. 4, no. 2, 2013, pp. 267–271.

[12] R. C. Gonzalez and R. E. Woods, *Digital image processing*, 3rd ed. Prentice Hall, 2008.

[13] H. S. Majunatha Reddy and K. B. Raja, (2009),"High Capacity and Security Steganography using Discrete Wavelet Transform,"International Journal of Computer Science and Security,2009, pp. 462-472.

[14] V. Nagaraj, Dr. V. Vijayalakshmiand Dr. G. Zayaraz,"Modulo Based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.