Secure RGB Image Steganography Based on Triple-A Algorithm and Pixel Intensity

Md. Mizanur Rahman, Pronab Kumar Mondal, Indrani Mandal, Habiba Sultana

Abstract— Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, even perceives the existence of the hidden message. In this paper, the concept of RGB intensity properties is being merged with randomization based Triple-A algorithm to increase the hidden capacity of the data-bits. Usually, storing variable number of bits in each channel (R, G or B) of pixel depend on the actual color values of that pixel. The concept- channels containing lower color values, can store higher number of data bits. This technique can be applied to RGB images where each pixel is represented by three bytes to indicate the intensity of Red, Green, and Blue of that pixel. This work shows more effective results, especially the capacity of the data-bits to be hidden with relation to the RGB image pixels.

Index Terms— Steganography, RGB Bitmap image, Randomization, High Capacity Embedding, Computer Security, Histogram.

1 Introduction

THE word Steganography originally derived from two Greek words-Steganos which means "covered or secret", and Graphein which means "writing or drawing". In this case, Steganography literally means covered writing. Basically, it is a secret transmission of message between two parties. It is the practices of encoding or embedding secret information in a manner that the existence of the information becomes invisible. This mechanism has been exercising for thousands of years in various forms. In ancient Greece, the common practices consisted of etching messages in wooden tablets and covering them with wax, or tattooing a messenger's head after shaving hair and then let his hair grow up before sending him to the receiver where his hair was shaved again to extract the massage. Other techniques use invisible ink, microdots, converting channels and character arrangement [1, 2, 3, 4].

Steganography is the art and science to covert communication. It can be achieved by using carriers like image, audio and video. In image Steganography the information is hidden exclusively in an image called cover media. After inserting the secret message it is referred to as stego-image or stego-medium. A stego key is used for hiding or encoding process to restrict detection or extraction of the embedded data. So image Steganography process can be described by the under-mentioned structure:

Cover image + Embedded message + Stego key = Stego image

The stego-image then sends to the receiver over the public channel. The receiver can extract the message through using the stego key which is same as used by the sender. The Fig. 1 shows basic Steganography process.

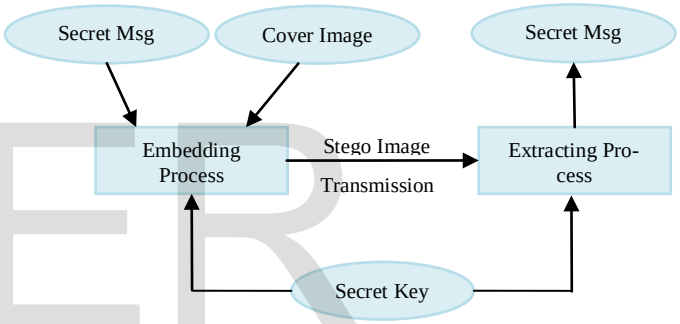


Fig. 1: Steganography process

Pixel is the smallest unit of an image. Digital images are stored in computer systems as an array of points (pixels) where each pixel has three color components: Red, Green, and Blue (RGB). Each pixel is represented with three bytes to indicate the intensity of these three colors (RGB).

There are many applications of image based Steganography, such as-confidential communication and secret data storing [5, 15], access control system for digital content distribution [6], digital watermarks [7, 14], and modern printers [9]. Moreover, it can also be used to tag notes to online images and illegitimate purposes.

This paper endeavors to improve Triple-A algorithm [12] by adding intensity of pixel that was not considered before. The basic concept is, the lower intensity of the pixel decides the number of bits to embed in the cover-image. Because the lower intensity pixel does not distort the visual quality of pixel, and it can also store higher number of bits, which has been showed in Fig. 3.

The rest of the paper is organized as follows: Section 2 presents some Steganography related existing methods. Section 3 describes our improved technique based on Triple-A algorithm and intensity property. The experimental results and comparison will be in section 4. Finally, conclusions are given in section 5.

- ***Md. Mizanur Rahman*** *is a Lecturer in Department of Computer Science and Engineering at Ranada Prasad Shaha University, Dhaka, Bangladesh. E-mail:* ***mizan173@gmail.com***
- ***Pronab Kumar Mondal*** *and* ***Indrani Mandal*** *are Assistant Professor, and* ***Habiba Sultana*** *is Lecturer in Computer Science and Engineering Department, Jatiya Kabi Kazi Nazrul Islam University, Dhaka, Bangladesh.*

2 Related Work

Several methods have been proposed for image based Steganography where the Least Significant Bit (LSB) substitution is the simplest one [10, 13, 16]. In LSB, the least significant bit of each pixel for a specific color channel or for all color channels is replaced with a bit from the secret data. Although LSB is simpler than other techniques, it has long standing probability of detecting the hidden data. But hiding information through this algorithm has significant risk. Later Pixel Indicator (PI) based stego system proposed by Adnan Gutub [1, 17] has substantiated the overall concept. This technique uses the least two significant bits of one of the channels from Red, Green or Blue as an indicator for existence of data in the other two channels. The indicator bits are set randomly in the channel. But it is hard to predict the embedding capacity through Pixel Indicator methodology. However, another notable technique is the Stego Color Cycle (SCC) [11].This SCC technique uses the RGB images to hide the data in different channels. That is, it keeps cycling the hidden data between the Red, Green and Blue channels, utilizing one channel at a cycle time. This technique is more secure than the LSB but still it is suffers detecting the cycling pattern that will reveal the secret data. Also it has less capacity than the LSB. Overall Triple-A technique uses the same principle of LSB, where the secret is hidden in the least significant bits of the pixels, with more randomization in selection of the number of bits and the color channels that are used [12]. This randomization is expected to increase the security and capacity of the system.

3 Proposed Method

In this section, at first we review the Triple-A technique in [12].Triple-A algorithm taking the message (M), the carrier image (C), and the password based generated key (K) depending on password (P), as inputs and produces the message (M) hidden inside the carrier image (C). This algorithm can be divided into two major parts, Encryption and Hiding as it is shown in Fig. 2.

In part one the message (M) encrypted using AES algorithm which will produce Enc (M, K). The key K can be generated from a set of user passwords each with a specific key using simple XOR.

In part two, the RGB Image is used as a cover media. It utilizes the advantage of the Bmp images, where every pixel is independent from the rest of the image file. Enc (M, K) is hidden according to Triple-A algorithm which needs to have a pseudo random number generator (PRNG). The assumption for PRNG is to give two new random numbers per iteration. The seeds of these PRNGs namely Seed1 (S1) and Seed2 (S2) are formed as a function of the Key (K). S1 is restricted to generate numbers in [0-6] while S2 is restricted to the interval [1-3].

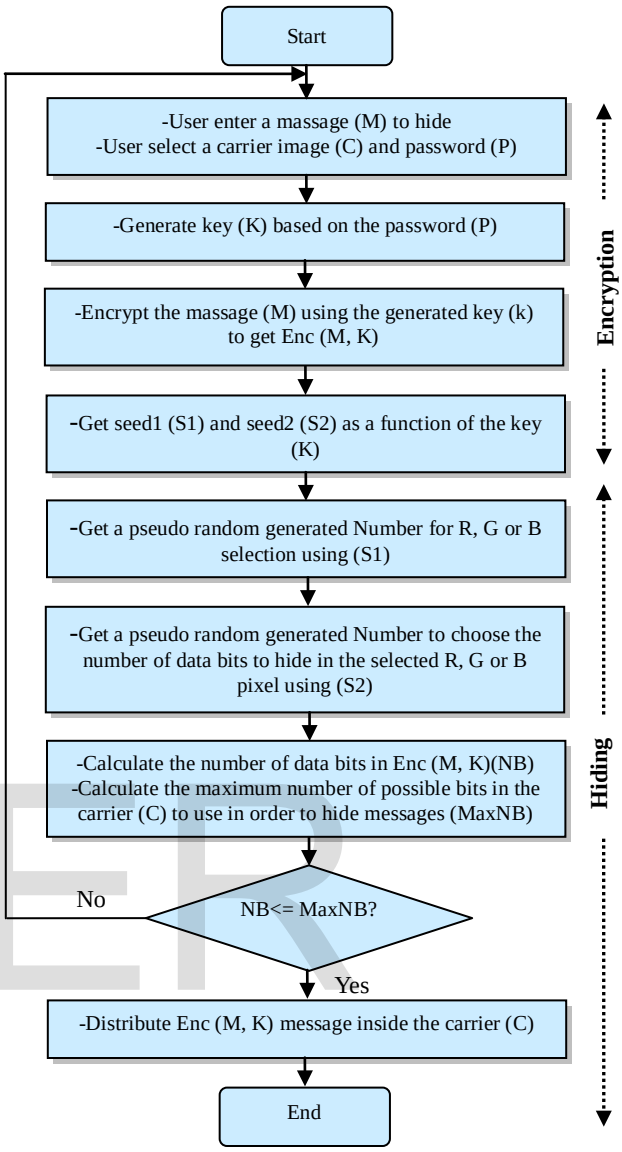


Fig. 2: Flow chart of Triple-A algorithm

Table 1 shows how S1 random number is used to determine the component of the RGB image which is used in hiding the encrypted data Enc (M, K). On the other hand, Table 2 shows how (S2) random number determines the number of the component(s) least significant bits that is used to hide the secret data. On the same way (S2) random number determines the number of component bits.

Table 1: Seed1 Random Number Usage

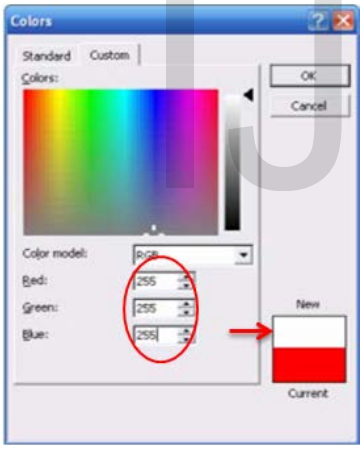
	Random number	Meaning to the algorithm
1st PRNG	0	use R.
	1	use G.
	2	use B.
	3	use RG.
	4	use RB.
	5	use GB.
	6	use RGB.

Table 2: Seed2 Random Number Usage

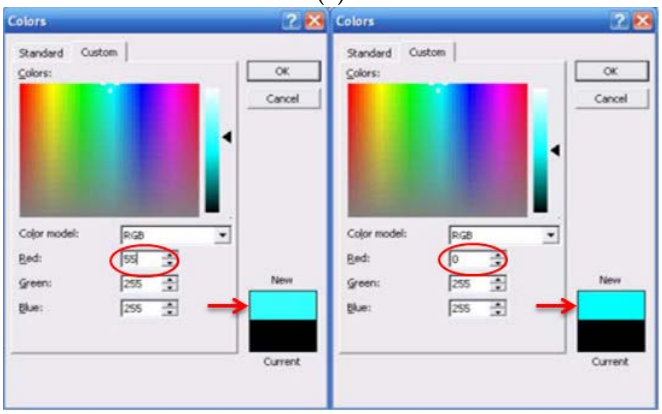
2nd PRNG	Random number	Meaning to the algorithm
	1	use 1 bit of the component(s).
	2	use 2 bit of the component(s).
	3	use 3 bit of the component(s).

Two tables show that the algorithm may add up to a maximum of ± 7 to the value of the color component(s) in that pixel. Also, by combining data from the previous tables, we can see that the minimum number of bits used in each pixel is 1 if we use only one bit of one chosen components of the RGB image. The maximum is 9 bits if we used all the three components with three bits.

We have improved Triple-A algorithm [12] with respect to pixel intensity, where color intensity (values of R-G-B) is used to decide the number of bits to store in pixel. Our technique ensures a minimum capacity and can accommodate to store large amount of data. Our idea is that, 'insignificant' colors, significantly more bits can be changed per channel of an RGB image, because change in lower intensity pixel value has less visual degradation quality effects. For example according to the Fig. 3, three pixels (R=255, G=255 and B=255) are generating White color in (a). In (b), the color component is same as (a), except that R = 55 generate Green color. In (c), we again set the 4 LSBs of R to zeros, resulting in a color which seems to be same as (b).



(a)



(b) (c)

Fig. 3: Effect of colors for changes in the 'Red' values

Same scenario occurs for Fig. 3 where if we modify the 4 LSBs (0 to 15) of all pixels (RGB). So, if pixel intensity is less than 16, it can be modified into 0 to 15 ranges, which will not be degrade the visual quality of that pixel. So we can also embed up to 4 bits into that pixel.

Our conception is that, in comparison with higher value of channel the lower color value has less effect on the overall color of pixel. Therefore, more bits can be changed in a channel having 'low' value than a channel with a 'high' value. When RGB component has to be chosen we need to select the lower color-value channel among the three channels to store higher number of bits. Therefore, the structure demands to insert the following steps, and Fig. 4 shows the steps in flow chart.

- Calculate the channel, whose color value is lowest among the channels.
- Decide the maximum number of data bits to store in its least significant bits.
- Store the decided number of data-bits in that channel.

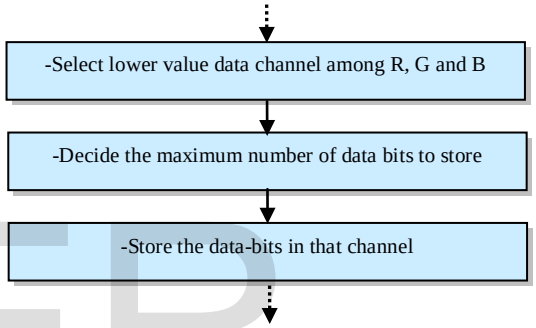


Fig. 4: Flow chart of our proposed steps

Fig. 5 demonstrates one example of storing data bits in a channel. Suppose the data channel (R) is chosen where pixel value is **22** (**00010110**) and data bits to embed is **0101**. After embedding data bits pixel output value will be **27** (**00011011**).

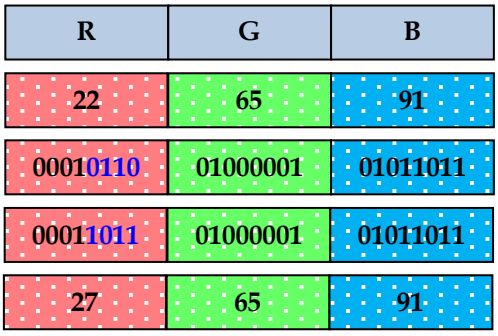


Fig. 5: An example of hiding data bits inside a channe

4 Result Analysis and Comparison

This section of the paper describes the experimental results of our proposed method, and also the comparison with the other works. Carrier images have been used to hide text message. Fig. 6 shows an original carrier compared to the same carrier with secret message using our modified algorithm. From the first moment, the visual change between the original image and stego-image cannot be predicted; but the histogram of the

images which is shown in Fig. 7 shows a minor different in the value of the components: R, G and B.

(a) Original carrier

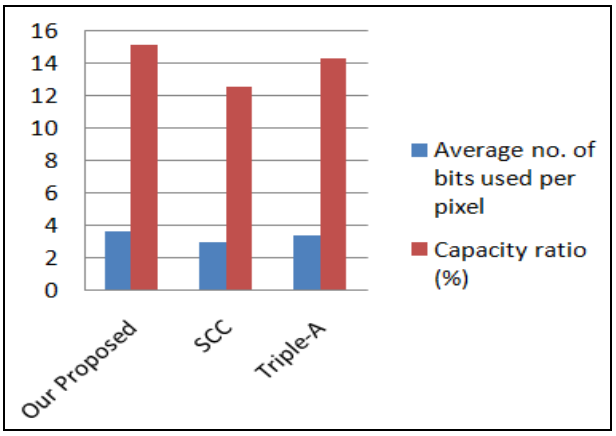
(b) Carrier with secrete using modified algorithm

Fig. 6: Image Steganography testing example

Theoretically, the average number of bits are used per pixel is equal to 3.62 where the average number for Triple-A is 3.42, SCC is 3, and for LSB is 1. This shows us that the capacity of the new proposed technique is higher than the previous techniques. The average capacity ratio of our method is 15.08% of the original cover media size. This is better than SCC and Triple-A algorithm where the capacity ratio is 12.50% and 14.28% respectively. Another advantage of this technique is that the use of minimum number of pixels to hide a message M inside carrier C.

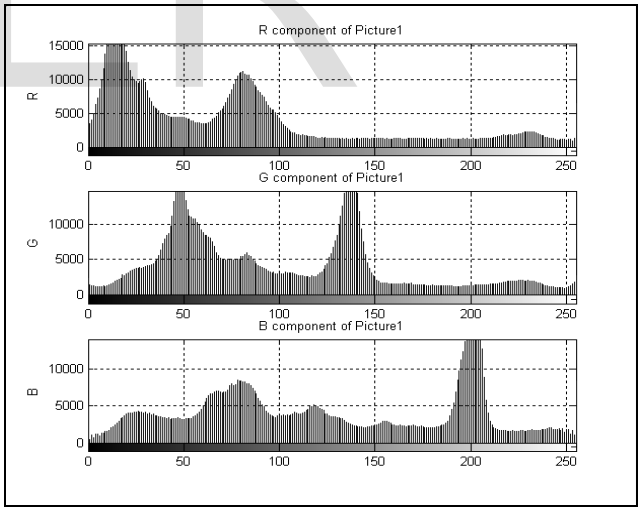
Table 3: Comparing SCC, Triple-A and proposed technique

Size of M (bytes) 28 KB	Average no. of bits used per pixel	Pixels used to hide M inside C	Capacity ratio
Our Proposed	3.62	6958	15.08%
SCC	3.00	27984	12.50%
Triple-A	3.43	7169	14.28%

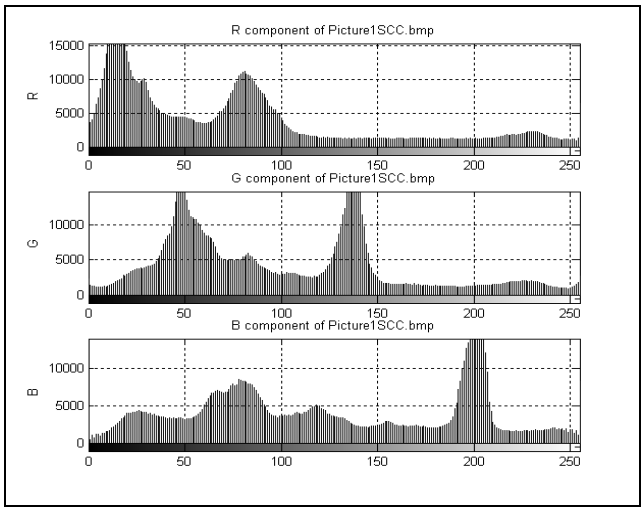


Graph 1. Average number of bits and Capacity in KB

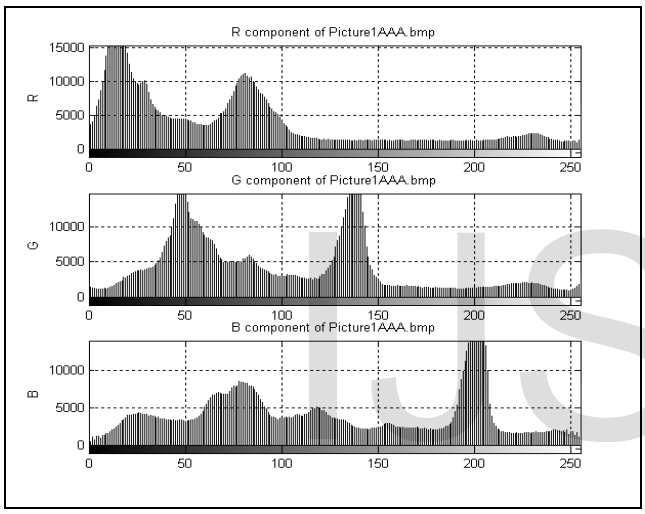
The main advantage of our proposed method is if we utilize the color intensity value of cover-image to hide the data bits, then our algorithm has very high capacity of data hiding as compare Triple-A algorithm. In Triple-A [12] it does not utilize the lower intensity based pixel for high capacity data embedding. Table 3 and Graph-1 shows a comparison result of our proposed algorithm with Triple-A and SCC. The table and graph shows that the capacity ratio of our proposed method is more than Triple-A. The result is obtained using different carrier images and averaging the number of pixels used in the hiding operation. It also shows that our technique enhance the capacity ratio without affecting the image with noise or distortion.



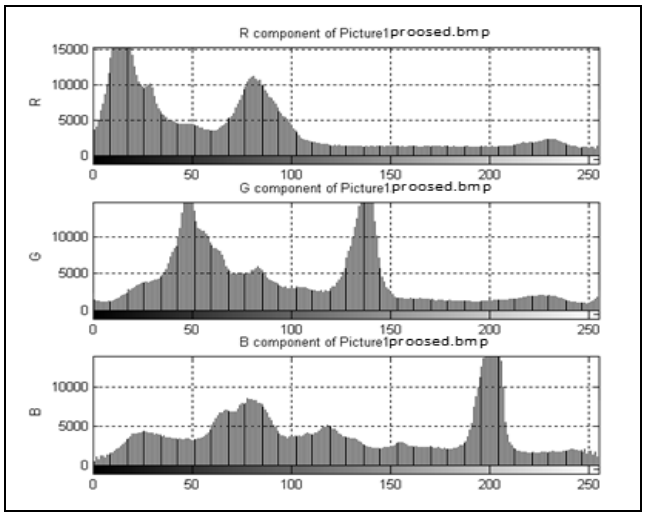
(a) Original carrier



(b) Carrier with secrete using SCC algorithm



(c) Carrier with secrete using Triple-A algorithm



(d) Carrier with secrete using Proposed algorithm

Fig. 7: Image Steganography histograms

5 Conclusion

In this paper we have explored the existing image Steganography techniques, and have improved the data hiding capacity of existing Triple-A algorithm [12]. Mainly the proposed algorithm uses actual color of the channel in conjunction with pseudo random number generator (PRNG) to decide the number of data bits to store. In our technique we have utilized the lower intensity based pixel for high data embedding. This approach leads to very high capacity with visual quality is as close to Triple-A algorithm.

Acknowledgment

The authors would like to express their sincere thanks to the anonymous reviewers for their constructive feedback, which helped significantly improving technical quality of this paper.

References

[1] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, AbdulrahmanShaheen, and AleemAlvi, "Pixel Indicator high capacity Technique for RGB image Based Steganography", WoSPA 2008 – 5thIEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008.

[2] Adnan Gutub, LahouariGhouti, Alaaeldin Amin, TalalAlkharobi, and Mohammad K. Ibrahim, "Utilizing Extension Character 'Kashida' With Pointed Letters For Arabic Text Digital Watermarking", InternationalConference on Security and Cryptography - SECRYPT, Barcelona, Spain, July 28 - 31, 2007.

[3] Adnan Gutub and ManalFattani, "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", WASET InternationalConference on Computer, Information and Systems Science andEngineering (ICCISSE), Vienna, Austria, May 25-27, 2007.

[4] Mohammad TanvirParvez and Adnan Gutub, "RGB Intensity Based Variable-Bits Image Steganography", APSCC 2008 – Proceedings of 3rdIEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12 December 2008.

[5] N.F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE computer, Vol. 31, No. 2, pages 26-34, February 1998.

[6] Fridrich, Jiri. "Applications of data hiding in digital images." Signal Processing and Its Applications, 1999. ISSPA'99. Proceedings of the Fifth International Symposium on. Vol. 1. IEEE, 1999.

[7] F.A.P. Petitcolas, "Introduction to information hiding", in: S. Katzenbeisser and F.A.P. Petitcolas, (ed.) (2000) Information hiding techniques for steganography and digital watermarking, Norwood: ArtechHouse, INC.

[8] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." Security & Privacy, IEEE 1.3 (2003): 32-44.

[9] Silman, Joshua. "Steganography and steganalysis: an overview." Sans Institute 3 (2001): 61-76.

[10] C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.

[11] S. Venkatraman, A. Abraham, M. Paprzycki, "Significance of Steganography on Data Security", International Conference on Information Technology: Coding and Computing (ITCC'04), 5-7 April 2004.

[12] Gutub, Adnan, Ayed Al-Qahtani, and AbdulazizTabakh. "Triple-A: Secure RGB image steganography based on randomization." Computer Systems and Applications, 2009.AICCSA 2009.IEEE/ACS Inter-

national Conference on.IEEE, 2009.

[13] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods", Multimedia Tools and Applications, Vol. 30, No. 1, Pages: 55 – 88, July 2006.

[14] J.-L. Dugelay and S. Roche, "A survey of current watermarking techniques," in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. A. P. Petitcolas, Eds. Norwood, MA: Artech House, 1999, ch. 6.

[15] Bender, Walter, et al. "Techniques for data hiding." IBM systems journal 35.3.4 (1996): 313-336.

[16] Donovan Artz, Los Alamos National Laboratory, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing: May, 2001.

[17] Nabarun Bagchi. Article: Secure BMP Image SteganographyUsing Dual Security Model (I.D.E.A, image intensity andBit Randomization) and Max-Bit Algorithm. InternationalJournal of Computer Applications 1(21)(2010):18–22.