An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection

Marwa M. Emam
Computer Science Department
Minia university, Egypt

Abdelmgeid A. Aly
Computer Science Department
Minia university, Egypt

Fatma A. Omara
Computer Science Department
Cairo university, Egypt

***Abstract*—with the rapid advance in digital network, information technology, digital libraries, and particularly World Wide Web services, many kinds of information could be retrieved any time. Thus, the security issue has become one of the most significant problems for distributing new information. It is necessary to protect this information while passing over insecure channels. Steganography introduces a strongly approach to hide the secret data in an appropriate media carriers such as images, audio files, text files, and video files. In this paper, a new image steganography method based on spatial domain is proposed. According to the proposed method, the secret message is embedded <u>randomly</u> in the pixel location of the cover image using Pseudo Random Number Generator (PRNG) of each pixel value of the cover image instead of embedding sequentially in the pixels of the cover image. This randomization is expected to increase the security of the system. The proposed method works with two layers (Blue and Green), as (<u>2</u>-<u>1</u>-<u>2</u>) layer, and the byte of the message will be embedded in three pixels only in this form (<u>3</u>-<u>2</u>-<u>3</u>). From the experimental results, it has found that the proposed method achieves a very high Maximum Hiding Capacity (MHC), and higher visual quality as indicated by the Peak Signal-to- Noise Ratio (PSNR).**

Keywords—Image Steganography; PRNG (Pseudorandom Number Generator); Peak Signal-to-Noise Rate (PSNR); Mean Square Error (MSE)

I. Introduction

Data security or data privacy has become increasingly important as more and more systems connected to the internet. In general, protecting the secret messages during transmission becomes an important research issue. To protect secret message during transmission, there are two ways to solve this problem. One way is encryption, which refers to the process of encoding secret information in such a way that only the right person with the right key can decode and recover the original information successfully. Another way is steganography technique, which hides secret information into a cover media or carrier so that it becomes unnoticed, and less attractive [1]. Steganography is one of the important and elegant tools used for securely transfer secret message in an imperceptible manner [2]. The word steganography in Greek means " covered writing" (Greek words "stegos" meaning "cover" and "grafia" means "writing") [3]. In general, steganography is the art of hiding a message signal into a host signal without any perceptual distortion of the host signal. It hides the secret message within other innocuous looking cover files, called carriers, (i.e. images, text files, audio files, or video files) so that it cannot be observed [4]. The most frequently used carriers are digital images.

There are two common techniques of embedding in image steganography; ***spatial domain*** and ***transform domain*** [5].According to spatial domain, the secret data or secret message has directly embedded into the LSBs (**<u>L</u>**east **<u>S</u>**ignificant **<u>B</u>**it) of image pixels. One of the most known examples of spatial domain method is LSB insertion [6]. In transform domain, the message embedded by modifying frequency coefficients of the cover image [7]. The work in this paper concerns about the spatial domain.

The basic types of steganography are ***linguistic*** and ***technical*** steganography. Linguistic steganography takes advantage of the properties of natural language, such as the linguistic structure to hide the messages. While technical steganography is the method of steganography where a tool, device, or method is used to conceal the message and it can be classified into; image, audio, video and text steganography [8].

The basic model of steganography is shown in Fig.1. According to this Figure, steganography process consists of carrier, message, and password. Carrier is also known as cover-object or cover-image, in which message is embedded. The message can be any type of data (plain text, cipher text, or image) that the sender wishes to remain confidential. Password has known as stego-key, which ensures that only recipient who has the stego-key will be able to extract the message from a stego-object. Finally, the cover-object with the secretly embedded message called the stego-object or stego-image [9].

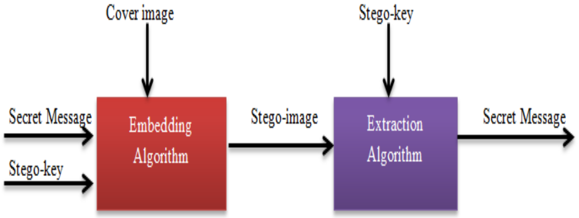

Fig. 1. The Basic model of Steganography

The main goal of stenographic system is the image quality. The **<u>P</u>**eak **<u>S</u>**ignal-to-**<u>N</u>**oise **<u>R</u>**atio (**PSNR**) and **<u>M</u>**ean **<u>S</u>**quared **<u>E</u>**rror (**MSE**) metrics are the most common measures used to evaluate the quality of the image [10].

PSNR is one of the metrics to determine the degradation in the embedding image with respect to the cover image. MSE measures the difference between two images. PSNR and MSE defined in equations 1 and 2 [10].

$$MSE = \left(\frac{1}{MN}\right) \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - X'_{ij}\right)^{2} \qquad (1)$$

$$PSNR = 10\, log_{10}\, \frac{I^2}{MSE} \qquad (2)$$

Where X_{ij} is the i^{th} row and the j^{th} column pixel in the original (cover) image, X'_{ij} is the i^{th} row and the j^{th} column pixel in the reconstructed (stego) image, M and N are the height and the width of the image, I is the dynamic range of pixel values, or the maximum value that a pixel can be taken, for 8-bit images; I=255.

The rest of this paper is organized as follows; related work will discuss in section 2, the proposed method will discussed in details in section 3, performance evaluation will give in section 4. Finally, section 5 concludes the paper.

II. Related Work

In [11], a modified image steganography method based on LSB technique has presented. This method presents the message by six binary bits by using LSBraille method (Braille method of reading and writing for blind people) instead of using the ASCII encoding format. This method works with two layers of the RGB image (Blue, and Green layer). The byte of the message is hidden in two pixels only; the first three message bits is hidden in the first pixel and the last three message bits sre hidden in the second pixel by starting with the blue layer then the green layer in the same pixel. According to this embedding way, only two bits for each character of the cover image are changed; 1-bit from blue layer and 1- bit from green layer. In the Blue layer, two bits per pixel are embedded, the message is not only embedded in the first least significant bit (LSB), but also the second least significant bit, and the third least significant bit are allowed to be changed. However, during each process of embedding, only 1-bit of the Blue layer will allowed to be changed. This process is done by taking the last three bits of the Blue layer pixel and applied two equations using the XOR function. Then the third bit of the message in the least significant bit of the Green layer will embedded in the same pixel, and so on as.

In [12], the authors have proposed a secure method of steganography in which three main entities are exercises; pseudo random number generator, Least Significant Bit (LSB) substitution, and Optimal Pixel Adjustment Process (OPAP). In this method, cyclic pixel and indicator technique are used where two channels have been used as data channels and the remaining channel is used as an indicator channel. Red plan has been taken as indicator channel for the first pixel for the subsequent pixels the indicator channels follows a periodic cycle of R, G, and B barring the indicator channel, the other two channels act as the data channels for the corresponding pixels. The pixel intensity determines the bits to be embedded (i.e., LSB's of the indicator channel). If the LSB's of the indicator channel (say R channel) are 00 embed k bit in G and k+1 bits in B; in case of 01 embed k+1 bits in G and B. if LSB(R) is 10 embed k+1 bits in G and k+2 bits in B. If LSB(R) equals 11 embed k+2 bits in G and K+2 bits in B. A novel 2-key based pseudo random generator is employed which is used to embed data completely in a unique random fashion based on the user's choice.

Madhu et al [13] have proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. It generates random numbers and selects the region of the interested where in the required message is embedded along the random pixels. This method is target to improve the security where password is added by LSB of pixels.

In [14], an algorithm called Triple-A algorithm has been proposed. This algorithm uses the same principle of LSB, where the secret message is hidden in the least significant bits of the pixels with more randomization in the selection of the number of used bits and the color channels that are used. This algorithm is divided into two parts (encryption, and hiding). In the hiding part, the RGB image is used as a cover media, which needs to have a pseudorandom number generator. The assumption of PRNG is in every iteration provide two new random numbers as seeds. The seeds of these PRNGs are namely Seed1 (S1), and Seed2 (S2). S1 is restricted to generate numbers in [0, 6], while S2 is restricted to the interval [1, 3]. S1 random number is used to determine the component of the RGB image that is going to be used in hiding the encrypted data. On the other hand, (S2) random number determines the number of the component(s) least significant bits that is used to hide the secret data.

In [15], a spatial domain method has been proposed. The principal of the proposed method is that LSB -3 (Third Least Significant Bit) of the cover image has been used to embed the message bits, and LSB -1, 2 may be modified according to the bits of the message to minimize the difference between the cover and the stego-cover. For more protection to the message bits, a stego-key has been used to permute the message bits before embedding it. However, the results of this method showed that the LSB -1 method has more PSNR values than that the proposed method, which means the LSB -1 image's quality is better than of the modified one, in the same time, the capacity still the same as the modified one.

In [16], a new method is proposed. This method hides the secret message based on searching about the identical bits between the secret message and image pixel value. One pixel of the image is chosen randomly and the image is divided into three layer (Red, Green, and Blue), and then two bits of the secret message are embedded in each layer in the two least significant bit by searching about the identical.

III. The Proposed Method

In this section, the proposed method will present. The proposed method is divided into two algorithms; the embedding algorithm, and the extraction algorithm. The embedding algorithm will plan to hide the byte of the secret message in three pixels only based on randomization in the cover image. It takes the cover image and the secret message characters as an input and converts each byte from the secret message to its binary format using the ASCII encoding format (each byte equal 8-bits). Then, the cover image is converted into three layers (Red, Green, and Blue) layer. Each pixel in the (Blue, and Green) layers is converted to its binary using the

ASCII encoding format. In the embedding technique, **(2-1-2)** layer is used (i.e. two layers (Blue and Green) are used in the first iteration), in the second iteration only one layer is used (i.e., Blue). In the next iteration, two layers are used (Blue and Green) and so on. The using of two layers then one layer then two layers leads to more secure and getting better PSNR value. The secret message is embedded randomly in the pixel locations using **P**seudo **R**andom **N**umber **G**enerators (**PRNG**) instead of sequential. This method of embedding is considered more secure than the embedding in a sequential manner. The message bits have been embedded in the form of **(3-2-3)**. In which the first 3-bits from the message are embedded in the first random pixel (2-bits in the blue layer at the least and second less significant bit, and 1-bit at the LSB of the green layer). Then, the second 2-bits from the message (fourth and fifth bits) are embedded in the second random pixel at the least and second less significant bit LSB of the Blue layer. After that, the last 3-bits from the message (the sixth, seventh, and eighth bits) are embedded in the third random pixel (2-bits in the blue layer at the least and second less significant bit, 1-bit at the LSB of the green layer), and so on as.

Pseudo Random Number Generator:

Pseudorandom number generator acts as a black box, which takes one number (called the seed), and produces a sequence of numbers. The ideal PRNG can generate a unique random integer, to implement the PRNG define a one-to-one function on the integers. Let's call such function a permutation [17]. It is known in Finite Mathematics that when $\boldsymbol{p}$ is a prime number, $\boldsymbol{x^2 \bmod p}$ has some interesting properties. Numbers which are produced by this way are called quadratic residues. The quadratic residues are computed in C using expression (3). In particular, the quadratic residue of x is unique as long as $\boldsymbol{2x < p}$.

For example, when $\boldsymbol{p}$ =11, the quadratic residues of 0, 1, 2, 3, 4, 5 are all unique (0, 1, 4, 9, 5, 3) (see Fig. 2).The remaining integers are fitted perfectly into the remaining numbers using expression (4). This only works for prime $\boldsymbol{p}$, so new output numbers of 6, 7, 8, 9, and 10 are all unique (8, 6, 2, 7, 10) (see Fig. 3) [17].

$$x * x \% p \qquad (3)$$

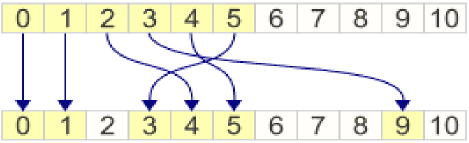

Fig. 2. Quadratic residues of 0, 1, 2, 3, 4, 5 [17]

$$p - x * x \% p \qquad (4)$$

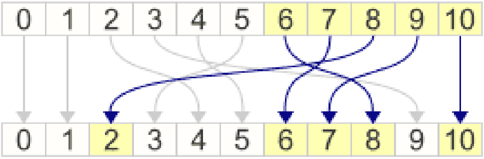

Fig. 3. Quadratic residues of 6, 7, 8, 9, and 10 [17]

The pseudo code of the proposed method is as follows:

Embedding Algorithm:

Input: Cover Image C, Secret Message M, Permutation P

Output: Stego Image S.

Steps:

1. Split the Cover Image C into three layers Red (R), Green (G), Blue (B).
2. Convert B, and G into blocks; B= $\{b_1, b_2, b_3 ... b_n\}$, G= $\{g_1, g_2, g_3 ... g_n\}$ where each block is only one pixel.
3. Convert each block from B, and G to its ASCII format.
4. Split M into characters, M= $\{m_1, m_2, m_3 ... m_n\}$.
5. Take m_i from M, and Convert it to its binary format.
6. Declare an array X of integer numbers.
7. For i =1 to length (X)
8. Generate RN (i) using PRNG generator by applying the equation 3, and 4. Each number of these random numbers will represent the location of the pixels in C.
9. End for
10. Select 8 numbers from RN (i) which located between {1 to 8}, put these numbers in another array called SN.
11. for q=1 to length (M)*3
12. RS(q)=SN(i)+8
13. End for
14. For msgCount=1 to length(M)
15. j=1
16. Take b_i from B, and g_i from G.
17. b(RS(j),7:8)= m_i(msgCount ,1:2)
18. g(RS(j),end)= m_i(msgCount,3)
19. j++
20. b(RS(j),7:8)= m_i(msgCount ,4:5)
21. j++
22. b(RS(j),7:8)= m_i(msgCount ,6:7)
23. g(RS(j),end)= m_i(msgCount,8)
24. j++
25. end for
26. Convert b, and g from binary to decimal.
27. Merge the three layers R, G, B again to construct the stego Image S.

Example:

Suppose that the secret message "**abc**" needs to hide in cover image (Lena 128.bmp). According to the proposed method, the message characters are converted into its binary format **01100001, 01100010, 01100011**, and then the Blue and Green channels are considered and its pixels are converted into binary format. Each byte from the message will be hidden in three pixels only. Based on the proposed method, it needs to generate nine random numbers to hide the message (message length * number of pixels). By using the PRNG generator, these random numbers are **RS= {1, 4, 5, 3, 8, 6, 2, 7, 9}**. Therefore, the first byte of the message will be hidden in pixel 1, pixel 4, and pixel 5(i.e., not sequential). Table I shows the embedding process.

TABLE I. RANDOM BASED IMAGE STEGANOGRAPHY EXAMPLE

Pixel no. in sequence manner	Pixels before embedding				Pixels after embedding	
	Blue pixel	Green pixel	Blue pixel bits	Green pixel bits	Blue pixel bits	Green pixel bits
1	131	137	10000011	10001001	10000001	10001001
2	120	135	01111000	10000111	01111001	10000111
3	106	132	01101010	10000100	01101001	10000101
4	113	131	01110001	10000011	01110000	10000011
5	109	129	01101101	10000001	01101100	10000001
6	111	131	01101111	10000011	01101101	10000010
7	103	127	01100111	01111111	01100100	01111111
8	112	133	01110000	10000101	01110000	10000101
9	108	122	01101100	10000100	01101101	10000101

IV. THE PERFORMANCE EVALUATION

In this section, the proposed method has been tested by taking different messages with different lengths and hiding them in some RGB cover images (i.e., standard images). The proposed method is implemented using MATLAB 11.1.0 software running on a personal computer with a 2.27 GHz Intel (R) Core (TM) I3 CPU , 4 GB RAM and windows 7 as the operating system.

Several experiments with 512 x 512 and 256 x 256 standard images are performed to evaluate the proposed method. Embedding capacity and stego image's visual quality (PSNR) are used to evaluate the performance of the proposed image steganography method. The results of these experiments are recorded and are summarized in the following tables.

The results in Table II explain that, the proposed method is tested using many images with different capacity, it produces high PSNR and the stego images appears approximately as the cover image that is explained in the MSE. Fig. 4 shows the cover image Lena 512 x 512 and the histograms of its B, and G layers which are used to embed the message given in Table II with capacity (21.845) bytes. Fig. 5 shows the stego image which is obtained after embedding that message and its corresponding histograms.

TABLE II. PSNR AND MSE OF OUR PROPOSED METHOD IN DIFFERENT COVER IMAGES AND DIFFERENT CAPACITY

Cover Image (512 x 512)	Message capacity (bytes)	PSNR of our proposed method (dB)	MSE
Lena	43.690	51.8283	0.4268
	32.768	53.0805	0.3199
	21.845	54.8254	0.2141
Baboon	43.690	51.8436	0.4253
	32.768	53.1012	0.3184
	21.845	54.8664	0.2120
Pepper	43.690	51.8544	0.4243
	32.768	53.1094	0.3178
	21.845	54.8864	0.2111
Bird	65.536	50.0949	0.6362
	43.690	51.8738	0.4224
	32.768	53.1370	0.3158
	21.845	54.8800	0.2114

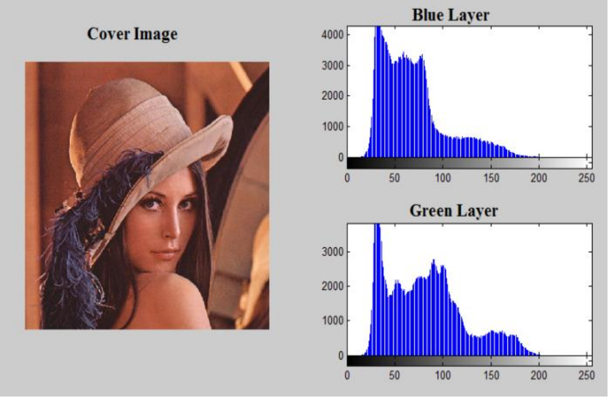

Fig. 4. Cover image Lena and histograms

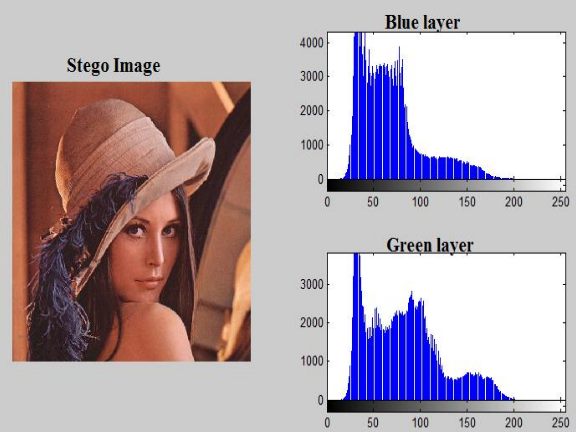

Fig. 5. Stego image Lena and histogram

The results of the comparison study between the proposed method and method in [11] by using different number of characters (bytes) secret message and 512 x 512 cover images (Lena, Baboon, Pepper) are presented in Table III.

TABLE IV. COMPARISON BETWEEN PSNR OF METHOD IN [11] AND OUR PROPOSED METHOD

	Cover Images	**Message Capacity (bytes)**	**PSNR (dB)**	
			Method in [11]	**Proposed method**
512 x 512	Lena	75.836	49.1564	49.4263
	Baboon	82.407	47.7283	49.0871
	Pepper	75.579	47.4422	49.4602

According to the comparison results, it has found that the proposed method has PSNR values better than the method in [11], which mean that the stego image quality of the proposed method will be higher than the stego image quality of the method in [11]. In addition, the average improvement of method in [11] is 48.1089 %, while the average improvement of the proposed method is 49.3245 %. So the proposed method outperforms the method in [11] by 1.22 %. Table IV represents the comparative results of our proposed method and method in [18] using different number of characters bytes (secret message), and 512 x 512 cover images (Lena, Baboon, Airplane).

TABLE V. COMPARISON BETWEEN PSNR OF METHOD IN [18] AND OUR PROPOSED METHOD

	Cover Images	**Message Capacity (bytes)**	**PSNR (dB)**	
			Method in [18]	**Proposed method**
512 x 512	Lena	28.672	43.335	53.6535
	Baboon	28.672	44.902	53.6796
	Airplaine	28.672	43.026	53.7138

According to the comparative results, it is found that our proposed method has more PSNR values than that the method in [18], which means that the stego image quality of our proposed method will be higher. In addition, the average improvement of method in [18] is 43.7543 %, while the average improvement of the proposed method is 53.692 %. So the proposed method outperforms the method in [18] by 9.93 %.

Table V represents the comparison of the proposed method and the method in [19] by hiding (145,787 - 144,916 - 145,995) secret bits in 512 x 512 cover images (Lena, Baboon, Pepper) respectively.

TABLE VI. COMPARISON BETWEEN PSNR OF METHOD IN [19] AND OUR PROPOSED METHOD

	Cover Images	**Message Capacity (bits)**	**PSNR (dB)**	
			Method in [19]	**Proposed method**
512 x 512	Lena	145.787	42.26	55.6199
	Baboon	144.916	38.44	55.6750
	Pepper	145.995	42.28	55.6657

According to the results in TABLE V, it is found that the proposed method has more PSNR values than method in [19], which means that the stego image quality of the proposed method is higher than the stego image quality of this method. In addition, the average improvement of method in [19] is 40.993 %, while the average improvement of the proposed method is 55.6535%. So the proposed method outperforms the method in [19] by 14.66 %.

V. CONCLUSION AND FUTURE WORK

In this paper, a new Steganographic method has proposed, which provides high embedding capacity and PSNR. In addition, by using Pseudo Random Number Generator (PRNG), the security of the system has improved. Experimental results showed that our proposed method is considered an effective Steganographic method while it satisfies the Steganographic system goals.

In the future work, we are looking forward to try applying the proposed method on audio and video. Also, we are looking forward to enhance the proposed method to make the capacity higher than it while keeping the same PSNR or higher.

REFERENCES

[1] A. A. Ali and A. H. Seddik, "Image Steganography Technique By Using Braille Method of Blind People (LSBraille)", International Journal of Image Processing (IJIP), Vol. 7, Issue 1,PP. 81-89, 2013.

[2] A. Ahmed, N. Agrawal, and S. Banerjee, "Image steganography by closest pixel-pair mapping", IEEE- International Conference On Computing, Communications and Informatics (ICACCI), PP. 1971 - 1975, 24-27 Sept. 2014.

[3] A. Nag, S. Ghosh, S. Biswas, D. Sakar, and P.P. Sakar, "An Image Steganography Technique using X-Box Mapping", IEEE- International Conference On Advances In Engineering, Science and Management(ICAESM-2012), Vol. 3, Issue 12, PP. 709-713, March 2012.

[4] A. A. Ali and A. H. Seddik, "New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM)", International Journal of Computer Science Engineering and Information Technology Research (IJCSITR), Vol. 3, Issue 2 ,PP. 1-10, Jun 2013.

[5] S. Nazari, A-M. Eftekhari, and M. Sh. Moin, "Secure Information Transmission using Steganography and Morphological Associative Memory", International Journal of Computer Applications, Vol. 61, No. 7, PP. 23-29, January 2013.

[6] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method with Adaptive Number of Least Significant Bits Modification Based on Private Stego-Key", International Journal of Computer Science and Security, Vol. 4, Issue 1, PP. 40-94, March 2010.

[7] S. Sharda and S. Budhiraja, "Image Steganography: A Review", International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol.4, Issue 1, PP. 707-710, January 2013.

[8] A. A. Ali and A. H. Seddik, "New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM)", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 3, Issue 2, PP. 1-10, Jun 2013.

[9] M. E. Saleh, A. A. Ali, and F. A. Omara, "Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding", International Journal of Computer Science and Security (IJCSS), Vol. 9, Issue 2, PP. 96-107, 2015.

[10] A. Almohammad, "Steganography-based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility", Doctor of Philosophy Thesis, Department of Information System and Computing, Brunel University, August 2010.

[11] M. M. Emam, A. A. Ali, and F. A. Omara, "A Modified Image Steganography Method based on LSB Technique", International Journal of Computer Applications (IJCA), Vol. 125, No. 5, PP. 12-17, 2015.

[12] R. Amirtharajan, R. subrahmanyam, J. N. Teja, K. M. Reddy, and J. B. B. Rayappan, “Pixel Indicated Triple Layer: A Way for Random Image Steganography ”, Research Journal of Information Technology, Vol. 5, Issue 2,PP. 87-99, 2013.

[13] V. Madhu Viswanatham and J. Manikonda, “A Novel Technique for Embedding Data in Spatial Domain”, International Journal on Computer Science and Engineering, IJCSE, vol. 2, PP. 233-236 , (2010).

[14] A. Gutub, A. A. Qahtani, and A. Tabakh, “Triple-A: Secure RGB Image Steganography Based on Randamization”, IEEE, International Conference on Computer System and Application, PP. 400-403, 2009.

[15] A. I. Abdul-Sada," Hiding Data Using LSB-3", J.Basrah Researches (Sciences), Vol. 33, No.4, PP. 81-88, DEC 2007.

[16] J. J. Roque and J. M. Minguet, "SLSB: Improving the Steganographic Algorithm LSB", WOSIS, PP. 57-66. INSTICC Press, 2009.

[17] Jeff Preshing, (December 24, 2012), "How to Generate a Sequence of Unique Random Integers", [Online]. Available: http://preshing.com/20121224/how-to-generate-a-sequence-of-unique-random-integers/.

[18] U. Lokhande, and A. K. Gulve, “Steganography using Cryptography and Pseudo Random Numbers ”, Internatioal Journal of Computer Applications, Vol. 96, No. 19, PP. 40-45, June 2014.

[19] J. K. Mandal and D. Das, “ Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain ”, International Journal of Information Sciences and Techniques (IJIST), Vol. 2, No. 4, PP-83-93, July 2012.