A LSB Based Image Steganography Using Random Pixel and Bit Selection for High Payload

U. A. Md. Ehsan Ali

Department of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur-5200, Bangladesh
E-mail: ehsan_cse@hstu.ac.bd

Emran Ali, Md. Sohrawordi and Md. Nahid Sultan

Department of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur-5200, Bangladesh
E-mail: emran.cse@hstu.ac.bd, mdsohrawordicse@gmail.com, nahid.sultan@hstu.ac.bd

Abstract: Security in digital communication is becoming more important as the number of systems is connected to the internet day by day. It is necessary to protect secret message during transmission over insecure channels of the internet. Thus, data security becomes an important research issue. Steganography is a technique that embeds secret information into a carrier such as images, audio files, text files, and video files so that it cannot be observed. In this paper, based on spatial domain, a new image steganography method is proposed to ensure the privacy of the digital data during transmission over the internet. In this method, least significant bit substitution is proposed where the information embedded in the random bit position of a random pixel location of the cover image using Pseudo Random Number Generator (PRNG). The proposed method used a 3-3-2 approach to hide a byte in a pixel of a 24 bit color image. The method uses Pseudo Random Number Generator (PRNG) in two different stages of embedding process. The first one is used to select random pixels and the second PRNG is used select random bit position into the R, G and B values of a pixel to embed one byte of information. Due to this randomization, the security of the system is expected to increase and the method achieves a very high maximum hiding capacity which signifies the importance of the proposed method.

Index Terms: Steganography, LSB substitution, data hiding, embedded message, retrieved message, PRNG

1. Introduction

In the rise of the information age with the Internet and multimedia techniques, various digital data such as texts, images, videos and audios now have been widely used in our daily life. Human lives become more convenient through sharing information with others. Although people can transfer huge information via computer networks, an illegal user can grasp or intercept the transmitted data due to the insufficient security of these computer networks. Therefore, for effective, safe and secured communication via the Internet is an essential issue [1, 2]. Steganography is a technique to hide messages inside other harmless messages in a way that does not allow any unauthorized person to even detect that there is a second message present. Both steganography and cryptography are used to protect important information. But in steganography, the message is kept hidden from an unauthorized third party rather than being unfathomable to the third party, as is the case with cryptography [3], that is, in steganography it appears that no information is hidden at all. In short, steganography is one such technique where existence of secret messages cannot be noticed, and it can be used as a tool to transmit the confidential information in a secure and protected way [4].

Due to the easiest distribution, digital images can be found almost in every page on the Internet. For this reason, researches on steganography and developed methods are mainly in the context of image steganography. It is possible to hide any digital data inside an image file. In image steganography, hiding a secret information include two files [5]. The first file, called the cover image, is the image file which is used to hide the secret information as a payload. The second file is the payload or the message to be hidden such as plain text, cipher text, other images or bitmaps, etc. The procedure or algorithm that is used to hide the message to the cover image is called the embedding technique. As the result of the embedding process, the resultant image file is called "stego image". The counter part of embedding is called extraction technique which is used to recover the message from the stego image. There are two different methods for image steganography:

1. Spatial / Image Domain Technique
2. Frequency / Transform Domain Technique

In Spatial Domain or Image Domain, the pixels of the cover image are directly changed in embedding process [6, 7]. In spatial domain technique, Least Significant Bit (LSB) substitution method is the most commonly used. In Frequency Domain or Transform Domain, embedding the secret data take place after the cover image is transformed in frequency domain from spatial domain and after hiding, the image file is again transformed into spatial domain. An example of the Transform Domain technique is the discrete wavelet transform (DWT) implementation that use the wavelet coefficients of the cover image are modified to embed the secret message.

In image steganography, the size of the message is always been a key factor. In case of spatial domain techniques, there is tradeoff between the size of the message and changes in the original image. If a sender want to send a message other than text such as audio and image inside of another image using steganography, then a proper method is needed to embed the required huge information considering the above mentioned trade off. This paper provides a robust and secure LSB substitution based method using Pseudo Random Number Generator (PRNG) that can hide a large volume of data. Comparing with the other methods [14, 15] for embedding high capacity data using similar approach such as PRNG or Hash function, the proposed method produces good and encouraging results. In the next section, the literature survey of the similar steganographic techniques is discussed. Implementation of the proposed method is explained in section 4 and the performance of the proposed method is analyzed in section 5 with the conclusion in section 6.

2. Related Work

The main goal of the steganography process is to hide the original message in some container data in some way so that the message be kept secret within the container with minimally distorting or replacing the content the container data with the original message. To keep the message highly secret and difficult to break from the intruders and making the process faster are the main goals [8, 9]. To do so, different complex algorithms are used to embed the message into the container data.

One of the simplest steganography techniques to hide the secret message directly into the spatial domain by modifying the least significant bits (LSB) plane of the container data medium usually a cover-image [10]. The benefits of spatial domain data hiding techniques are high clearness of understanding, efficiency, and data hiding capacity with minimum effort.

Several LSB substitution techniques are well known and already proposed by different authors. Rather than using simple LSB technique as being relatively easy to reconstruct the message from the medium, modified methods of LSB technique is used mostly. As the authors in [11] proposed a method of doing random LSB substitution of 3 bits per pixel (1 bit per pixel value e.g. Red, Green and Blue) can be hidden. In this approach the secret message bit is hidden in the random bit position of the pixel value (e.g. Red, Green and Blue) and hides the reference in the least significant bit (LSB) position of the respective pixel value. To improve and increase the capacity of the message to be hidden, the authors in [12] have proposed a hash based 2-3-3 method where 8 bits of message can be embedded to a single pixel (simply character per pixel). As the name suggested, in this approach, first 2 bits of the message replaces any 2 bits out of the least significant nibble (LSN) of the Red value of that pixel. Similarly second 3 bits replaces 3 bits of the LSN of the Green value, and last 3 bits message replaces 3 bits of LSN of Blue value of the corresponding pixel. In this case the bit selection is done randomly with the help of a hash function. Although this method performs well in terms of increased capacity of the message, but they did not provide any clear solution of collision problem in hash function.

Later on considering the nature of human vision system and sensitivity of light [13], some other methods were proposed in [14] called 4-4-4 and 3-3-2 methods. In first one, authors proposed the method for the situation where high capacity data transfer is more considerable than the security. But the 3-3-2 method was based on the logic of [12] considering the quality of the image except they choose to replace the data bits in 3-3-2 fashion without randomness or use of hashing which make it less secure.

For the simplicity of the rules in [12] and [14], the authors of [15] proposed another method, the improved 3-3-2 to increase the security with more complex rule. This method is mainly a combination of two other methods, literally be called as the 2-1-1 which is used to hide the upper nibble of the message and the 1-2-1 is used to hide the lower nibble. The bit selection from the pixel values for these methods are sequential and similar to the method explained before except the authors used their own method to transform the message bits. With the combination of two method, it become too complex.

In [16], Pseudo Random Number Generator (PRNG) is used to randomly select pixels in the cover image for hiding each byte of the message in three pixels. Peak signal-to-noise ratio (PSNR) indicated in this paper shows good hiding capacity with higher visual quality. Since the method use three pixels for a single byte, it will not be able to hide other multimedia messages such as image and audio due to the low hiding capacity compared to the other methods.

Up to this point considering the capacity and the security of the message, a novel technique is proposed where each character is embedded in a pixel to increase the capacity of the message and random pixel is selected for each character to enhance the security.

3. Research Methodology

Based on the cover media, steganography can be divided into five categories which include image steganography, audio steganography, video steganography, text steganography and network steganography. In Image Steganography, the hiding of secret message is done by taking an image as the cover object. In this process, the pixel intensities of the cover image are used to hide the secret data. There are many techniques to embed information in the cover image including LSB Substitution, Pseudorandom Technique, Distortion Technique, Singular value Decomposition, Discrete Fourier Transformation Technique(DFT), Discrete Cosine Transformation Technique(DCT), Discrete Wavelet Transformation Technique(DWT) etc. which can be classified mainly into spatial domain and transform domain Techniques.

The general steganographic system is showed in Figure 1. Using a proper method with a stego key in embedding system the secret information is implanted into the cover image. The stego image is then transferred over the communication channel to the receiving end where the message is extracted from the stego image using the used method and the stego key.
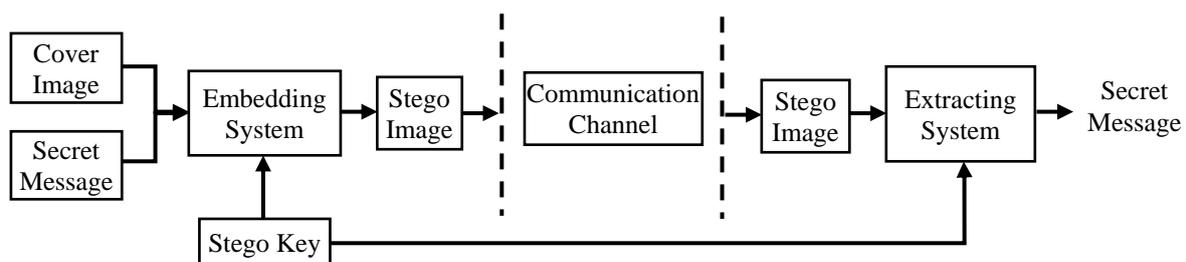

Fig. 1. General Image steganographic system for hiding information.

There are two important requirements that are essential for hiding process and researchers take care about in image based steganography. Firstly, a steganography technique is able to hide secret message bits in an image in such a way that that human eye cannot distinguish between the original image and the stego- image, in other words the secret message is imperceptible. Secondly, the technique should be able to insert high amount of secret data in the cover image without hampering the imperceptibility. The relationship between these two requirements should be balanced, for e.g. if we increase the capacity more than a specified threshold value then the Imperceptibility will be affected and so on, therefore the parameters of digital steganography technique should be chosen very carefully.

4. Proposed Method

To establish a secure transfer of an image with high capacity message embedded in it, the proposed method used a 3-3-2 approach to hide a byte in a pixel of a 24 bit color image. That means, the size of the message can be reach up to 33.33% of the size of cover image. A color picture of 512×512 resolution may contain 1 byte of message for each pixel. Meaning that $512 \times 512 = 262144$ pixels, which means there will be maximum 262144 bytes of information or characters can be hidden to that image. For the security of the secret message the proposed method uses Pseudo Random Number Generator (PRNG) in two different stages of embedding process. The method of message embedding is explained with the following procedure:

1. Choose a pixel randomly from the cover image to embed the message byte using non-repeating PRNG.
2. Separate message byte in 3 groups of the form 3-3-2 to embed in the RGB values of that pixel.
3. To embed 1st group to the Red value:
    (a) Choose a bit randomly from 5 most significant bits using PRNG.
    (b) XOR the selected bit with the 1st bit of the group and substitute the result in 3rd LSB.
    (c) Repeat (a) and (b) to embed 2nd and 3rd bits of the group in 2nd and 1st LSB respectively.
4. Repeat step 3 to embed 2nd group to the Green value.
5. To embed 3rd group to the Blue value:
    (a) Choose a bit randomly from 5 most significant bits using PRNG.
    (b) XOR the selected bit with the 1st bit of the group and substitute the result in 2nd LSB.
    (c) Repeat (a) and (b) to embed 2nd bit of the group in 1st LSB.
6. Repeat steps from 1 to 5 to embed all message bytes.

As it can be seen from the above procedure that, two PRNG is used to hide the secret message. The first one is used to select the pixels in random order to hide the message bytes. In this case the PSNR should follow a non-repeating

approach that means there is no repetition of same pixel in the selection order. Hence, every pixel in the image can be used to hide one byte of information. Fig. 2 shows 3 randomly chosen pixels of a 10×10 image.
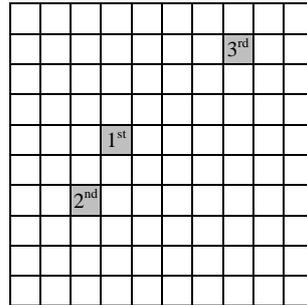

Fig. 2. Randomize selection of pixels for hiding information.

For 24-bit color images, every pixels are composed of 3 prime colors (R, G, B) of 8-bit each. The second PRNG is used to embed one byte of information into the R, G and B values of a pixel. Hence, the message byte is divided in 3, 3 and 2 bits to form 3 different groups for the R, G and B values of a pixel respectively. To embed 1st bit of the 1st group in Red value, the PRNG chooses a random bit from 5 MSB of that Red value. Then an Exclusive-OR operation is performed on randomly selected bit and chosen message bit and the result is substituted in 3rd LSB of Red value. This process is used to transform and embed the 2nd and 3rd message bit of the 1st group to 2nd and 1st LSB of Red value.
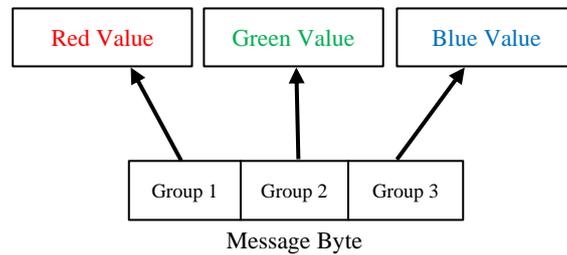

Fig. 3. Byte of message to embed in each pixel (Red, Green, Blue).

The similar approach is followed to embed the 3 bits of 2nd group in Green value and 2 bits of 3rd group in Blue value of the pixel. But in the case of 3rd group, 2 LSB of Blue value is used.
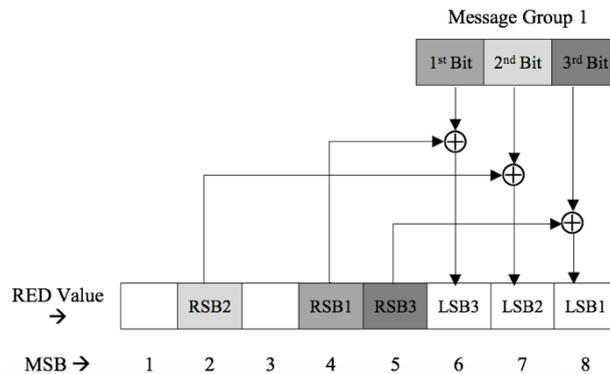

Fig. 4. Embedding process of message group 1 (3 bits) using randomly chosen bit positions RSB1, RSB2 and RSB3 of Red value.

The encryption key of this procedure is the seed values of two PRNG and this key must be used in the decryption procedure. For example, the above procedure is used to embed 1 byte of massage that is, 01000101 to the R, G and B values of a randomly selected pixel of an image by the first PRNG. If the randomly chosen bit positions by second PRNG are 5, 1, 4 for Red value, 2, 4, 2 for Green value, and 3, 5 for Blue value. Table 1 illustrates how the encryption procedure hide the message byte in that pixel.

Table 1. Embedding of 1 byte information in a pixel

Message Group	Message Bit	Pixel value (R/G/B)	Binary pixel value with randomly chosen position from 5 MSB	XOR of message bit with randomly chosen bit	Substitute the result with different LSB position
G1	0	R	1001*1*001	$0 \oplus 1 = 1$	10011*1*01
	1	R	*1*0011001	$1 \oplus 1 = 0$	100111*0*1
	0	R	100*1*1001	$0 \oplus 1 = 1$	1001110*1*
G2	0	G	1*1*000101	$0 \oplus 1 = 1$	11000*1*01
	0	G	110*0*0101	$0 \oplus 0 = 0$	110001*0*1
	1	G	1*1*000101	$1 \oplus 1 = 0$	1100010*0*
G3	0	B	10*1*01110	$0 \oplus 1 = 1$	101011*1*0
	1	B	1010*1*110	$1 \oplus 1 = 0$	1010111*0*

The extraction procedure is simply the reverse of the embedding procedure with same seed values for the two PRNG. The following procedure explains the method of message extraction from the image:

1. Choose a pixel randomly from the cover image to extract the message byte using same non-repeating PRNG used in embedding process.
2. To extract 1st group of 3 message bits from the Red value:
    (a)   Choose a bit randomly from 5 most significant bits using same PRNG used in embedding process.
    (b)   XOR the selected bit with 3rd LSB to extract 1st bit of the group.
    (c)   Repeat (a) and (b) to extract 2nd and 3rd bits of the group using 2nd and 1st LSB respectively.
3. Repeat step 3 to extract 2nd group of 3 message bits from the Green value.
4. To extract 3rd group of 2 message bits from the Blue value:
    (a)   Choose a bit randomly from 5 most significant bits using same PRNG used in embedding process.
    (b)   XOR the selected bit with 2nd LSB to extract 1st bit of the group.
    (c)   Repeat (a) and (b) to extract 2nd bit of the group using 1st LSB.
5. Combine 3 groups to form the message byte.
6. Repeat steps from 1 to 5 to extract all message bytes.

The extraction process of the massage byte 01000101 is illustrated in Table 2. The randomly chosen bit positions by second PRNG for the same seed value are 5, 1, 4 for Red value, 2, 4, 2 for Green value, and 3, 5 for Blue value.

Table 2. Extraction of 1 byte of information from a pixel

Pixel value (R/G/B)	Binary pixel value with randomly chosen position from 5 MSB	XOR of message bit with randomly chosen bit	Message Bit	Message Group
R	1001*1*101	$1 \oplus 1 = 0$	0	
R	*1*0011101	$1 \oplus 0 = 1$	1	G1
R	100*1*1101	$1 \oplus 1 = 0$	0	
G	1*1*000101	$1 \oplus 1 = 0$	0	
G	110*0*0101	$0 \oplus 0 = 0$	0	G2
G	1*1*000100	$1 \oplus 0 = 1$	1	
B	10*1*01110	$1 \oplus 1 = 0$	0	G3
B	1010*1*110	$1 \oplus 0 = 1$	1	

From the above discussion shows that the proposed method is simple LSB substitution based method which includes two pseudorandom techniques to hide a single byte of information in a single pixel of the cover image. This two pseudorandom layers are expected to increase the imperceptibility or security of the method as well as a single byte of information in a single pixel make it possible for high amount of secret data to be inserted into the cover image.

5. Result and Discussion

In this section, the proposed method has been tested by considering a message with different lengths using the mostly available three 24-bit images (Lena, pepper and baboon) with size 512×512. The proposed method is implemented using PyCharm IDE (Python 3.7.2) running on a personal computer with a 2.7 GHz Intel Core i7 CPU, 16 GB RAM and MacOS as the operating system.

To evaluate the performance of the proposed image steganography method, Embedding capacity and stego image's visual quality (PSNR) with Mean Square Error are used. Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics are the most common measures used to determine the quality of image. MSE is to estimate the mean of the squares of the error between stego image and the original image.
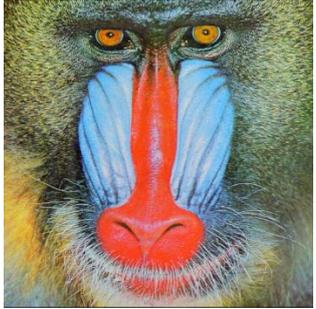
$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - X'_{ij}) \qquad (1)$$

PSNR is often used a s a quality measurement to determine the degradation in the embedding image with respect to the cover image, that is, the difference between the original and the stego image.

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

Where X_{ij} is the pixel in the original image (cover image) in i^{th} row and j^{th} column, X'_{ij} is the pixel in the stego image in i^{th} row and j^{th} column, MN is the size of the image where M is the height and N is the width and I is the range pixel value. For 8 bit images, I=255. The following table shows the results of the experiment.

Table 3. The measures of MSE, and PSNR of the proposed method for different images.

Image Size: 512×512 =262144 pixels	Image Name: Lena.bmp		Image Name: Baboon.bmp		Image Name: Peppers.bmp	
Data in Bytes	MSE	PSNR	MSE	PSNR	MSE	PSNR
100	0.002893	73.517601	0.002825	73.619975	0.002712	73.797507
1000	0.029078	63.495134	0.029092	63.493045	0.028628	63.562889
10000	0.290938	53.492798	0.294664	53.437537	0.295779	53.421132
50000	1.467086	46.466249	1.466100	46.469168	1.464748	46.473173
100000	2.933533	43.456894	2.933393	43.457101	2.937068	43.451664
150000	4.394489	41.701720	4.387656	41.708478	4.413038	41.683427
200000	5.868726	40.445365	5.862803	40.449750	5.862278	40.450140
262144	7.676342	39.279260	7.695947	39.268183	7.705682	39.262693

The results in Table 3 explain that, the proposed method produces satisfactory PSNR and the stego images appears approximately as the cover image that is explained in the MSE. Fig. 5 represent the bar chart of MSE and PSNR for Lena.bmp image with different message capacity. From the chart we can see that PSNR decreases and MSE increases with the increase of message capacity. With maximum message capacity, the MSE and PSNR is acceptable considering the security of the message.
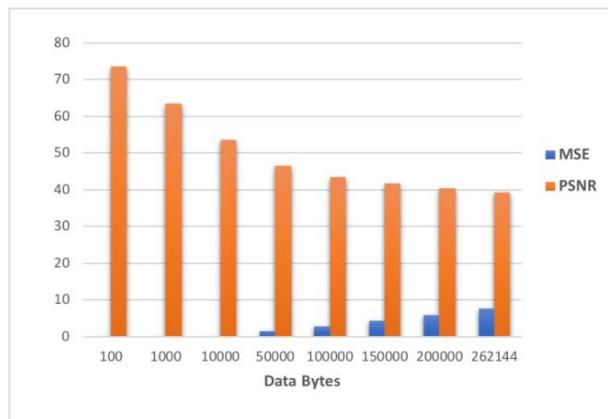

Fig. 5. The bar chart of MSE and PSNR for Lena image.

Table 4 represents the comparison of PSNR of the proposed method with the other methods which use similar approaches of pseudorandom techniques. The higher performance of the proposed method is clearly visible than the method proposed by Alam et al. [14] due to the insertion of message in helical traversal way in the cover image. It also make it predictable of the possible location of the secret message. The performance of the method, proposed by Sharma

et. al. [15], is quite similar to the proposed method, but the combination of two method make it more complex than the proposed method.

Table 4. Comparison of PSNR of the proposed method with other methods for 512×512 Lena image.

Data in Bytes	Alam et al. [14]	Sharma et. al. [15]	Proposed Method
100	71.224386	72.936582	73.517601
1000	60.684362	63.037268	63.495134
10000	52.284334	53.206538	53.492798
100000	41.969563	42.984537	43.456894

Due to the randomness in pixel and bit selection, an unauthorized person cannot retrieve the message although they detect the presence of the secret message in the image. In addition, to enhance the security of the proposed method can be enhanced by applying an encryption technique for the message. Hence, the proposed method provides a robust and secured image steganography for communication with high payload.

6. Conclusion

With the advancement of communication technology, information sharing is becoming essential part of modern life. In case of image steganography, security and capacity are the main concern of the researchers. A method with proper security and ability to hide huge amount of data in the cover image is needed for secret communication over the Internet. The proposed method of image steganography is introduced that uses Pseudo Random Number Generator for random pixel and bit selection to embed the message in the cover image to secure the message from intruder. Experimental results showed that the proposed method provide better security and high embedding capacity compared with the results of the other LSB methods. With the two layer of PRNG in pixel and bit level and a single byte in each pixel, the method provide improved security and high embedding capacity. As the method is satisfied the steganographic system goals, it can be contemplated as an effective steganographic method.

References

[1] N. Chowdhury and P. Manna, "An Efficient Method of Steganography using Matrix Approach", *Copyright © 2012 MECS I.J. Intelligent Systems and Applications*, vol. 1, pp. 32-38, 2012. (http://www.mecspress.org/) DOI: 10.5815/ijisa.2012.01.04.

[2] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", *3rd IEEE International Conference on Informatics, Electronics & Vision, Dhaka, Bangladesh*, May 23-24, 2014.

[3] M. H. Moon, A. K. M. T. I. Tanim, M. Z. Shoykot, M. N. Sultan, U. A. M. E. Ali and E. Ali, "Mapping Character Position Based Cryptographic algorithm with Numerical Conversions", *International Journal of Computer Science and Software Engineering (IJCSSE)*, vol. 9, issue 3, pp. 56-59, 2020.

[4] M. P. Uddin, M. Saha, S. J. Ferdousi, M. I. Afjal and M. A. Marjan, "Developing an Efficient Solution to Information Hiding through Text Steganography along with Cryptography", *9th IEEE International Forum on Strategic Technology, CUET, Bangladesh*, October 21-23, 2014.

[5] Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R., "A Novel Security Scheme for Secret Data using Cryptography and Steganography", *Copyright © 2012 MECS I.J. Computer Network and Information Security*, vol. 2, pp. 36-42, 2012. (http://www.mecs-press.org).

[6] P. Basak, L. Arjuman, A. M. Nitu, M. I. Afjal, M. P. Uddin, M. F. Rabbi, and M. R. Islam, "A Modified Blind Steganalysis Method Based on the Moments of Characteristic Function", *HBRP Advancement in Software Engineering and Testing*, vol 1 issue 2, pp. 1-9, 2018.

[7] S. Sultana, A. Khanam, M.R. Islam, A. M. Nitu, M. P. Uddin, M. I. Afjal, and M. F. Rabbi, "A Modified Filtering Approach of LSB Image Steganography Using Stream Builder along with AES Encryption", *HBRP Recent Trends in Information Technology and its Applications*, vol 1 issue 2, pp. 1-10, 2018.

[8] Manish Mahajan, Dr. Navdeep Kaur, "Adaptive Steganography: A survey of Recent Statistical Aware Steganography Techniques", *Copyright © 2012 MECS I.J. Computer Network and Information Security*, vol. 10, pp. 76-92, 2012. (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2012.10.08.

[9] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", Copyright © 2012 MECS I.J. Modern Education and Computer Science, 6, pp27-34, 2012. (http://www.mecs-press.org/) DOI: 10.5815/ijmecs.2012.06.04.

[10] S. M. M. Karim, M. S. Rahman and M. I. Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", *Proceedings of 14th IEEE International Conference on Computer and Information Technology*, pp. 286 – 291, 2011.

[11] U. A. M. E. Ali, M. Sohrawordi and M. P. Uddin, "A Robust and Secured Image Steganography using LSB and Random Bit Substitution", American Journal of Engineering Research (AJER), vol. 8, issue 2, pp. 39-44, 2019.

[12] G. R. Manjula and A. Danti, "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 4, issue 1, pp. 11-20, 2015.

[13] B. Zaidan, A. A. Zaidan, and F. Othman, "Quality of Image vs. Quantity of Data Hidden in the Image", International Conference Image Processing, Computer Vision and Pattern Recognition, pp. 343-347, 2009.

[14] S. Alam, S. M. Zakariya and N. Akhtar, "Analysis of Modified Triple-A Steganography Technique using Fisher Yates Algorithm", 14th International Conference on Hybrid Intelligent Systems, Kuwait, 2014.

[15] H. Sharma, S. Chauhan and K. Sharma, "Improved Spatial Domain Image Steganography using LSB & MSB", International Journal of Innovative Research in Science, Engineering and Technology, vol. 4, issue 10, pp. 10001-10007, 2015.

[16] M. M. Emam, A. A. Aly and F. A. Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", *International Journal of Advanced Computer Science and Applications*, vol. 7, issue 3, pp. 361-366, 2016.

Authors' Profiles

U. A. Md. Ehasn Ali received his B. Sc. degree in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh in 2013. Now, he is pursuing M. Sc. degree in Computer Science and Engineering from Rajshahi University of Engineering & Technology (RUET), Rajshahi, Bangladesh. His main working interest is based on Image Processing, Expanding the Applications of Artificial Intelligence, Machine Learning, Data Mining, Data Security etc. Currently, he is working as an Assistant Professor in Dept. of Computer Science and Engineering in Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh. He has several scientific research publications in various aspects of Computer Science and Engineering.

Emran Ali received the Bachelor of Science in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh in the year of 2010. From February 2012 to August 2014 he worked on Software and Application development for Smartphone in various software firms in the country. In September 2014, he joined as an Assistant Professor in the department of Computer Science and Engineering, HSTU, Dinajpur-5200, Bangladesh. His research interest includes Information Security and Cryptanalysis, Artificial Intelligence, Image Processing and Bio-informatics.

Md. Shohrawordi is working as an Assistant Professor in Dept. of Computer Science and Engineering in Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh. He received his B. Sc. degree in Computer Science and Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh in 2013. Now, he is pursuing M. Sc. degree in Computer Science and Engineering from Rajshahi University of Engineering & Technology (RUET), Rajshahi, Bangladesh. His main working interest is based on Image Processing, Artificial Intelligence, Data Mining, Mobile Networks, cryptography etc. He has several scientific research publications in various aspects of Computer Science and Engineering.

Nahid Sultan received the Bachelor of Science in Computer Science and Engineering from Islamic University (IU), kushtia-7003, Bangladesh in the year of 2011. He received M.Sc. in Computer Science and Engineering from Islamic University (IU), kushtia-7003, Bangladesh in the year of 2012. From February 2015 to September 2015 he worked on a Private University name UITS as a Lecturer in the country. In September 2015, he joined as a Lecturer in the department of Computer Science and Engineering, HSTU, Dinajpur-5200, Bangladesh. Then, he became an Assistant Professor in September 2017. His research interest includes Artificial Intelligence, Machine Learning, Cognitive Radio Network, Image Processing, Bio-informatics, and Internet of Things.