International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Impact of Message Size on Least Significant Bit and Chaotic Logistic Mapping Steganographic Technique

Tokey Ahmmed[1], Ipshita Tasnim Raha[1], Faizah Safwat[2], Nakib Aman Turzo[1]

[1]Lecturer,
[1,2]Department of Computer Science & Engineering, Varendra University, Rajshahi, Bangladesh

ABSTRACT

Steganography is the technique of hiding information in other objects. Although many carrier objects can be used, digital images are the most popular because of their usage over the internet. For this purpose, many types of images steganographic techniques have been invented. Each of them has both pros and cons. It depends on the complexity, hiding capacity, security, and so on. In our research, we studied the two most popular techniques of image steganography, least significant bit (LSB) and chaotic logistic mapping to find the similarities, dissimilarities, and many other factors. In this paper, we presented a detailed comparison of the LSB and chaotic logistic mapping-based image steganography for various carrier images and messages.

KEYWORDS: *image steganography, cover image, various steganographic technique, hidden message, invisible communication, communicated message, steganography overview, multimedia content, least significant bit (LSB), chaotic logistic mapping (chaotic LM).*

How to cite this paper*:* Tokey Ahmmed | Ipshita Tasnim Raha | Faizah Safwat | Nakib Aman Turzo "Impact of Message Size on Least Significant Bit and Chaotic Logistic Mapping Steganographic Technique" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.1100-1104, URL: www.ijtsrd.com/papers/ijtsrd42494.pdf

IJTSRD42494

INTRODUCTION:

Security of information is one of the most important factors of information and communication technology. Cryptography is associated with the process of securing secret communication in presence of adversaries to maintain information security such as data confidentiality, data integrity, authentication etc.

But the cryptography method is not suitable for hiding information where the user wants to avoid unwanted attention. This is where the steganography comes in to the role.

It is an important branch of information hiding. In the present year steganography is gaining attraction because sometimes hiding the contents of a message for secrecy might not be enough. it may also be necessary to hide the existence of the secret message due to the security issues over the internet.

cryptography and Steganography differ in the sense that where cryptography keeps the contents of a message secret, steganography focuses on keeping the presence of a message secret [1].

Steganography is best known for the techniques of hiding messages or information. The main benefit of this is, it also hides the existence of the communication which cannot be recognized by human vision. Such techniques are accomplished in a way that secret contents are hidden in a carrier file like image for hiding its presence without a distortion in a carrier. Hence covering up the presence of the communicated message or information.

Depending on the nature of the hidden information (embedded information), steganography can be divided mainly into four types: Text Steganography. Image Steganography, Video Steganography, Audio Steganography [2]

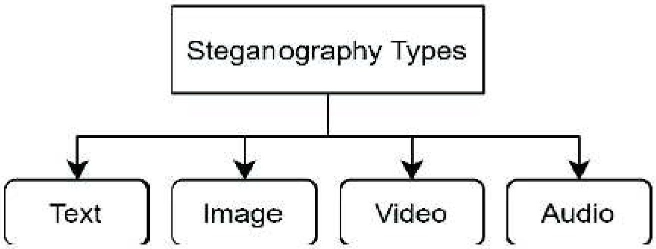


Fig 1: Types of Steganography

But we will mainly focus on the various techniques of image Steganography. As the name suggests, Image Steganography is a process of hiding secret message within an image file.

Steganography has recently become an important image working tool because it provides a powerful security, especially when it is joined with digital images due to the inability of the human eye to focus on the sensitive details of photos. A little change in the steganography of an image has no tangible effect on the image. So, image steganography can be used to hide unnatural secret messages within a carrier image, so the carrier image quality will have a small change, thus unrecognizable by human vision.

Image steganography techniques are classified in two prime kinds, spatial domain and frequency domain (transform)

Image Steganography model consists of a secret message, cover image, stego message, secret key and embedding algorithm.

Cover Image (C): It is the carrier of secret message that acts as a medium in which any secret message is embedded. As a result, the existence of the sent secret message stays hidden. Some embedding algorithms are used to embed/hide the secret message into the cover.

Stego Image (S): the image obtained after steganography is called the stego image. Stego image must not distort cover image quality. So maintaining the stego image quality is important.

Secret Key (K): it is used to encode/decode the embedded secret message.

Secret Message (M): A secret message can be any kind of data, like, text or image etc., It is covered within cover image. [3]

Steganography process basically consists of encoding at the sender end to obtain the Stego-Image and decoding at the receiver end to provide the secret or private information. the secret message is encrypted using an encryption key in encoding step. On the other hand, the decoder uses a decryption algorithm on the received stego image to decrypt it and provide output in decoding step.

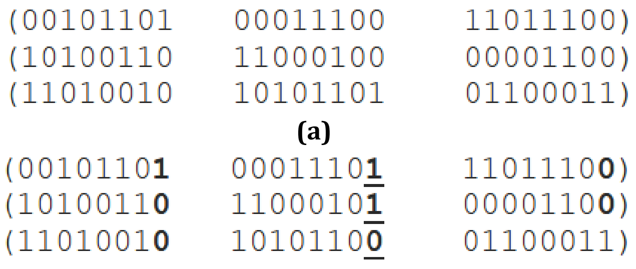
While there are several image steganography techniques, we will be focusing on the 2 most common technique LSB and Logistic Mapping.

LSB is one of the most well-known algorithms in this field. It is also very efficient algorithm used to embed the information in a cover file. This is method for embedding data into cover image. The least significant bit of each pixel of an image is altered to a bit of a message that is to be hidden [2]. The change is undetectable by the human eye but still can be recognized by some statistical tests [7].

In a simple Least significant bit (LSB) insertion method information bits are embedded in [14] in the least significant bit (in other word, the 8th bit) of a cover image. In this case some or all of the bytes inside an image is changed to a bit of the secret message. This method can be used in both grayscale or RGB colored image. When using a 24-bit image RGB image, a bit of each of the red, green and blue components can be used for the LSB bit. In that case, one can store 3 bits in each pixel.

An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [1].

The given figure shows the pixel values of RGB cover image. After embedding a secret data 200 in a binary form which is 11001000, into the least significant bits of the image, the stego image became this:



```
(00101101   00011100   11011100)
(10100110   11000100   00001100)
(11010010   10101101   01100011)
```

(a)

```
(00101101   00011101   11011100)
(10100110   11000101   00001100)
(11010010   10101100   01100011)
```

(b)

Fig 2: (a) Pixel values of RGB cover image (b) Pixel values after embedding secret data using LSB algorithm.

Logistic map is also one of the well-known techniques which used in many data hiding methods. In image steganography the popularity of this technique increased because of its chaotic nature. This technique is very simple and fast. Mathematically, the logistic map can be written as [8],

$$f(x) = rx(1-x)$$

$$x_{n+1} = f(x_n)$$

Though it is simple and fast but the downfall is it has short key space [5]. The main purpose of using chaotic logistic mapping is sensitivity to initial conditions and very small changes in the input can cause large changes in the output [5].

LITERATURE REVIEW

In paper written by K.Thangadurai and G.Sudha Devi used various types of LSB techniques in spatial domain. The LSB method is widely used for its simplicity in image steganography. In this approach, the least significant bit (LSB) value of each pixel is exploited. The paper also shows the operations involving the replacement of pixel's LSB value of cover image. The method may achieve high capacity, but still susceptible to sensitive image manipulation such as compression and cropping of images.[2]

In 2018 Mohammed Mahdi Hashim, Mohd Shafry Mohd Rahim, Fadil Abass Johi, Mustafa Sabah Taha and Hassan Salman Hamad published a paper [3] which evaluated the performance of LSB based image steganography on various formats such as BMP, GIF, PNG and JPEG. Based on the reading, the JEPG format tends to have a balanced result considering both security and payload capacity. Whereas, GIF and PNG both were moderate in payload capacity but performed low in security. On the other hand, BMP file image had a high payload capacity but still showed low security performance.[3]

Another significant effort made By Stuti Goel, Arun Rana & Manpreet Kaur in the year 2013, they compared few image steganography techniques in both spatial and frequency domain. A comparison of least significant bit (LSB), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) based steganography has been shown. Where LSB is implement in spatial domain and DCT, DWT was implemented in frequency domain. The payload capacity of LSB in this paper was also high comparing to the DCT, DWT. The invisibility of LSB was low, whereas it was high in both DCT, DWT. The PSNR and MSE value was found average in LSB, meaning there was medium distortion of the stego-image.[4]

In 2017 Milad Yousefi Valandar, Peyman Ayubi, Milad Jafari Barani proposed a new transformation domain steganography on chaotic based logistic mapping. The experiment showed high capability of hiding information in any type of images. In this technique they used integer wavelet transformation before embedding the message into the cover image. After that an inverse integer wavelet transformation has been done to get the stego-image. Based on the result the proposed technique was claimed to be better than previous algorithm.[5]

METHOLODOGY

In this method we compared LSB and chaotic logistic mapping technique for image steganography. The comparison was based on the image invisibility (using MSE, SNR, PSNR) and embedding time of the techniques. As cover image for our work, we have used data 3 popular images (Peppers, Tulips, Baboon). The details are given below –

Table I: Property of selected images

Property	Peppers	Tulips	Baboon
Format	PNG	PNG	PNG
Dimensions	512 x 512	768 x 512	512 x 512
Width	512	768	512
Height	512	512	512
Size	527	664	623
Horizontal resolution	350	350	350
Vertical resolution	350	350	350
Bit depth	24	24	24

As the secret message we have used 2 strings of alphanumeric characters. For the first experiment 11-character message **"Hello world"** was used. The message was encoded in 3 separate images (Peppers, Tulips, Baboon) using both LSB and Chaotic Logistic Mapping based image steganography method.

Table II: Summary of secret messages

S/N	Message	Size
1	**Hello world**	11
2	**A quick brown fox jumps over the lazy dog**	43

In the second experiment a 43-character message **"A quick brown fox jumps over the lazy dog"** was used. We also embedded the message in 3 separate images (Peppers, Tulips, Baboon) using both LSB and Chaotic Logistic Mapping based image steganography method.

In LSB method the cover image was first converted into grayscale. Then it was embedded with the secret messages into the 8th bit of the LSB of the image. In chaotic logistic mapping method, the secret message was embedded in the RGB image.

Each image steganography technique has different strong and weak points and it is important to select the most suitable algorithm for an application. All steganographic algorithms have to comply with a few basic requirements. These requirements are as follows:

A. MSE: The mean-squared error (MSE) used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image. MSE between two images I1 (m,n) and I2(m,n) is [4]:

M and N are the number of rows and columns in the input images, respectively.

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N}$$

B. PSNR: whereas peak signal-to-noise ratio (PSNR) is also used for comparing image compression quality. It represents a measure of the peak error. The lower the value of MSE, the lower the error [6]

C. Payload capacity: the maximum size of a message that can be embedded in a cover image is called Payload capacity. usually, it is measured using bits per pixel (bpp) or bits per byte (bpb) [1].

$$PSNR = 10\log_{10}\frac{256^2}{MSE}$$

D. Invisibility: The invisibility of a steganographic algorithm is the ability to be unnoticed by the human eye. The algorithm considered to be compromised no one can see that an image has been tampered with [1].

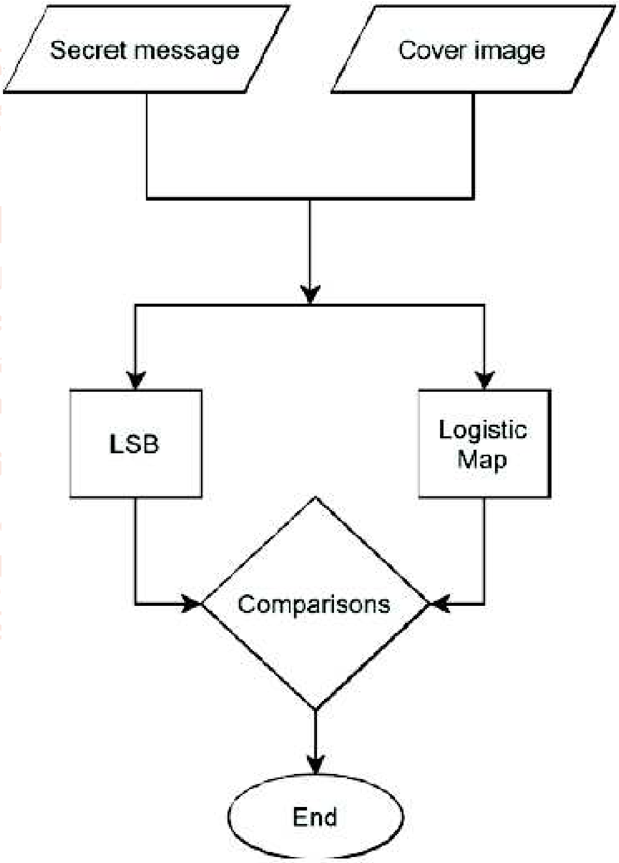


Fig 3: Dataflow diagram of proposed methodology.

EXPERIMENTAL RESULTS AND PERFORMANE ANALYSIS

Steganography algorithm should fulfill every requirement to be perfect. Unfortunately, the algorithms evaluated here don't satisfy all the requirements. So, a trade-off is required for specific application. In Table III a generic comparison of performance factor is depicted.

For the experiment at first the message "Hello world" is hidden using the previously stated images and LSB and chaotic mapping is implemented on them. The result of the required time, MSE, SNR and PSNR values are calculated. Then the same values are calculated for the same images but this time for a different message.

Table III: Comparison of Performance factors

Evaluation Factor	LSB	Chaotic LM
Invisibility	**High**	**Low**
Image Distortion	**Low**	**Moderate**
Payload capacity	**High**	**Moderate**

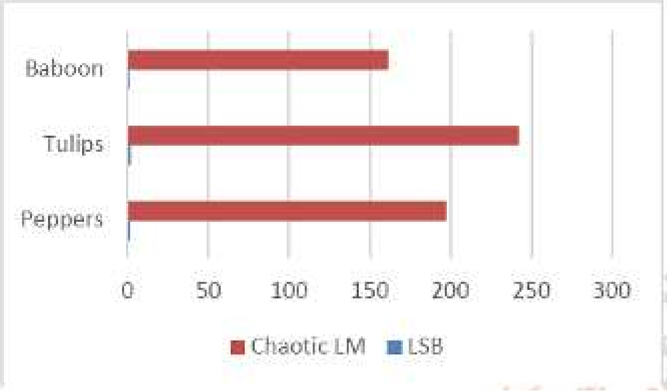


Fig 4: Required time in seconds for message size of 11.

From figure 4 and 5 it is clearly observed that chaotic logistic mapping. takes much higher time than LSB. In case of single image processing's perspective chaotic logistic mapping took more time for high resolution images in case of 11 character message. For 43 character message required time is almost identical for both LSB and chaotic logistic mapping.

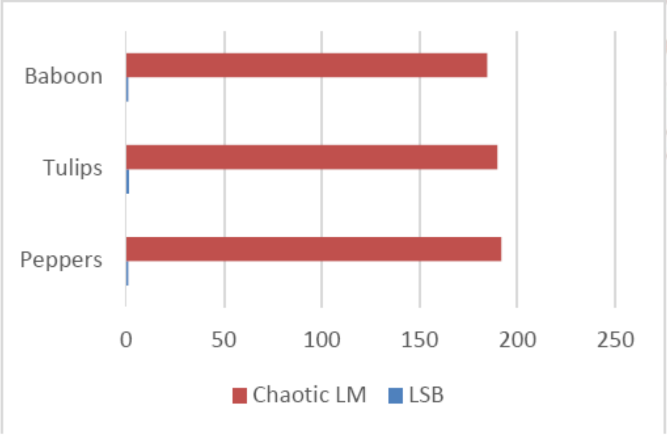


Fig 5: Required time in seconds for message size of 43.

Now from individual algorithm's perspective MSE value can be seen increasing rapidly with message size increase in LSB algorithm as shown in figure 6. While for the same images and message size very low increment is in MSE values are seen for chaotic logistic mapping.

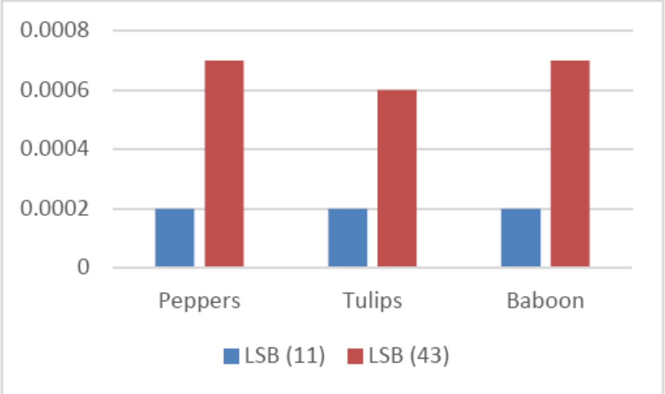


Fig 6: Comparison of LSB MSE values for message size of 11 and 43.

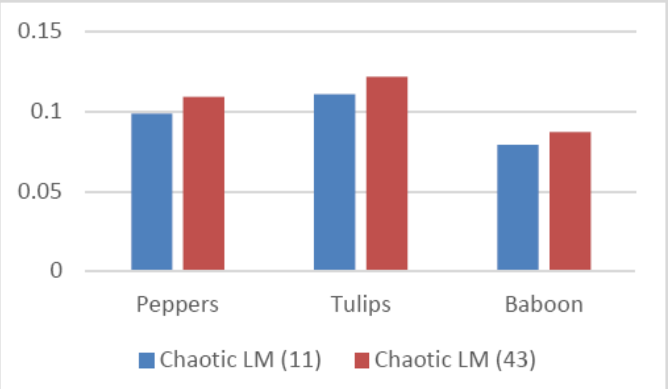


Fig 7: Comparison of Chaotic LM MSE values for message size of 11 and 43.

From figure 7 and 8 relative comparison of PSNR value can be seen for both LSB and Chaotic LM. For LSB increase in message size results in increasing noise between stego-image and original image. 43 character message almost resulted in 2 times multiplied noise for LSB.

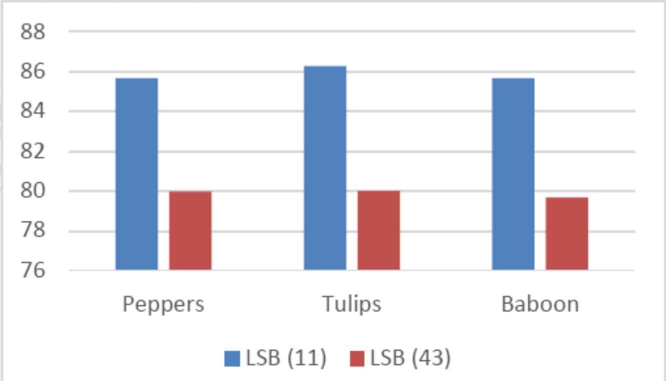


Fig 8: Comparison of LSB PSNR values for message size of 11 and 43.

While noise is almost similar in case of Chaotic LM for increasing message size. So according to the findings it can be evidently said that Chaotic Logistic Mapping is more scalable with respect to LSB in case of steganographic purposes. It is also observed that although generic implementation of Chaotic Logistic Mapping requires more time than LSB but impact of message size is also very little for the previous one.

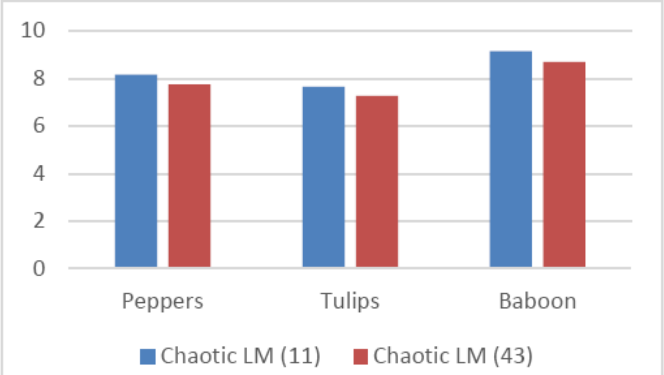
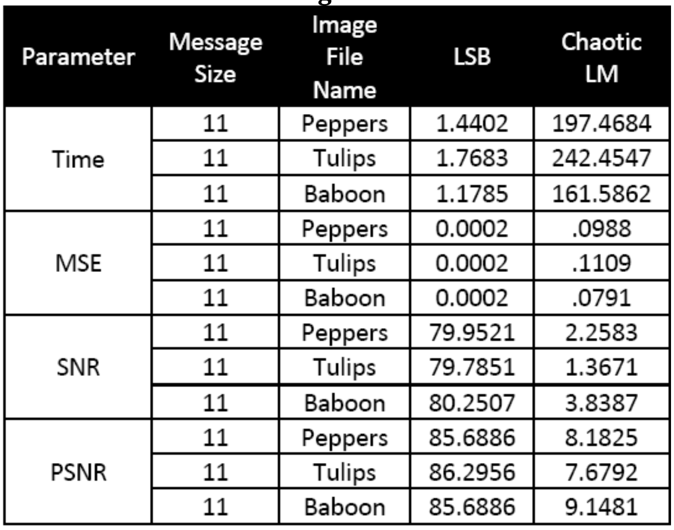


Fig 9: Comparison of Chaotic LM PSNR values for message size of 11 and 43.

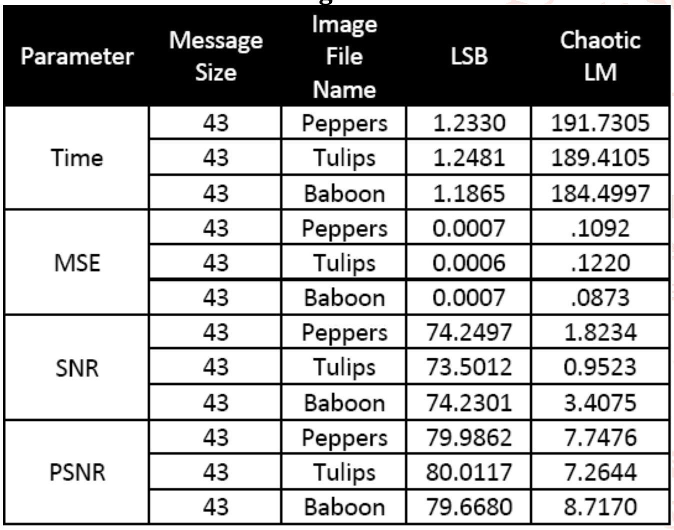
Table IV: Summary of Time, MSE, SNR and PSNR values for message size of 11.



Parameter	Message Size	Image File Name	LSB	Chaotic LM
Time	11	Peppers	1.4402	197.4684
	11	Tulips	1.7683	242.4547
	11	Baboon	1.1785	161.5862
MSE	11	Peppers	0.0002	.0988
	11	Tulips	0.0002	.1109
	11	Baboon	0.0002	.0791
SNR	11	Peppers	79.9521	2.2583
	11	Tulips	79.7851	1.3671
	11	Baboon	80.2507	3.8387
PSNR	11	Peppers	85.6886	8.1825
	11	Tulips	86.2956	7.6792
	11	Baboon	85.6886	9.1481

An overview of all findings is depicted in table IV and table V. For clearance respected SNR values are also included with required Time, MSE and PSNR values for each image and respective message size.

Table V: Summary of Time, MSE, SNR and PSNR values for message size of 43.



Parameter	Message Size	Image File Name	LSB	Chaotic LM
Time	43	Peppers	1.2330	191.7305
	43	Tulips	1.2481	189.4105
	43	Baboon	1.1865	184.4997
MSE	43	Peppers	0.0007	.1092
	43	Tulips	0.0006	.1220
	43	Baboon	0.0007	.0873
SNR	43	Peppers	74.2497	1.8234
	43	Tulips	73.5012	0.9523
	43	Baboon	74.2301	3.4075
PSNR	43	Peppers	79.9862	7.7476
	43	Tulips	80.0117	7.2644
	43	Baboon	79.6680	8.7170

Since, the larger the value of PSNR, the more similarity between the hidden image and the cover image [6]. From this experimental result stego-image in LSB has more remain more similar to the cover image.

CONCLUSION

In this paper, two of the major image steganography techniques have been discussed. Although both techniques have structural differences, based on our experiments, we have found that chaotic logistic mapping is more suitable when the message size is larger. It provides better security for the secret message. On the other hand, the least significant bit (LSB) is more suitable when a short message needs to be embedded on the cover image. The LSB is the better choice if we want to embed the message in a short amount of time since the embedding time in LSB is significantly less the chaotic logistic mapping. Impact of significant increase or decrease of message size on Chaotic Logistic Mapping and Least Significant Bit should be further explored to find the tolerance limit. The above findings can also help to predict the number of cover images required for sending a specific message based on selected steganographic technique. Optimal algorithm can also help sending bigger messages using lowest number of cover images.

REFERENCES

[1] Morkel, T., J. Eloff and M. Olivier. “An overview of image steganography, Proceedings of the ISSA 2005 New Knowledge Today Conference,” 2005, pp. 1-11.

[2] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques, 2014 International Conference on Computer Communication and Informatics,” 2014, pp. 1-4, doi: 10.1109/ICCCI.2014.6921751.

[3] Mohammed Mahdi Hashim, Mohd Shafry Mohd Rahim, Fadil Abass Johi, Mustafa Sabah Taha, Hassan Salman Hamad, “Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats, International Journal of Engineering and Technology,” Volume 7, Issue 4, 2018, pp. 3506-3514, doi:10.14419/ijet.v7i4.17294.

[4] Goel, Stuti. (2013), “A Review of Comparison Techniques of Image Steganography, IOSR Journal of Electrical and Electronics Engineering,” Volume 13, Issue 4, 2013, pp. 41-48, ISSN 2214-2126, pp. 41-48. 10.9790/1676-0614148.

[5] Milad Yousefi Valandar, Peyman Ayubi, Milad Jafari Barani, “A new transform domain steganography based on modified logistic chaotic map for color images, Journal of Information Security and Applications,” Volume 34, Part 2, 2017, pp. 142-151, ISSN 2214-2126, doi:10.1016/j.jisa.2017.04.004.

[6] X. Zhou, W. Gong, W. Fu and L. Jin, "An improved method for LSB based color image steganography combined with cryptography, 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS),” 2016, pp. 1-4, doi: 10.1109/ICIS.2016.7550955.

[7] Xia, Zhihua & Wang, Xinhui & Xingming, Sun & Wang, Baowei. (2014). Steganalysis of least significant bit matching using multiorder differences. Security and Communication Networks. 7. 10.1002/sec.864.

[8] Mandal, M., Nandi, D., Banik, G., & Chattopadhyay, D. (2012). An image encryption process based on Chaotic logistic map. IETE Technical Review, 29(5), 395. doi:10.4103/0256-4602.103173