DOI: https://doi.org/10.33103/uot.ijccce.20.1.4

A Development of Least Significant Bit Steganography Technique

Mohammed Majid Msallam
Control and Systems Engineering Department, University of Technology, Baghdad, Iraq
60190@uotechnology.edu.iq

Abstract— *Recently, the world has been interested in transferring data between different devices. The transmission of data must be encrypted so that the intended receiver can only read and process a secret message. Hence, the security of information has become more important than earlier. This paper proposes the least significant bit Steganography method to hide a secret message inside an image cover via using dynamic stego-key. To check the effectiveness of the proposed method, many factors are used for evaluation and compared with another method. The results illustrate more robustness at steganography since stego-key depends on the cover image to hide a secret message.*

Index Terms— *Encryption, dynamic Stego-key, Steganography, Least Significant Bit*

I. INTRODUCTION

The encryption of secret information is very old. It was started at Greek time [1]. At present, the communication is very important and popular to transform data from one device to another. A message travels from a side to another side and the unauthorized side may listen and discover the content of the message. Therefore the message must be protected from the unauthorized side. Various techniques have been developed to protect sending the message; Figure 1 shows the classification of different information hiding techniques.

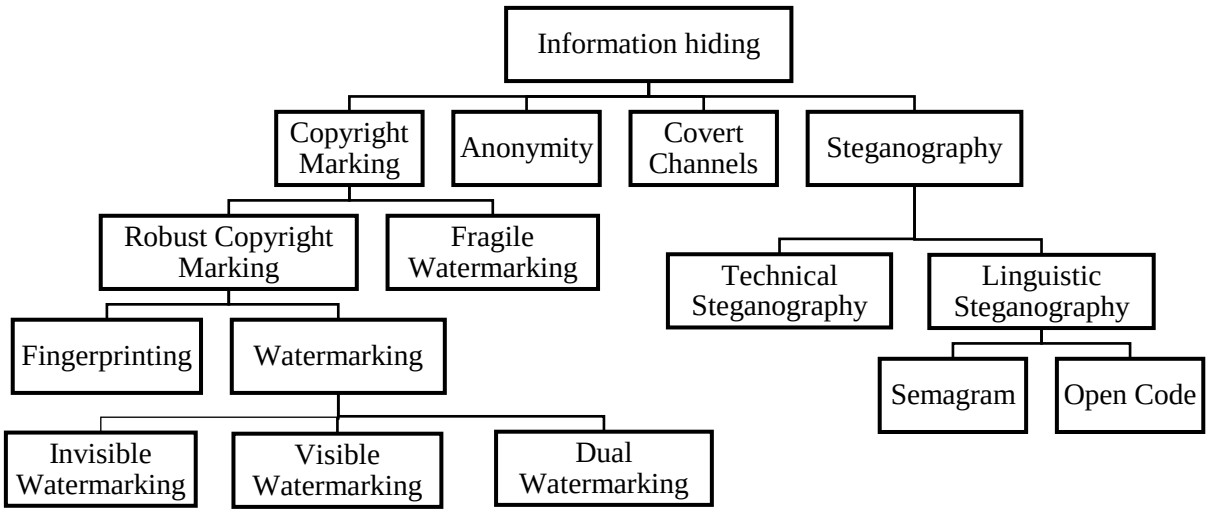

FIGURE1: INFORMATION HIDING TECHNIQUES.

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

In computer science, steganography is derived from the Greek language, which means "covered writing". Steganography is the art and science of communicating in a way that does hide a secret message inside the main information. The main goal of steganography is to hide messages inside other messages in a way that does not allow anyone to detect that there is a hidden message. Cryptography is referred to as "secret writing" [2]. Cryptography is a method of sending a message in a distinct form so that the intended receiver can read and process it.

At cryptography, the hidden message is called plain text and a disguised message is called ciphertext. The process of converting a plain text into ciphertext is enciphering or encryption and the reverse process is called deciphering or decryption [3]. whereas steganography, the process of embedding a secret message inside data cover is called encoding or embedding and the reverse process is called decoding or extraction or detection which is shown in Figure 2.

The types of Steganography are Pure Steganography, Secret Key Steganography, and Public Key Steganography. Pure Steganography does not use Stego-key so that the sender and receiver can rely only upon the supposition that no one is aware of this secret message. Secret Key Steganography uses Stego-key so that anyone who knows the Stego-key can reverse the process and read the secret message. Public Key Steganography includes two keys, one is private and the other is public, the public key is used in the embedding process and the private key is used to extract the secret message [4].

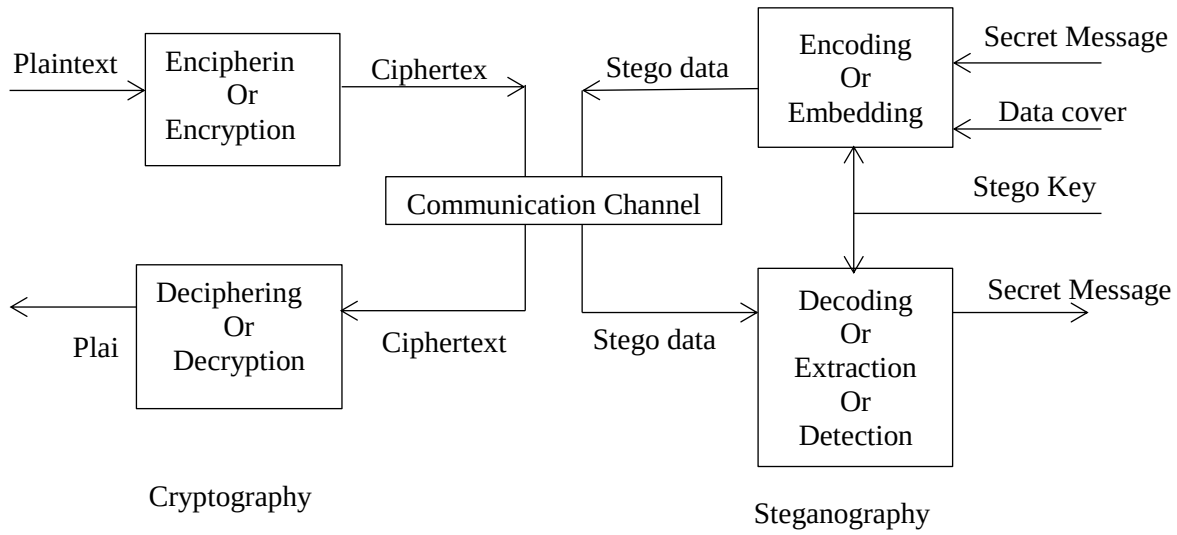

FIGURE 2: STEGANOGRAPHY AND CRYPTOGRAPHY.

There are several types that have been used to hide information on various digital mediums such as image, audio, video, Network, and Text.

1. Image Steganography: in this method, the image is a cover object in steganography is known as image steganography. Generally, in this technique, pixel values are changed based on Secret message values in such a way that changes in data cover remains approximately unnoticeable [5].
2. Audio Steganography: In this technique, audio formats like WAV, MIDI, AVI, MPEG ,etc. are used as a covered object is used Audio Steganography is very important and popular because of the high popularity of voice over IP (VOIP) [5].

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

3. Video Steganography: In this technique, Video (series of pictures) is used as a cover object. Discrete cosine transform (DCT) alters the pixel value of the image so that impossible to recognize by a human eye because of negligible change in the image. Format video is used as a cover object like MP4, MPEG, AVI and etc.[5].
4. Network Steganography: In this technique, a cover object at network Steganography is TCP, UDP, ICMP, IP and etc. The secret message hides in the header of the protocol [5].
5. Text Steganography: this technique uses a number of tabs, white spaces, capital letters, just like Morse code and etc. to achieve information hiding [5].

American Standard Code for Information Interchange (ASCII) is a format character in the digital systems. In digital systems, ASCII code represents each alphabetic, numeric, and special character with an 8 bits binary number. For example, the ASCII Code for (A, a) is (65, 97) respectively. In this paper, each character of the secret message converts into the binary of ASCII code.

TABLE 1: LETTERS ASCII VALUES AND BINARY [6].

LETTER	ASCII VALUES	BINARY VALUES	LETTER	ASCII VALUES	BINARY VALUES
A	65	01000001	A	97	01100001
C	67	01000011	C	99	01100011
D	68	01000100	D	100	01100100
E	69	01000101	E	101	01100101
F	70	01000110	F	102	01100110
G	71	01000111	G	103	01100111
H	72	01001000	H	104	01101000
I	73	01001001	I	105	01101001
J	74	01001010	J	106	01101010
K	75	01001011	K	107	01101011
L	76	01001100	L	108	01101100
M	77	01001101	M	109	01101101
N	78	01001110	N	110	01101110
O	79	01001111	O	111	01101111
P	80	01010000	P	112	01110000
Q	81	01010001	Q	113	01110001
R	82	01010010	R	114	01110010
S	83	01010011	S	115	01110011
T	84	01010100	T	116	01110100
U	85	01010101	U	117	01110101
V	86	01010110	V	118	01110110
W	87	01010111	W	119	01110111
X	88	01011000	X	120	01111000
Y	89	01011001	Y	121	01111001
Z	90	01011010	Z	122	01111010

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

Mohit [7] has been proposed a method to embed a secret message in two images (Master and Slave image) by three levels. The first level is to encode a secret message into binary form, then XORing the binary message with the slave image and finally hiding it into a master image by LSB. Ajit et al. [3] have been proposed a model to encode a secret message by two methods. The first method is used to encrypt the secret message by using Blowfish Encryption Algorithm, then using LSB steganography hiding the encrypted text. The authors in [8] use a new method to encrypt a secret image, the stego key which encrypts with their method, then encrypting the image with a secret image using one-bit sequence. Sheshadri et al. [9] have been encrypted a secret message inside the cover image using LSB and Zigzag algorithm by Symmetric Key.

In fact, normally the enemy knows about the design and implementation details of the steganographic system, so when the key is detected, the secret message can be found. The proposed model introduces an approach to hide the secret message using a dynamic key. Many encryption approaches use the static key after encrypting. In this work, the key is depended on the cover data which means it is dynamic.

II. LEAST SIGNIFICANT BIT (LSB)

Least significant bit (LSB) is a technique being used to embed a secret message into an image cover. Image pixels can be converted into binary form and secret message can be converted into ASCII in binary form also. A least significant bit of image pixel is substituted with one bit of secret message binary [10].

The secret message must be converted into a binary format based on the ASCII code which is shown in Table 1. The ASCII code for space is 32 and the binary of 32 is 00100000. Let suppose that the secret message is "A", and image pixels are {4, 134, 42, 78, 200, 33, 76 and 57}. The binary of the secret message is 01000001 and the binary of image pixels converted into binary form in column Binary Pixels of Table 2. One bit of the secret message embedded inside the least significant bit for one image pixel which shown in Table 2.

TABLE 2: LSB ALGORITHMS

image Pixels	Binary Pixels	Binary Embedded	Embedded Pixels
4	00000100	0000010***0***	4
134	10000110	1000011***1***	135
42	00101010	0010101***0***	42
78	01001110	0100111***0***	78
200	11001000	1100100***0***	200
33	00100001	0010000***0***	32
76	01001100	0100110***0***	76
57	00111001	0011100***1***	57

LSB can be developed to become more secure. Our algorithm is similar to LSB, which converts the message and image pixels into binary form, but the difference is in substituting. The most significant bit (MSB) uses to decide the substituted bit of a message if it is the first bit of LSB or the second bit. Our algorithm is a protocol between the sender and the receiver. For example, when MSB is '1', it substitutes the first bit of the LSB and when MSB is '0', it substitutes the second bit of the LSB. This algorithm is called a development least significant bit (DLSB). The DLSB is shown in Table 3 for the message "A".

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

TABLE 3: DLSB ALGORITHMS

Image Pixels	Binary Pixels	Binary Embedded	Embedded Pixels
4	00000100	0000010**0**	6
134	10000110	1000011**1**	135
42	00101010	0010100**0**	40
78	01001110	0100110**0**	76
200	11001000	1100100**0**	200
33	00100001	0010000**1**	33
76	01001100	0100110**0**	76
57	00111001	0011101**1**	59

There are many factors to evaluate the effectiveness of steganography such as entropy, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and adjacent pixel correlation analysis.

1. Entropy: Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. The entropy of the message has given [11] :

$$H = -\sum_{i=0}^{2^N-1} P(s_i)\log_2 P(s_i) \quad (1)$$

Here $P(s_i)$ is the probability of symbol is and N is the number of bits to represent a symbol s_i. There are 256 states of the information in an image with the same probability.

2. Mean Square Error (MSE): MSE calculates the squared differences of the entire pixel image then dividing by the total pixel count. MSE is defined as [7]:

$$MSE = \frac{1}{W \times H} \sum_{r=0}^{W-1} \sum_{c=0}^{H-1} (I(r,c) - D(r,c))^2 \quad (2)$$

Where I (r, c) is the pixel value of the original image at the (r, c) locations, D (r, c) is the value pixel of the stego image at the same locations (r, c), H is the number of columns, and W is the number of rows.

3. Peak Signal to Noise Ratio (PSNR): PSNR is a measure of the stego image relative to the original image. The higher the value of PSNR means the higher the quality of hiding . PSNR is defined as [7] :

$$PSNR\ (db) = 10 \log_{10} \frac{(2^n-1)^2}{MSE} \quad (3)$$

Where n is the number of bits per image sample and MSE is the Mean Squared Error between the distorted image and the original image.

4. Adjacent pixel correlation analysis: it is a relationship between two adjacent pixels in an image. A high correlation value between adjacent pixels is image pixels very close to each other. The question of a correlation coefficient is as follows [10]:

$$cc = \frac{cov(x,y)}{\sigma x \times \sigma y} \quad (4)$$

$$\sigma x = \sqrt{var(x)} \quad (5)$$

$$\sigma y = \sqrt{var(y)} \quad (6)$$

$$var\ (x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \quad (7)$$

$$var(y) = \frac{1}{N} \sum_{i=1}^{N} (y_i - E(y))^2 \quad (8)$$

$$cov(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))\ (y_i - E(y)) \quad (9)$$

Here x and y are adjacent pixels in a plain image of size M *N.

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

III. EXPERIMENTAL RESULTS

The proposed model was implemented in MATLAB® 2019b to obtain many factors so as to evaluate the effectiveness of steganography. In this work, four images were used to send a secret message that contains capital letters, space, and small letters. The four images are Lenna, Baboon, Fruits, and Boat with the size 512x512 and type PNG which shown in Figure 3. A first and second of the least significant bits are called a changeable bit and the first of the most significant bit is called a checkable bit. Then the bit of secret message is called an embedded bit.

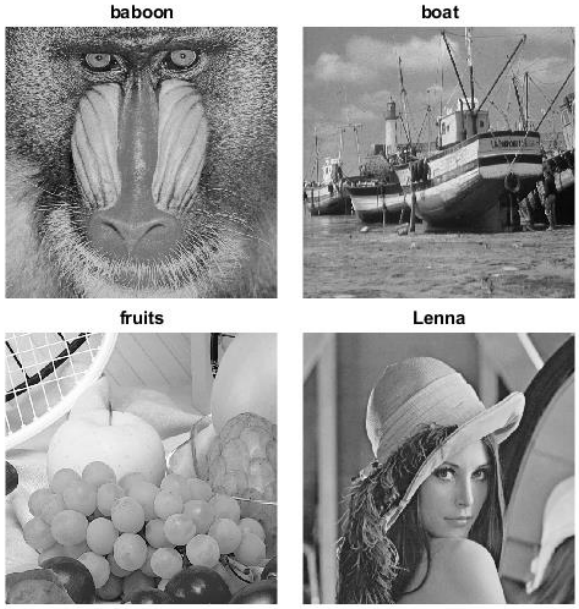

FIGURE 3: TEST IMAGE.

In encryption, the embedded bit will be replaced with changeable bit as shown in Figure 4. If a checkable bit is '1', an embedded bit will be substituted with the first changeable bit. As well if a checkable bit is '0', an embedded bit will be substituted with the second changeable bit. In decryption, the DLSB algorithm will read a changeable bit based on a checkable bit, which means reverse that shown in Figure 4.

TABLE 4: RESULT

Image	Entropy		MSE		PSNR	
	DLSB	LSB	DLSB	LSB	DLSB	LSB
Lena	7.4451	7.4451	0.0011	3.7766e-04	77.9071	82.3599
Baboon	7.3583	7.3583	9.1934e-04	3.2425e-04	78.4960	83.0220
Fruits	7.4518	7.4518	6.6757e-04	3.7384e-04	79.8858	82.4039
Boat	7.1914	7.1914	0.0015	3.2425e-04	76.3944	83.0220

PNSR is a difference between a Stego and an original image as shown in Table 4. When LSB is used in encoding, the changing effect will not be recognized by human eyes. A changing effect of DLSB is also not realizing by human eyes. An LSB value is greater than a DLSB value which means that the noise is very low and security is low. The goal of Steganography is to make low noise and high security. DLSB noise is high, but is not observed by human eyes and security is high.

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

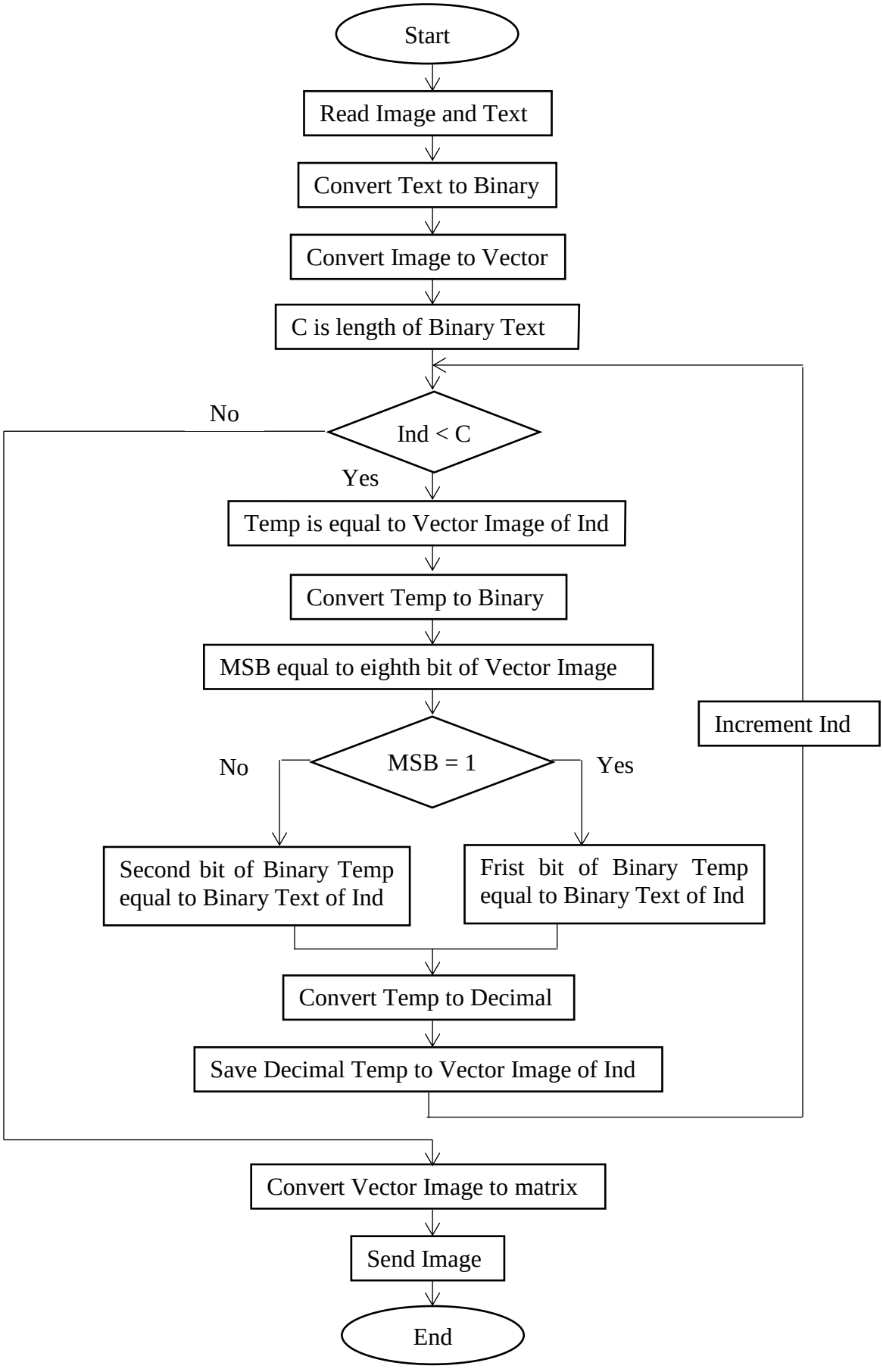

FIGURE 4: FLOW CHART OF THE PROPOSED MODEL.

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

The LSB value and DLSB value of entropy are the same because the image pixels change simply. The image pixel value changes between ±2 by the DLSB algorithm so that small change effects on PSNR. Luckily, the embedding bit has the same changeable bit so that there is no effect on color grade.

The adjacent pixel sequence (horizontal, vertical and diagonal) in the original image and corresponding stego image has already been shown in Figures 5 and Figures 6.

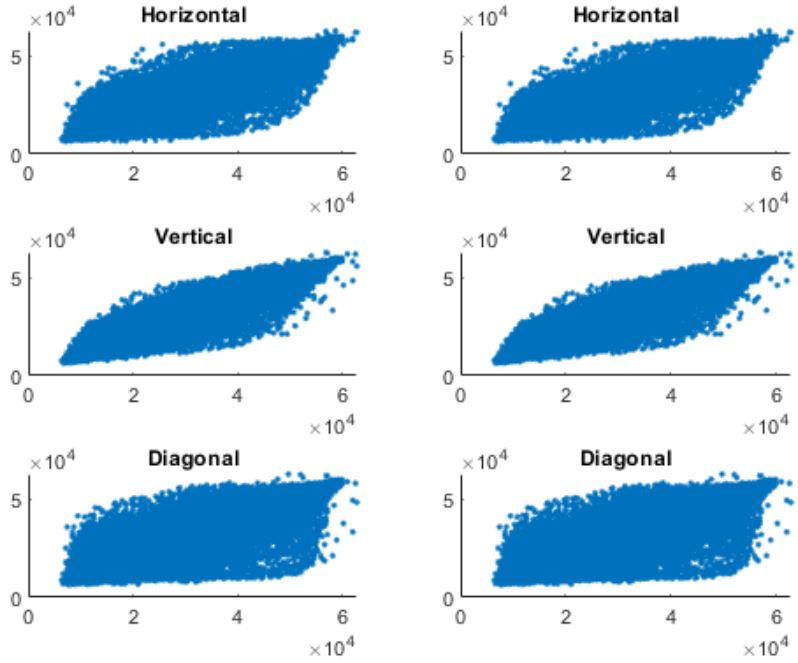

FIGURE 5: ADJACENT PIXEL CORRELATION OF LENNA IMAGE FOR DLSB.

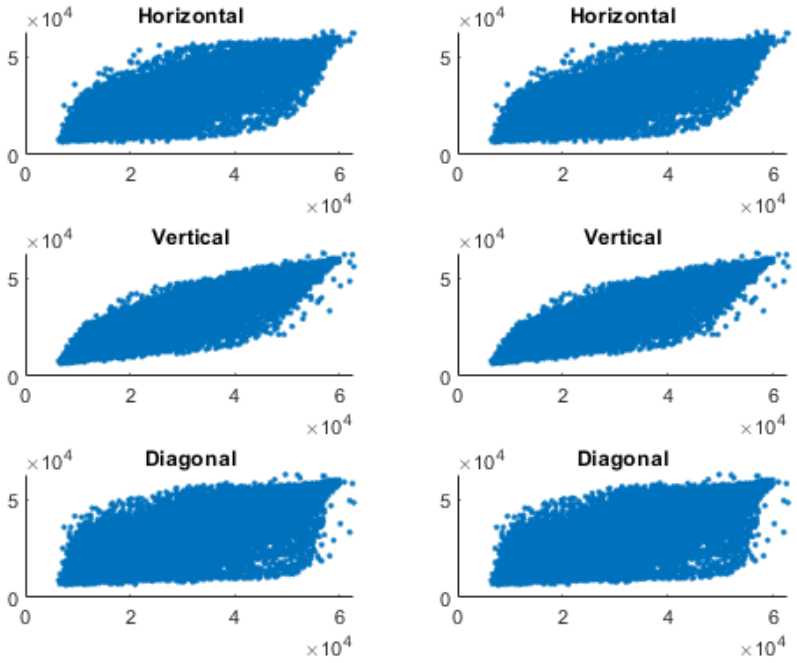

FIGURE 6: ADJACENT PIXEL CORRELATION OF LENNA IMAGE FOR LSB.

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

IV. CONCLUSIONS

The focus of this paper is on image steganography. The DLSB approach has been applied to images for hiding a secret message as well as the LSB has been used for the purpose of comparison. The maximum number of bits that can be hidden is equal to the number of pixels in the image.

The application of a dynamic key of the DLSB is one of the main advantages that has been provided in this work. The results show a small change between DLSB and LSB. In the LSB method, the color grade of the image pixel changed between ±1 from the original value. Whereas, in DLSB, the color grade of the image pixel is changed between ±2 from the original value. Hence, it is impossible to recognize the difference between cover and stego image by a human eye because of the small change in color grade. In addition, the key dynamic will now depend on the cover image which rarely can be recognized. Further work can be applied by employing more methods of encrypting on the secret message.

REFERENCES

[1] Muneera Alotaibi, Daniah Al-hendi, Budoor Alroithy, Manal AlGhamdi, and Adnan Gutub, "Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination," Journal of Information Security and Cybercrimes Research (JISCR), vol. 2, no. 1, 2019.

[2] Geetika Dhand, "information hiding techiques," proceeding of the national conference, 2008.

[3] Ajit Singh, and Swati Malik, "Securing data by using cryptography with steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, 2013.

[4] Mohammed Abbas Fadhil Al-Husainy, and Diaa Mohammed Uliyan, "A Secret-Key Image Steganography Technique using Random Chain Codes," International Journal of Technology, vol. 10, no. 4, 2019.

[5] Shahid Rahman, Fahad Masood, Wajid Ullah Khan, Abdus Salam1, and Syed Irfan Ullah ""The Investigation of LSB based Image Steganographic Techniques in Spatial Domain for Secure Communication," Sukkur IBA Journal of Emerging Technologies, vol. 2, no. 1, 2019.

[6] Wikipedia, "https://en.wikipedia.org/wiki/ASCII."

[7] Mohit, "An Enhanced Least Significant Bit Steganography Technique," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 5, no. 6, 2016.

[8] Bhanupriya Katre, and Bharti, "Dynamic Key based LSB Technique for Steganography," International Journal of Computer Applications, vol. 167, no. 13, 2017.

[9] H. S. Sheshadri, and Wa'el Ibrahim A. Almazaydeh, "Image Steganography Using a Dynamic Symmetric Key," Proceedings of the 2nd International Conference on Inventive Computation Technologies (ICICT), 2017.

[10] O. Osunade and I. A. Ganiyu, "Enhancing the Least Significant Bit (LSB) Algorithm for Steganography," International Journal of Computer Applications, vol. 149, no. 3, 2016.

[11] Shafali Agarwal, "A Review of Image Scrambling Technique Using Chaotic Maps," International Journal of Engineering and Technology Innovation, vol. 8, no. 2, 2018.

Received 2 July 2019; Accepted 8 October 2019

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352