

A New Approach of Data Hiding in BMP Image Using LSB Steganography and Caesar Vigenere Cipher Cryptography

I Gede Arya Putra Dewangga

*Departement of Computer Engineering, Faculty Of Electrical Engineering, Telkom University, Bandung, Indonesia.
Orcid: 0000-0001-8038-2317*

Tito Waluyo Purboyo

*Departement of Computer Engineering, Faculty Of Electrical Engineering, Telkom University, Bandung, Indonesia.
Orcid: 0000-0001-9817-3185*

Ratna Astuti Nugrahaeni

*Departement of Computer Engineering, Faculty Of Electrical Engineering, Telkom University, Bandung, Indonesia.
Orcid: 0000-0002-5471-9593*

Abstract

The digital image is one of the most common media is known by the public. Steganography is a method of cryptography used to hide data in a digital image so that data transmitted cannot be identified by irresponsible parties. One of a kind of digital imagery that is is a BMP format or bitmap, bitmap file format may consist of 1, 4, 8, 24, and 32 bits of color for each pixel. The method used to conceal secret messages is to how to insert cryptography messages into the low bits (least significant bit) to the pixel data that make up a digital image file BMP. By developing a method of steganography then sending data which do not only have a good level of security, but also has a level of security to protect a copyright of a digital image.

Keywords: Cryptography, LSB, Steganography, BMP

INTRODUCTION

In the current era of globalization with a variety of technologies that have already matured, any person can easily make use of technology to do business in order to meet the needs of his life. However, with advances in technology nowadays, anyone can easily do piracy against the work of others to profit from piracy results the results of the work of others. Based on the provisions of the legislation that the hijacking was a copyright infringement, said copyright infringement for having violated the exclusive rights of the creator or copyright holder. Exclusive rights are rights that are solely reserved for the holder so that there is no other party may utilize such as announcing or reproduce those rights without the permission of the holder.

To protect the copyright of digital image can be done by inserting messages of text, where the text contains information from the photographer or owner of the digital image. One way to insert messages into digital image steganography technique by. Steganography is a technique used to hide data in a digital

image so that data transmitted cannot be identified by irresponsible parties. One goal of steganography is submitting confidential information without causing suspicion.

Besides that steganography can also be used to perform authentication against an artwork as the utilization of watermarking [2]. Steganography requires at least two properties. The first property is the container (cover) and the second is data or messages that are hidden. One of the methods of steganography can be used to insert messages into digital imagery is a method of LSB. The process of inserting a message method LSB (Least Significant Bit) is by way of inserting the bit messages into every last pixel bits of digital imagery. The process of exploiting LSB senses that human eyes can not see the shift from very little color.

To increase the level of security of the data stored can be done by adding a key property (key) the secret. This key property can be either a symmetric key or a public key or a private in cryptographic techniques can be from. This cryptography which will secure messages to be inserted into a digital image. After the message is secured with cryptography then the message will be posted on a digital image using steganography techniques.

LITERATURE REVIEW

Steganography

Steganography is a technique to hide personal information by something that the result will look like other normal information. The medium used is generally a different media with media bearer of confidential information, where this is a function of the technique of steganography using disguises techniques as other media are different so that confidential information in the initial media is not clearly visible [12].

Steganography is usually often in incorrectly sense with cryptography ,therefore both equally to protect valuable

information [4]. The fundamental difference between the two i.e. steganography-related information hidden so it looks like there is no hidden information at all [8]. If one observes the object store hidden information, he will not think that there is a secret message in the object, and therefore he will not attempt to solve the information (decryption) of the object.

Basic concepts from steganography are that an image which has a cover that was used in order to cover images of the original message [10]. The output of images called stego image with, which has a hidden message. Stego images are then sent to recipients where the recipients take a picture message with steganography [9].

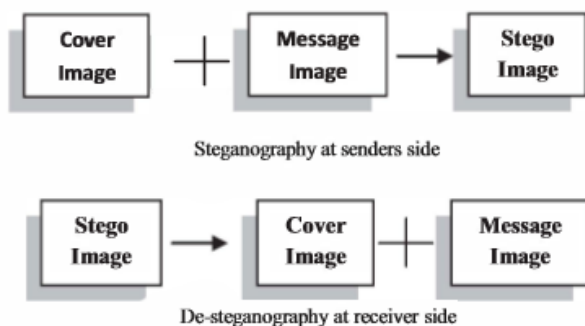


Figure 1: Encoding and Decoding Process [9]

Digital Image

A digital image is an image that is stored in a digital format. Only the digital image can be processed using a computer. If the type of the image wants to be processed by the computer, the image should be converted into a digital image. Digital images are usually stored as image files with a size of 24-bit or 8-bit. Image size 24-bit known as the true color image. The 24-bit image is scattered with 3 bytes at each pixel represents the color red, green, and blue (RGB) respectively. The color is derived from combining the light red, green, and blue with different proportions. For the 8-bit image, each pixel is represented by 1 byte, which has a range of values from 0 to 255 with 256 possibilities, so there are 256 color or grayscale values for black and white images.

BMP Digital Image

The bitmap is a representation of the graphic image which consists of a point that is stored in computer memory. Developed by Microsoft and the value of each point by a single bit of data for an image in black and white, or more for color images. This file type is usually used for the Windows operating system and OS/2. Excess BMP file type is to be opened by almost all image processing programs.

Either the compressed BMP files or uncompressed, BMP files have a size much larger than the other types. Excess is the Bitmap Image supports the use of up to 32-bit color 1bit.

Suitable for bitmap images such as logo design, banner and so on. While the shortage of bitmap image is larger than the size of the image to other formats. On the representation of the bitmap, an image divided into small boxes where each box stores the value of the intensity of color called pixels

BITMAPFILEHEADER
BITMAPINFOHEADER
RGBQUAD array
Color-Index array

Figure 2: BMP Data Structure

LSB Steganography

The simplest method for hiding data in pictures is a method of LSB (least significant bit) [1]. LSB method exploiting human visual senses in the observed changes a bit in the picture [5]. Figure 24 bit or often called with RGB true color, very suitable for the insertion of this because the lsb method consists of 3 components i.e. red, green and blue. When using a 24-bit image, bits of channel red, green and blue can be used, so the number of bits for each pixel can be inserted as much as 3 bits [7]. For example, the image of 3 pixels of a 24-bit image uses 9 bytes of memory [6]:

```
(00100110 11101111 11001010)
(00100101 11001010 11101011)
(11001100 00100011 11101101)
```

When the letter D (ASCII 68), with the binary number 1000100, inserted and the results :

```
(00100111 11101110 11001010)
(00100100 11001011 11101010)
(11001100 00100011 11101101)
```

In the example above is not significant pixel replacement done in order. No significant pixel replacement can also be sorted by, even this can increase the level of data security (imperceptibility). Beside that also might do the conversion pixel is not at the beginning of the file container. Conversion pixels can also be selected starting from the Middle, or from another point from the file container that it is possible to keep all information confidential, without causing problems when the disclosure of the data.

Although the methods are easy to implement LSB, steganography with this method will produce an easily broken

stego file (botched). Using LSB steganography technique, a little change on the file stego is very likely also would damage the confidential information stored on it [11].

In addition to the possibility of damage to information stored in a file on the file changes due to stego stego, LSB steganography method also only able to store information with a very limited size. For example, a 24-bit image (R = 8-bit, 8-bit G =, B = 8 bits) is used as a container to store the data size is 100 bits, if each color component (RGB) used one pixel to store confidential information, then each pixelnya stored 3 bits of information, so at least it takes the image of a container measuring 34 x 34 pixel or equivalent 3 x 8 = 816 bits (8 fold). So a 24-bit image if used to store confidential information is only able to accommodate the maximum size of information 1/8 of the size of the image of the reservoir [8].

Cryptography

Cryptography is a science that studies mathematical techniques associated with information security aspects such as data confidentiality, the validity of the data, data integrity, and data authentication [16]. A few definitions concerning Cryptography:

- Cryptography is a branch of mathematics which provides a technique to allow confidential information to be sent via public networks [17].
- data integrity (data integrity) data integrity is a service that aims to prevent the occurrence of the alteration of information by Parties not authorized. To assure the integrity of data must be ensured so that information systems are able to detect the occurrence of data manipulation. Data manipulation in question here includes the insertion, deletion, or replacement of data.
- the Authentication (authentication) authentication is a service related to the identification of the parties who wish to access the information system (entity authentication) as well as the authenticity of the data from the information system itself (data origin authentication).
- The absence of denial (non-repudiation) the absence of denial is a service that serves to prevent the occurrence of denial of an action performed by the offender information systems.

The Mechanisms of Cryptography

A cryptography system works by encoding a message into a secret code that is understandable by the offender information systems only. Basically, the mechanism of action of this kind has been known since antiquity. The nation's ancient Egypt around 4000 years ago even had stemmed from a very primitive way. In the era of information technology is today, the same mechanism still used but of course, the

implementation of the system is different. Before discussing further the mechanisms of modern cryptography, the following are given some of the terms commonly used in the discussion of Cryptography.

- The Plaintext (the message) is the original message that likes to sent and guarded security. This message is none other than the information.
- Ciphertext is encoded messages (encoded) so that it is ready to be shipped.
- Cipher is a mathematical algorithm used for the encryption process the plaintext into ciphertext.
- Encryption is a process that is done to encode the plaintext so it becomes ciphertext.
- Decrypt (decryption) is a process that is done to recover plaintext from the ciphertext.
- A cryptosystem is a system designed to secure an information system by making use of Cryptography.

The cryptographic process sequences can be described as follows.

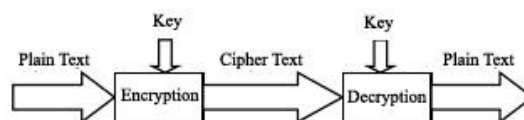


Figure 3: The Cryptography Process

The process is basically very simple. A plaintext (m) will be skipped in the encryption process (E) resulting in a ciphertext (c). Subsequently to reclaim the plaintext, then the ciphertext (c) through the process of decryption (D) that will result in returning the plaintext (m). Mathematically this process can be expressed as, $E(m) = c$ $D(c) = m$ $D(E(m)) = m$

This is as simple as using a cryptographic encryption algorithm called cipher. Security relies on confidentiality that encryption algorithms, algorithms must keep secret. On the group with a large number of members and the ever-changing, its use will cause problems. Every Member who is leaving the group, the algorithm should be replaced because the members can only divulge the algorithms. Modern cryptography in addition to utilizing the algorithm also uses a key (key) to solve the problem. The process of encryption and decryption is done by using this key. Each Member has their respective key used for the encryption and decryption process is going to do. Thus there are a few changes to be made on the mechanism illustrated in Figure 4 image be as following. :

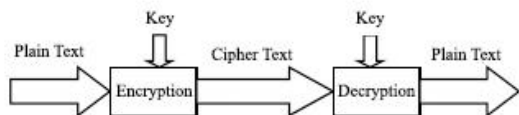


Figure 4: Cryptography Cipher Process

Vigenere Encryption Example :

Plain Text: PESAN INI SANGAT RAHASIA

Key: ARMADA

Cipher Text: PVEAQ INZ EAQGAK DAKASZM

Caesar Cipher

Caesar cipher is taken from the name of the Roman Emperor Julius Caesar, in Julius Caesar mengamankannya sending a message by way of the existing content of the message is encoded by replacing the position of each letter of the message with others who have a position difference the other letters of the alphabet [4]. As for steps-steps that are performed are as follows: a. Determine the magnitude of the shift amount of letters that will be replaced b. Replace each letter of the message according to the number of shifts in the specified font. c. return the number of letter Arrangement in accordance with the order of the original message.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	1	1	1
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	1	1	1	1	1	1	2	2	2	2	2	2
3	4	5	6	7	8	9	0	1	2	3	4	5

Figure 5: The Orde of The Alphabet

To encode a message simply replacing the letters in the message with the letter password corresponds to the number of shifts in the desired letter.

Caesar Encryption Example:

Original text: PESAN INI SANGAT RAHASIA

Sliding Number (Key): 120

Cipher Text: BQEMZ EMZSMF DMTMEUM UZU

Vigenere Cipher

The Vigenere algorithm used for the Encryption of data or messages by means of data or messages are encoded by using a keyword (Key) in the form of a word or words of the chorus [4]. Each letter on the data or message paired with a letter at the specified keyword, and then do the encryption process that is encryption.

DISCUSSION

Experiments and Result

Insertion of data applied by replacing bits of data in a data segment with bits of data confidential. One of the simple methods of concealing data is LSB. A suitable bit for bit LSB is replaced because just change the value of the byte is one higher or one lower than the previous value. Suppose these bytes a particular of gray color, then change one bit in LSB does not change the color of the gray levels significantly. It is because the human eye can't distinguish colors a slightly changed.

a. Encode Process

Following the process of inserting or encoding text into the RGB Image, measuring 8 x 8 pixel:



Figure 6: RGB Cover Image

Sequence of Pixel 8 x 8 pixel RGB image in red channel

104 108 116 118 115 106 102 110
 132 102 122 151 135 114 95 84
 152 144 123 98 98 107 84 88
 60 149 200 186 111 61 96 76
 13 13 104 173 195 196 230 166
 144 136 123 60 55 119 164 226
 149 148 157 162 106 104 69 61
 134 119 104 100 120 144 139 96

The maximum size of message that can be inserted into an 8 x 8 pixel RGB image

- The number of pixel 8 x 8 = 64
- There are 3 bytes, pixel 64 pixel x 3 bytes = 192 Bytes

- each Byte can insert 1-bit messages, 192 bytes/8 = 24 Bytes
- Then the maximum size of the = 24 Bytes

$$(\text{pixel} \times \text{pixel} \times 3) / 8 \dots\dots\dots (1)$$

Sequence of pixels in binary code from cover image

```
01101000 01101100 01110100 01110110 01110011
10000100 01100110 01111010 10010111 10000111
10011000 10010000 01111011 01100010 01100010
00111100 10010101 11001000 10111010 01101111
00001101 00001101 01101000 10101101 11000011
10010000 10001000 01111011 00111100 00110111
10010101 10010100 10011101 10100010 01101010
10000110 01110111 01101000 01100100 01111000
```

Columns 6 through 8

```
01101010 01100110 01101110
01110010 01011111 01010100
01101011 01010100 01011000
00111101 01100000 01001100
11000100 11100110 10100110
01110111 10100100 11100010
01101000 01000101 00111101
10010000 10001011 01100000
```

The text of the plain text or data will be processed using the caesar cipher that is “APD” The following is the process of using the Encryption algorithm of Caesar.

Caesar Cipher Encryption

Plain text: APD

Key: 4

The encryption process formula

$$E(P) = C, C = P + K \text{ Mod } 26 \dots\dots\dots (2)$$

Description: E (P): P: Encryption of the Plaintext

k: Key (the number of Shift)

Cipher Text: ETH

Vignere Cipher Encryption

Caesar encryption results later became the plain text message will be encoded again with Vignere cipher.

Plain text: ETH

Key: ARA

Cipher Text: EKH

Plain Text	E	T	H
Alphabet Position	5	20	8
key	A	R	A
Alphabet Position	0	17	0
Sum	5	37	8
CipherText	E	K	H

Figure 7 : Vignere Cipher Encryption Process

The insertion process of the letter "EKH" into the RGB cover image. The binary code of the letter "EKH" in the ASCII code is "01000101, 01001011, 01001000"

```
01101000 01101101 01110100 01110110 01110010
10000100 01100111 01111010 10010110 10000111
10011000 10010001 01111010 01100010 01100011
00111101 10010100 11001001 10111010 01101110
00001101 00001100 01101000 10101100 11000011
10010000 10001000 01111011 00111100 00110111
10010101 10010100 10011101 10100010 01101010
10000110 01110111 01101000 01100100 01111000
```

Columns 6 through 8

```
01101011 01100110 01101111
01110010 01011111 01010101
01101010 01010100 01011000
```

00111101 01100000 01001100
 11000100 11100110 10100110
 01110111 10100100 11100010
 01101000 01000101 00111101
 10010000 10001011 01100000

Binary code has slightly changed.

104 109 116 118 115 107 102 111
 132 103 122 152 135 114 95 85
 152 143 124 98 99 108 84 88
 60 149 200 186 111 61 96 76
 13 13 104 173 195 196 230 166
 144 136 123 60 55 119 164 226
 149 148 157 162 106 104 69 61
 134 119 104 100 120 144 139 96

Sequence has slightly changed of Pixel 8 x 8 RGB Image in red channel.

b. Decode Process

After the image is successfully inserted, the pixel sequence of cover image or stego image

104 109 116 118 115 107 102 111
 132 103 122 152 135 114 95 85
 152 143 124 98 99 108 84 88
 60 149 200 186 111 61 96 76
 13 13 104 173 195 196 230 166
 144 136 123 60 55 119 164 226
 149 148 157 162 106 104 69 61
 134 119 104 100 120 144 139 96

For the decoding process, we must change the image to binary code and decoding process only take the value of last bit binary code.

01101000 01101101 01110100 01110110 01110010
 10000100 01100111 01111010 10010110 10000111
 10011000 10010001 01111010 01100010 01100011

00111101 10010100 11001001 10111010 01101110
 00001101 00001100 01101000 10101100 11000011
 10010000 10001000 01111011 00111100 00110111
 10010101 10010100 10011101 10100010 01101010
 10000110 01110111 01101000 01100100 01111000

Columns 6 through 8

01101011 01100110 01101111
 01110010 01011111 01010101
 01101010 01010100 01011000
 00111101 01100000 01001100
 11000100 11100110 10100110
 01110111 10100100 11100010
 01101000 01000101 00111101
 10010000 10001011 01100000

The binary code " 01000101, 01001011, 01001000 " is the letter " EKH " from ASCII.

Vignere Cipher Decryption Process

Cipher Text: EKH
 Key: ARA
 Plain Text: ETH

Cipher Text	E	K	H
Alphabet Position	5	11	8
key	A	R	A
Alphabet Position	0	17	0
Min	5	-6	8
PlainText	E	T	H

Figure 8 : Vignere Cipher Encryption Process

Caesar Cipher Decryption Process

Caesar cipher decryption:
 formula: $D(C) = P, P = C - K \text{ Mod } 26$ (3)

Cipher text: ETH

Key: 4

Plaintext: APD

ANALYSIS

The number of characters that can be inserted into the image is based on the size of the image. Here are 5 Images used for analysis.






No	Image	Resolution	Size
1		8x8 Pixel	248 Byte
2		9x9 Pixel	308 Byte
3		10x10 Pixel	376 Byte
4		11x11 Pixel	452 Byte
5		12x12 Pixel	488 Byte

Figure 9: Resolution and Size of Image

In this experiment, the image consists of five RGB images and five Grayscale images. After we find out how the dimensions of images, then we can calculate the number of words that are inserted into the images using the formula:

RGB Image Formula

$$(\text{pixel} \times \text{pixel} \times 3) / 8 \dots\dots\dots (1)$$

The number of characters that can be inserted into the image is based on the size of the image. Here are ten Images used for analysis. After calculations are finished, we'll get the graph of five RGB images and five Grayscale images,

The following is an analysis of data from a number of texts with the resolution of the image and the maximum text size to the size of the image.

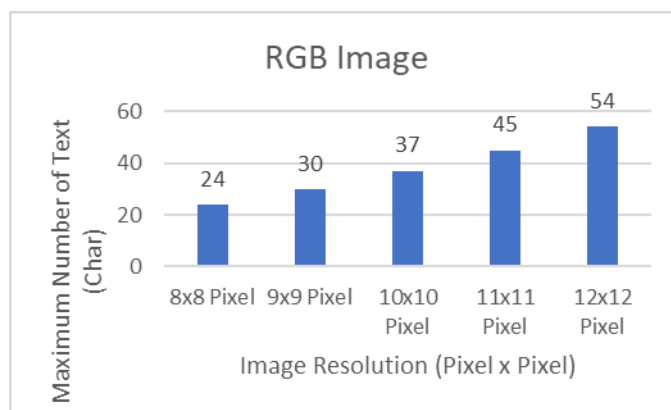


Figure 10: Maximum number of text that can be inserted into the RGB image

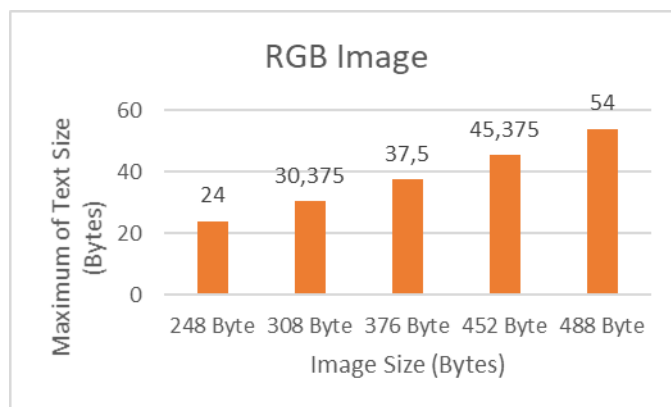


Figure 11: Maximum of text size that can be inserted into the RGB image

From the figure 10 and 11, the overall resolution of the larger image can be more inserted characters. It can be concluded The greater resolution of the image so more characters that can be inserted. From the analysis, it can be concluded that RGB image is better used for insertion process because RGB image can insert more character than Grayscale image.

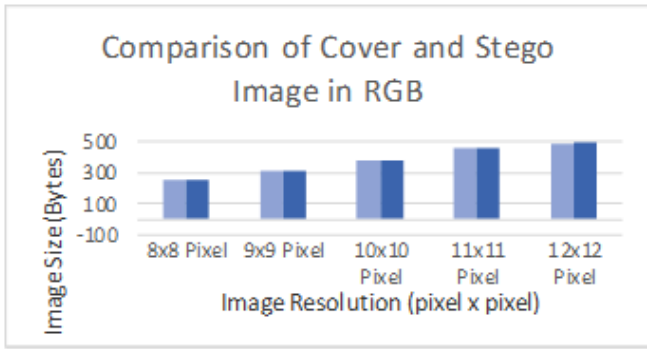


Figure 12: Comparison of Cover and Stego Image in RGB

From Figure 12, a comparison of the cover images as a whole the image size of the stego image is more large than the cover image.

Avalanche Effect

Avalanche effect is one way to determine whether or not a cryptographic algorithm, which will be known how big the changes which occurred in the ciphertext bits due to the encryption process. The greater the avalanche effect will the better cryptographic algorithms. How to calculate avalanche effect as follows:

$$Avalanche_Effect (AE) = \frac{\sum bit_change}{\sum bit_total} * 100\% \dots\dots\dots (4)$$

Plain text: APD

Cipher text: EKH

Avalanche_Effect = 100%

PSNR

Peak Signal to Noise Ratio (PSNR) is a comparison between the maximum value of the signal measured by the magnitude of the noise effect on the signal. The image is referred as the original source signal, and the noise is represented as error introduced after encoding. Although a maximum PSNR indicates that reconstruction of the image is up to its maximum quality. PSNR can be evaluated using the formula [17].

$$PSNR = 10 \log_{10} \left(\frac{C_{max}^2}{MSE} \right) \dots\dots\dots (5)$$






No	Image	Resolution	PSNR
1		8x8 Pixel	59,8584
2		9x9 Pixel	60,2599
3		10x10 Pixel	60,6315
4		11x11 Pixel	63,3499
5		12x12 Pixel	62,2151

Figure 13: The Result of PSNR

MSE

Mean Square Error calculates the difference between experimentally estimated value and true value, which signifies the loss in the quality or quantity of the image during the technique. In this case, the Mean square error is calculated for finding the quantity of deviation in pixel value after embedding the transformed data bits into it. The estimation of MSE (as shown in figure 14) showcases the quality change in the stego image, which has to be maintained in order to benefit the methodology. MSE is calculated by the formula [17].

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2 \dots\dots\dots (6)$$






No	Image	Resolution	MSE
1		8x8 Pixel	0,0677
2		9x9 Pixel	0,0617
3		10x10 Pixel	0,0567
4		11x11 Pixel	0,0303
5		12x12 Pixel	0,0394

Figure 14: The Result of MSE

No	Image Resolution	Image Type	Maximum number of text (Char)	Maximum of text size	Cover Image Size	Stego Image Size	PSNR	MSE
1	8 x 8 pixel	RGB	24	24 Bytes	248 Bytes	250 Bytes	59,8584	0,0677
2	9 x 9 pixel	RGB	30	30,375 Bytes	308 Bytes	310 Bytes	60,2599	0,0617
3	10 x 10 pixel	RGB	37	37,5 Bytes	376 Bytes	378 Bytes	60,6315	0,0567
4	11 x 11 pixel	RGB	45	45,375 Bytes	452 Bytes	454 Bytes	63,3499	0,0303
5	12 x 12 pixel	RGB	54	54 Bytes	488 Bytes	490 Bytes	62,2151	0,0394

Figure 15: The Result of Data

CONCLUSION

From the results of experiment and this analysis, then the conclusions to be drawn regarding the application of steganography with the method of Least Significant Bits, among others:

1. In comparison with a large number of characters, type the RGB image can be inserted more characters.
2. The size of the bitmap file after inserted character (Stego image) changes from the previous bitmap file size (Cover Image)
3. The larger image size, the more messages can be inserted
4. The integrity of the data before and after the process of extract does not change at all
5. The addition of cryptography in security messages then it is adding a level of security data text.

REFERENCES:

- [1] Karim Masud S.M, Rahman Saifur Md, Hossain Ismail md, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011) 22-24 December, 2011, Dhaka, Bangladesh.
- [2] Thangadurai K, Devi Sudha G, "An analysis of LSB Based Image Steganography Techniques", International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014.
- [3] Saha Abhisek, Halder Sholanki, Kollya Shama, "Image Steganography Using 24-Bit Bitmap Images", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011), 22-24 December, 2011.
- [4] Karthikeyan B, Deepak A, Subalakshmi K.S, M M Raj Anishin, "A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm", 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, 2017.
- [5] Thakur Ramesh Kumar, Saravanan Chandran, "Analysis of Steganography with Various Bits of LSB for Color Images", International Conference on Electrical, and Optimization Techniques (ICEEOT), 2016.
- [6] Arora Aman, Singh Manish Pratap, Thakral Prateek, Jarwal Naveen, "Image Steganography Using Enhanced LSB Substitution Technique", 2016 Fourth International Conference on parallel, Distributed and Grid Computing (PDGC), 2016.
- [7] Al -Afandy Khalid A, EL-Rabaie El-Sayed M, Faragallah Osama S, Elmalawy Ahmed, El-Banby Gh.M, "High Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography", 4th IEEE International Colloquium on Information Science and Technology (CiSt), 2016.
- [8] Bhatt Santhosi, Ray Arghya, Ghosh Avishake, Ray Ananya, "Image Steganography and Visible Watermarking using LSB Extraction Technique", IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO), 2015.
- [9] Akhtar Nadeem, Khan Shahbaaz, Johri Pragati, "An Improved Inverted LSB Image Steganography", 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014.
- [10] Chandramouli R, Memon Nasir, "Analysis of LSB based image steganography techniques", International Conference on Image Processing, Proceedings. 2001.
- [11] Bhukari Sadaf, Arif Shoaib Muhammad, Anjum M.R, Dilbar Samia, "Enhancing security of images by Steganography and Cryptography techniques", The Sixth International Conference on Innovative Computing Technology (INTECH), 2016.
- [12] Mishra Rina, Bhanodiya Praveen, "A review on steganography and cryptography", The International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015.
- [13] Saritha M, Khadabadi M. Vishwanath, Sushravya M, "Image and text steganography with cryptography using MATLAB", The International Conference on Signal Processing, Communication, Power and Embedded System (SCOPEs), 2016.
- [14] Jain Mamta, Lenka Kumar Saroj, "Digital Image Steganography using RGB Color Model: A Review", International Journal of Applied Engineering Research (IJAER).
- [15] Priyanka Kumari, Aritra Pal, Parth Dixit, Dr. A. Shanthini, "STEGANOGRAPHY USING DYNAMIC KEY GENERATION", International Journal of Advances in Engineering Research (IJAER) 2016, Vol. No. 11, Issue No. V.
- [16] Sriram, S, Karthikeyan, B, Vaithyanathan, V, Anishin Raj, M. M, "An Approach of Cryptography and Steganography using Rotor cipher for secure Transmission", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2015.

- [17] Shreyank N Gowda, “Innovative Enhancement Of The Caesar Cipher Algorithm For Cryptography”, International Conference on Advances in Computing, Communication, & Automation (ICACCA) 2016.
- [18] Fahrul Ikhsan Lubis, Hasanal Fachri Satia Simbolon, Toras Pangidoan Batubara, Rahmat Widia Sembiring, “Combination of Caesar Cipher Modification with Transposition Cipher”, Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 5, 22-25, 2
- [19] Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs, “Implementation of LSB Steganography and Its Evaluation for Various Bits”, 1st International Conference on Digital Information Management, 2006.
- [20] Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, “An improved method for LSB based color image steganography combined with cryptography”, 15th International Conference on Computer and Information Science (ICIS), 2016.