National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

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

Bhanupriya M, Shwetha B C, Sumana Bhat N M
Information Science and Engineering, GSSSIETW, Mysuru, Karnataka, India

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 the data in a digital image so that data transmitted cannot be identified by irresponsible parties. One of a kind of digital imageries that 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 how to insert cryptography messages into the low bits to the pixel data that make up a digital image file BMP. By developing a method of Steganography then sending the 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

I. 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.

The protect the copyright of digital image can be done by inserting messages of text, where the text contains information from the photography or owner of the digital image. One way to insert messages into digital image steganography techniques by.

Steganography is a technique used to hide data in 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. Steganography requires two properties. The first property is the container(cover) and the second is data that are hidden. One of the methods of steganography can be used to insert messages into digital imagery is a method of LSB is by way of inserting a bit messages into every last pixel bits of digital imagery.

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 symmetric key or public key or private key in cryptographic techniques can be form. This cryptography which will secure the messages to be inserted into digital image. After the message is secured with cryptography then the message will be posted on the digital image using steganography techniques.

II. METHODS AND MATERIAL

A.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.

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

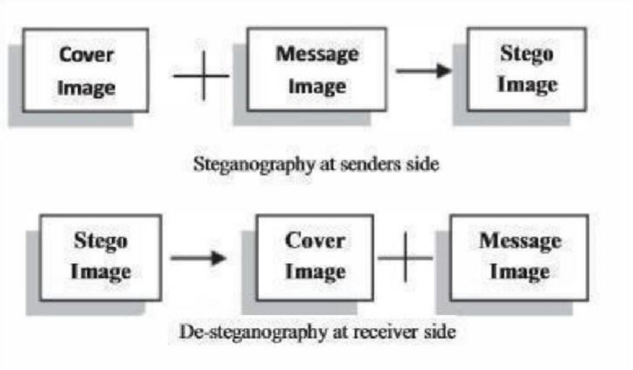


Figure 1: Encoding and Decoding Process

B. 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.

C. 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

D. 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 24bit 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).

In addition to the possibility of damage to information stored in file on the file changes due to stego , LSB steganography method also only able to store information with a very limited size. For example, a 24-bit image (R = 8-bit, 8bit 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 .

E. Algorithm for embedding data inside image

For the steganography algorithm, Fig.3 shows the algorithm for embedding the secret message inside the image. During the process of embedding the message inside the image, a secret key is needed for the purpose of retrieving the message back from the image.

From Figure 3, the secret message that is extracted from the system is transferred into text file first. Then the text file is compressed into the zip file. The zip text file then is used for converting it into the binary codes. The purpose of zipping the text file is because the zipped text file is more secured if compared with the file that is without the zipped.

The contents in the zipped file will significantly hard to be detected and read. Furthermore, this series of binary codes of the zipped text file and the key is a long random codes in which they only consist of one and zero figures. A data hiding method is applied by using this series of binary codes. By applying the data hiding method, the last two binary codes from the series are encoded into a pixel in image, then, next two binary codes are encoded to the next pixel in image, the process is repeated until all the binary codes are encoded. The secret key in this proposed steganography algorithm is playing an essential role where the key is acts as a locker that used to lock or unlock the secret message. For the data hiding method, each last two bit is encoded into each pixel in image. This will ensure the original image will not be tempered with too many changes.

```
Begin Input: Cover_Image, Secret_Message,Secret_Key;
Transfer Secret_Message into Text_File;
Zip Text_File;
Convert Zip_Text_File to Binary_Codes;
Convert Secret_Key into Binary_Codes;
Set BitsPerUnit to Zero;
Encode Message to Binary_Codes;
Add by 2 unit for bitsPerUnit;
Output: Stego_Image;
End
```

Figure 3. Algorithm for embedding data inside image.

F. Algorithm for retrieving data inside image

Once the message is hidden inside the image, this message can be extracted back from the stego image. Fig. 4 shows the algorithm for extracting the secret message from the stego image. In order to retrieve a correct message from the image, a secret key is needed for the purpose of verification.

From Figure 4, for the data extracting method, a secret key is needed to detect whether the key is match with the key that decodes from the series of binary code. Once the key is matched, the process continues by forming the binary code to a zipped text file, unzip the text file and transfer the secret message from the text file to retrieve the original secret message.

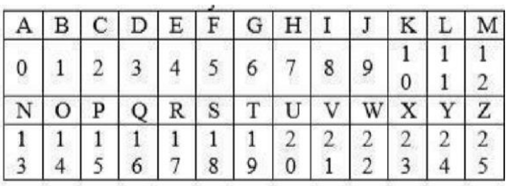
```
Begin
Input: Stego_Image, Secret_Key;
Compare Secret_Key;
Calculate BitsPerUnit;
Decode All_Binary_Codes;
Shift by 2 unit for bitsPerUnit;
Convert Binary_Codes to Text_File;
Unzip Text_File;
Output Secret_Message;
End
```

Figure 4. Algorithm for extracting data from stego image.

G. 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	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 5: The Order 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

H. 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 Each letter on the data or message paired with a letter at the specified keyword, and then do the encryption process that is encryption.

Vigenere Encryption Example :

Plain Text: PESAN INI SANGAT RAHASIA

Key: ARMADA

Cipher Text: PVEAQ INZ EAQGAK DAKA

III. RESULTS AND DISCUSSION

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.

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

(pixel x pixel x 3)/ 8 .... (1)

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 6: Resolution and Size of the Image

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

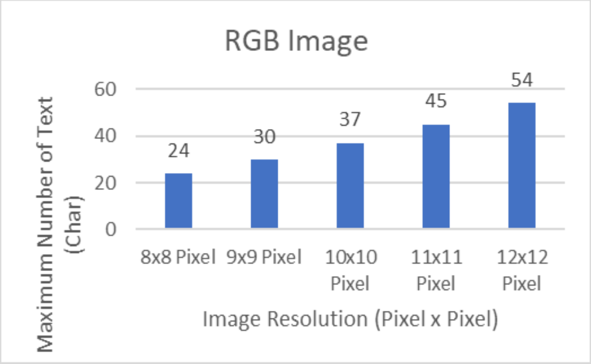


Figure 7: Maximum number of text that can be inserted into the RGB image

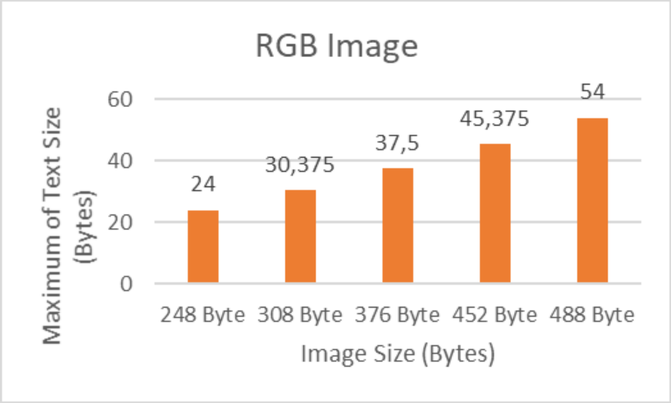


Figure 7: Maximum of text size that can be inserted into the RGB image

From the figure 6 and 7, 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 discussions, it can be concluded that RGB image is better used for insertion process because RGB image can insert more character than Grayscale image.

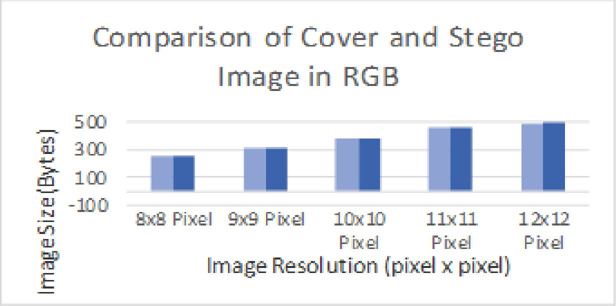


Figure 8: Comparison of Cover and Stego Image in RGB

From Figure 8, a comparison of the cover images as a whole the image size of the stego image is is more large than the cover image.

A. 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:

$$Avalanche\_Effect\ (AE) = \frac{\sum bit\_change}{\sum bit\_total} * 100\%$$

.... (2)

Plain text: APD

Cipher text: EKH

Avalanche_Effect = 100%

B. 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].

$$PSNR = 10\log_{10}\left(\frac{C_{max}^{2}}{MSE}\right) \text{ .... (3)}$$

C. 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 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].

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^{2} \text{ .... (4)}$$

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

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 9: Result of MSE

III. 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.

IV 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 201 I) 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. 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 201 I) 22-24 December, 2011, Dhaka, Bangladesh.
4. 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.
5. Saha Abhisek, Halder Sholanki, Kollya Shama, "Image Steganography Using 24-Bit Bitmap Images", Proceedings of 14th International Conference on Computer and Infonnation Technology (ICCIT 2011), 22-24 December, 2011.
6. 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 BioInformatics, 2017.
7. 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.
8. Arora Aman, Singh Manish Pratap, Thakral Prateek, Jarwal Naveen, " Image Steganography Using Enhanced LSB Subsitution Technique", 2016 Fourth Interntional Conference on parallel, Distributed and Grid Coumputing (PDGC), 2016.
9. Al -Afandy Khalid A, EL-Rabaie El-Sayed M, Faragallah Osama S, Elmhalawy 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.
10. 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.
11. 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.
12. Chandramouli R, Memon Nasir, "Analysis of LSB based image steganography techniques", International Conference on Image Processing, Proceedings. 2001.
13. Bhukari Sadaf, Arif Shoaib Muhammad, AnjumM.R, Dilbar Samia, "Enhancing security of images by Steganography and Cryptography techniques", The Sixth International Conference on Innovative Computing Technology (INTECH), 2016.

14. Mishra Rina, Bhanodiya Praveen, "A review on steganography and cryptography", The International Conference on Advances in Computer Engineering and Applications (ICACEA), 2015.

15. 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.

16. Jain Mamta, Lenka Kumar Saroj, "Digital Image Steganography using RGB Color Model: A Review", International Journal of Applied Engineering Research (IJAER).

17. 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.

18. Sriram, S, Karthikeyan, B, Vaithiyanathan, 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.

19. 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

20. Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 1st International Conference on Digital Information Management, 2006. 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.