International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1442-1452 www.ijaem.net ISSN: 2395-5252

Security Extensibility in steganography

Archan Dadhania Prof. Ami shah

[1]*College Student, Faculty of computer engineering,Student VIII SEM, B.E., Assistant Professor, Computer Science & Engineering, Institute of Technology & Management Universe, Vadodara, Gujarat India*

Submitted: 15-05-2021 Revised: 26-05-2021 Accepted: 28-05-2021

Abstract

Image Files are one among the foremost widely used file types today. This paper describes the utilization of JPEG image files in Steganography. Steganography is that the technique of hiding a message in a picture file (cover image) so as to not be known by people that don't have permission to access. This insertion utilizes the littlest little bit of pixel units in a picture file (Least Significant Bit). during this journal, steganography is going to be combined with AES. Steganography utilizes the weakness of the human eye in viewing the image file, steganography also uses mathematical calculations in inserting messages into the image file. this sort of insertion uses the binary of the ASCII code of a personality. This paper also compares the dimensions of a picture file to the dimensions of the knowledge which will be inserted.

Keywords: Steganography, LSB, F5, cover image, image, ASCII, AES

INTRODUCTION

Humans are social beings who always communicate with one another. some ways and sorts of communication made by humans. Everyone has their own interest in communicating sometimes they need to exchange tip.

At this point the sort of file that's fairly often used is a picture file. many sorts or image file formats are often used counting on the compression used. The JPEG format has become the foremost widely used format [2].

To solve the issues of human needs in exchanging tip, Steganography is employed as how to exchange information by utilizing the weakness of the human eye in viewing image files. The usable media isn't limited to image files, but also can are often applied to audio files and even video files. This method makes someone when watching a picture file, they're going to not realize that there's information hidden in it.

Steganography may be a method wont to insert or hide information into a media. The media are often image files, audio files, text files and video files [4].

Currently there are several techniques of steganography that are often to be used. Here are some commonly used techniques:

1. The substitution technique, by making a certain pixel replacement of the cover image. An example method is LSB.
2. Transform Domain Techniques, by storing confidential information through space transformation. An example of his method is DCT (Discrete Cosine Transform).
3. Spread Spectrum Techniques, In this technique the secret information is stored and spread in a certain frequency.
4. Statistical Techniques, the data is encoded with this technique through the conversion of some statistical information from the file container. The file container for the block where each block holds a hidden secret pixel.
5. Distortion Techniques, hidden information based on signal distortion.
6. Cover Generation Techniques, this technique hides confidential information that fits the cover [8].

STEGANOGRAPHY

Steganography may be a technique of inserting information during a media, which may be image files, sound files or video files [3]. this system aims to send information between the sender and therefore the recipient unnoticed by others.

There are criteria on steganography:

1. Fidelity: Image quality of the container doesn't change much after the addition of secret data.
2. Imperceptibility: The existence of data can't be seen with the human eye.
3. Recovery: Information that has been inserted are often re-issued to read [6].Some terms related to steganography:

1. Embedded message: hidden message.
2. *Coverobject*: object used to hide embedded message
3. *StegoImage*: object containing embedded message.

IMAGE STEGANOGRAPHY

Image steganography is steganography that uses image as a cover-file within the process of inserting secret messages to get stego-image. The technique of insertion of data into images isn't an equivalent for every cover-file used, because it refers to the character of various file cover [6].

Here is a simple illustration of the steganography process in Figure 1

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1442-1452 www.ijaem.net ISSN: 2395-5252

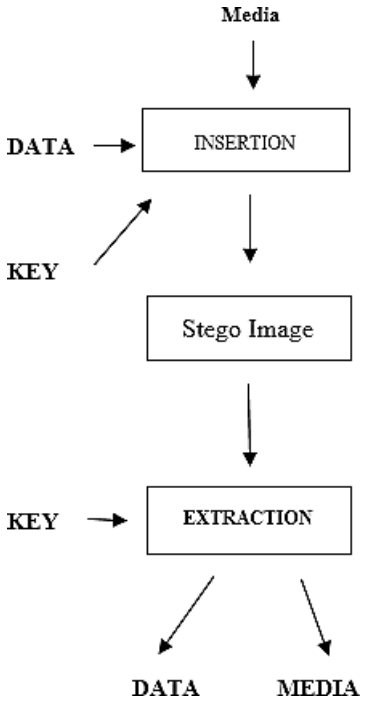


Figure 1: Steganography Process.

To perform a steganography technique, it takes two media aspects within the sort of media container and knowledge to be hidden. many of us use steganography through computer, because many digital files are often used as media container to cover message.

Some examples of media that can be used in the insertion of information with steganography techniques:

1. Text
2. Audio
3. Image
4. Video [4]

JPEG IMAGE

Joint Photography Expert Group (JPEG), is one among the compression schemes of bitmap files. Because bitmap may be a file that features a large size that causes not practical. So, with the existence of this compression scheme files that originally large size become smaller and practical use.

Since the mid-1980s ITU and ISO worked together in developing the International Standard for compression techniques.

Officially, JPEG may be a standard and is listed in ISO / IEC international standard 10918-1: digital compression and coding of continuous-tone still images [2].JPEG has 2 classes in the encoding and decoding process:

- Lossy Process
- Lossless Process [2]

VIGENERE

Vigenere chiper is a cryptography technique which were explained first by Giovan Batista belaso in his book entitled La cifra del. Sig. Giovan Batista belaso (1553). Then the password is enhanced by a French diplomat, Blaise de Vigenere (1586). Vigenere code includes alphabetic code-compound (polyalphabetic substitution cipher). Techniques to produce chiper text can be done using a substitute number and Vigenere table. Vigenere technique using numbers performed by exchanging letters with numbers, similar to the slide code. This method uses a vigenere squares that can be seen on figure 2 [11].

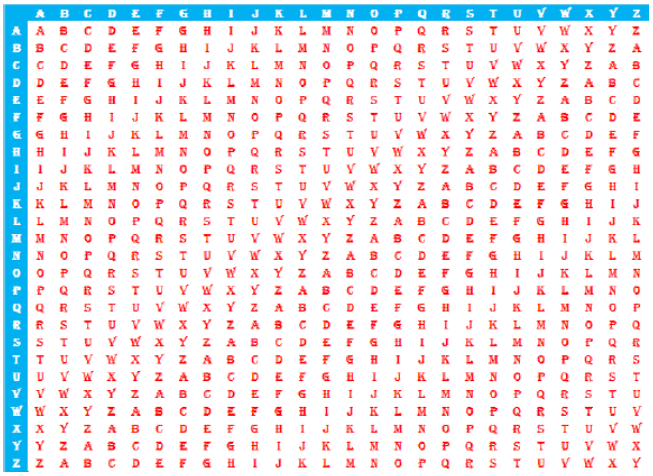
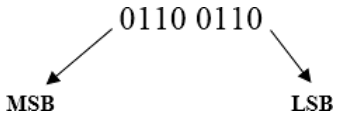


Figure 2. vigenere Table

LSB (LEAST SIGNIFICANT BIT)

Least Significant Bit is one among technique in steganography. LSB may be a widely used as steganography algorithm [5]. LSB utilizes the proper far little bit of the byte array that structure pixels in a picture file. within the order of bits during a byte, there are bits called LSB and a few are called MSB.



Steganography technique using Least Significant Bit (LSB) modification method is that the simplest technique, simple approach to insert information during a digital image (medium cover). Convert a picture from GIF or BMP format, which reconstructs an equivalent message because the original (lossless compression) to JPEG that's lossy compression, and when it's done it'll destroy the hidden information within the LSB [13]. The LSB bit becomes the place where the bit value of the binary arrangement of an information is inserted, because the change within the value only changes 1 bit higher or 1 bit less than the previous value. So, when the byte values change, the changes that occur within the pixel won't be too meaningful. The LSB algorithm utilizes the weakness of the human eye to ascertain very small color changes.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1442-1452 www.ijaem.net ISSN: 2395-5252

The number of pixels and color depth of a picture file will affect the quantity of data which will be inserted within the image file.

The insertion of data in a picture using the LSB algorithm are going to be illustrated as follows:

A 3x3 pixel Grayscale image will be inserted an information is character 'a'.

a = 0110 0001

and here are 3 x 3 images represented in binary numbers.

11010011	11000010	01000011
10110110	10101100	11001011
11101001	11010011	10101000

Then the byte of character 'a' will be inserted on the lsb of each pixel in the image.

11010010	11000010	01000010
10110111	10101100	11001011
11101001	11010010	10101000

Figure 3. Inserting binary message to image pixels

From the Figure 3, simple illustration is often seen that the insertion of data within the sort of characters that are shaped binary based ASCII.

ASCII

ASCII is a world standard in information exchange. This standard is employed by computers to represent a personality. ASCII code features a composition of binary numbers of 8 bits. ranging from 00000000 to 11111111 with a complete combination of 256.

DISCUSSION

If this implementation is completed, the system will have some specifications*:*

a. Can do steganography and encryption with AES process either insert messages or do extraction to urge the message.

b. Can calculate the file size after the steganography process

Experiment encryption using AES.

It is known that the plaintext we will encrypt using AES with the keys we specify. The work process is as follows:

Plaintext: aku

Key : ba

Do as follows:

Plaintext: aku

Key: bab

How to get cipher text from plaintext 'aku' is by watching AES table (figure 2). With the letters on the plaintext being rows, and therefore the letters on the key into columns.

then,

Chipertext: bkv

Experiment of Insertion and Extraction Methods

We will experiment with the insertion and extraction of messages during a Grayscale and RGB image file.

The encoding process in Grayscale Image 5 x 5

Given an Grayscale image has the following size 5 x 5 pixels

The pixels of the JPG image are shown on Illustration 2 :

10100010	01111000	10100010	10100011	10011001
01100100	01001010	01101011	01011001	00110110
01111011	01101111	10000001	01010111	10110011
01100110	01101010	10000111	01111011	11001101
10111001	10110111	10100010	10100111	10011000

Figure 4. Pixels from example grayscale image

From the Figure 4, we can know that:

- The size of the image resolution is 5 x 5 pixels = 25
- There are 1 bytes each pixel. 25 x 1 = 25 bytes
- Each message / character information (ASCII) requires 8 bits.
- Each bytes can be inserted 1 bit from message bits.
- Then the maximum number of messages that can be inserted is 3 characters.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1442-1452 www.ijaem.net ISSN: 2395-5252

In this experiment we'll insert a cipher text from AES 'bkv' character that has binary 01100010 01101011 01110110

1010001**0**	0111100**0**	1010001**1**	1010001**1** 1001100**0**
0110010**1**	0100101**1**	0110101**0**	0101100**0** 0011011**1**
0111101**1**	0110111**0**	1000000**1**	0101011**1** 1011001**1**
0110011**0**	0110101**0**	1000011**0**	0111101**1** 1100110**0**
1011100**0**	1011011**1**	1010001**1**	1010011**1** 1001100**0**

Figure 5. Inserting Binary of encrypted message

There is alittle change to the binary above. Which if formed in a picture won't be seen directly by the human eye.

The process of decoding in Grayscale Image 5 x 5

From the encode experiment we get an image with binary digits as follows.

1010001**0**	0111100**0**	1010001**1**	1010001**1** 1001100**0**
0110010**1**	0100101**1**	0110101**0**	0101100**0** 0011011**1**
0111101**1**	0110111**0**	1000000**1**	0101011**1** 1011001**1**
0110011**0**	0110101**0**	1000011**0**	0111101**1** 1100110**0**
1011100**0**	1011011**1**	1010001**1**	1010011**1** 1001100**0**

To decode, the message is taken from the last bit value of the binary of a picture. And if converted again binary 01100010 01101011 01110110 supported ASCII is character 'bkv'.

The encoding process on RBG Image 4 x 4

Given an RGB image has the following size 4x4 pixels.

Here is that the pixel arrangement of the JPEG image. Because the image file may be a RGB image. The pixels will form 3 layers which will be seen on Figure 6.

Red

10110001	01111011	10100000	10101101
01011110	00111100	01111101	01110000
01011111	01110101	10001101	01001101
01111001	01111000	10000001	10000101

Green

10011100	01111010	10101010	10110101
01101111	01001001	01110100	01011110
01101111	01110001	10001010	01000100
01101111	01101001	01101111	10000001

Blue

10001001	01011100	01001001	01011111
10001011	01010010	01100101	01001000
01111100	01110000	10011011	01011001
01100011	01100010	01100001	10000010

Figure 6. Pixels from example RGB Image

From the Figure 6 we can know that:

- The size of the image resolution is 4 x 4 pixels = 16
- There are 3 bytes each pixel. 16 x 3 = 48 bytes
- Each message / character information (ASCII) requires 8 bits.
- Each bytes can be inserted 1 bit from message bits.
- Then the maximum message that can be inserted is 6 characters.

In this experiment we will insert a 'a' character that has binary 01100001

Red

1011010**0**	0101101**0**	10101000	10111001
0101101**1**	0001110**0**	01110101	01100100
0101111**1**	0110010**0**	10001111	01011101
0111110**0**	0101100**1**	10001101	10010101

Green

10011100	01111010	10101010	10110101
01101011	01001101	01110110	01011110
01101011	01110101	10001110	01000100
01101011	01101001	01101111	10000001

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1442-1452 www.ijaem.net ISSN: 2395-5252

Blue

10001001	01011100	01001001	01011111
10001011	01010010	01100101	01001000
01111100	01110000	10011011	01011001
01100011	01100010	01100001	10000010

Figure 7. Inserting Binary Message

Binary code has slightly changed.

The decoding process on RBG Image 4 x 4.

From the encode experiment we get an image with binary digits as follows.

Red

1011000**0**	0111101**0**	10100000	10101101
0101111**1**	0011110**0**	01111101	01110000
0101111**1**	0111010**0**	10001101	01001101
0111100**0**	0111100**1**	10000001	10000101

Green

10011100	01111010	10101010	10110101
01101111	01001001	01110100	01011110
01101111	01110001	10001010	01000100
01101111	01101001	01101111	10000001

Blue

10001001	01011100	01001001	01011111
10001011	01010010	01100101	01001000
01111100	01110000	10011011	01011001
01100011	01100010	01100001	10000010

To decode, the message is taken from the last bit value of the binary of a picture and if converted again, binary 01100001 supported ASCII is that the character 'a'.
In this RGB image experiment the message is only inserted on the Red layer.

ANALYSIS

From the experiments and calculations performed the following is a chart that shows the number of characters that can be inserted from each image.

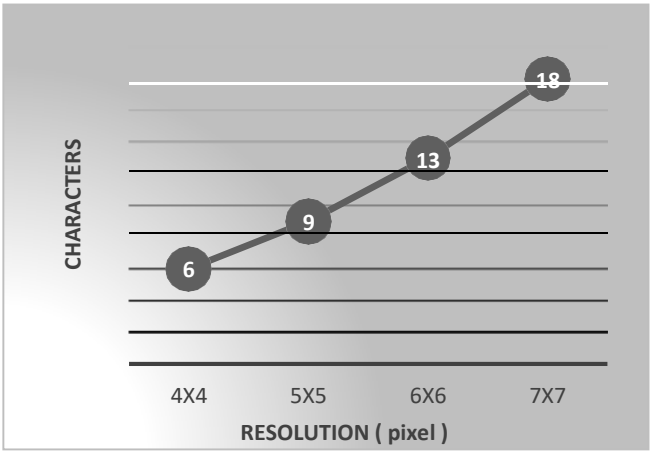


Figure 8. Image resolution and number of characters on RGB image

Figure 8 is shown the relationship between resolution and color depth (RGB) of an image file determines the number of characters that can be inserted.

The formula used to calculate the maximum number of characters exists with the following equation

$$\text{Char} = \frac{(\text{Vertical pixel x horizontal pixel}) \text{ x } 3}{8} \qquad (1)$$

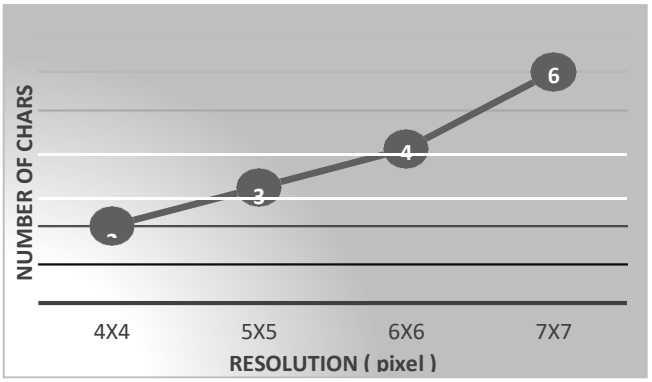


Figure 9. Image resolution and number of characters on grayscale image

Figure 9 is shown the relationship between resolution and color depth (Greyscale) of an image file determines the number of characters that can be inserted.

The formula used to calculate the maximum number of characters exists with the following equation.

$$\text{Char} = \frac{(\text{Vertical pixel x horizontal pixel}) \text{ x } 1}{8} \qquad (2)$$

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1442-1452 www.ijaem.net ISSN: 2395-5252

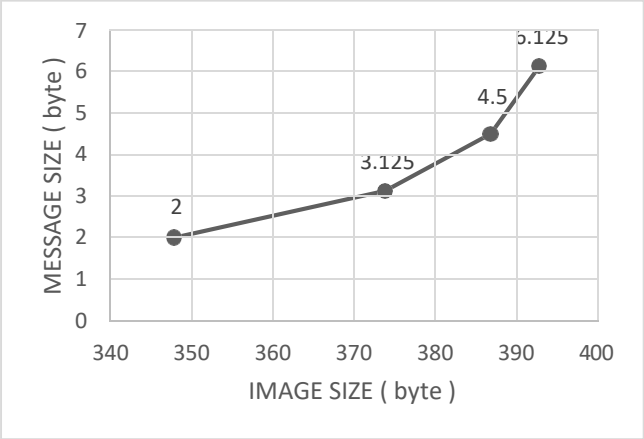


Figure 10. Image Size with Message Character Grayscale

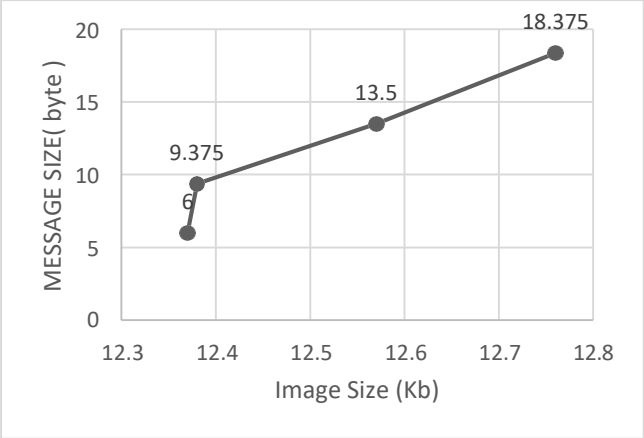


Figure 11. Image Size with Message Character RGB

The two graphs on figure 10 and 11 are graphs showing the dimensions of an information which will be inserted in bytes and therefore the size of the experiment cover image.

From Figure 8 and Figure 9 we will see that the greater the resolution of a picture, the greater number of character information which will be inserted. and can be directly proportional thereto seen from figure 10 and figure 11 the larger the resolution size of a picture , the larger size of the characters which will be inserted.

The Table 1 shows all data obtained in experiments performed on 4x4, 5x5, 6x6 and 7x7 images with 3 bytes color depth (RGB).

The Table 2 shows all the data obtained in experiments performed on 4x4, 5x5, 6x6 and 7x7 images with 1 byte color depth (Grayscale).

Table 1. Data Result RGB

No	Dimensions	Image Type	Max Number of Characters	Maximum Character	The size of the initial image (cover image)	Stego Image
1	4 x 4 pixel	RGB	6	6 bytes	12.37 Kb	12.37 Kb
2	5 x 5 pixel	RGB	9	9.375 bytes	12.38 Kb	12.38 Kb
3	6 x 6 pixel	RGB	13	13.5 bytes	12.57 Kb	12.57 Kb
4	7 x 7 pixel	RGB	18	18.375 bytes	12.76 Kb	12.76 Kb

Table 2. Data Result Grayscale

No	Dimensions	Image Type	Max Number of Characters	Maximum Character Size	The size of the initial image (cover image)	Stego Image Size
1	4 x 4 pixel	Greyscale	2	2 bytes	348 bytes	349 bytes
2	5 x 5 pixel	Greyscale	3	3.125 bytes	374 bytes	375 bytes
3	6 x 6 pixel	Greyscale	4	4.5 bytes	387 bytes	388 bytes
4	7 x 7 pixel	Greyscale	6	6.125 bytes	393 bytes	393 bytes

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1442-1452 www.ijaem.net ISSN: 2395-5252

CONCLUSIONS & FUTURE RESEARCH

From all the experiments that have been made to JPEG image by using LSB can be listed the conclusion as follows:

a. LSB is one technique that can be used to insert information in an image.

b. The size of the message does not exceed the size of the cover image.

c. The larger image resolution, the larger message or information can be inserted.

d. RGB images can hold more information or messages than with Grayscale images of the same resolution.

e. The data previously encrypted using AES after extracted from the stego image will then be processed again.

f. Differences in the use of AES encryption is when the message before it is inserted (plaintext) and after it is extracted (ciphertext). In the insertion process is the same as the usual LSB method.

Future research is predicted to use cryptography not only limited to at least one method only. Rather it are often applied some cryptographic methods that make messages or information safer albeit messages embedded during a media are often extracted by irresponsible parties, but the knowledge they really get isn't actual, but the encrypted information.

REFRENCES

[1]. K. Stefan, P. Fabien A.P., “Information Hiding Techniques for,Steganography and Digital Watermarking” , Artech House , London, 2000.

[2]. Cox, Ingemar J., “Digital Watermarking and Steganography”, Burlington, Morgan Kaufmann Publisher, 2008.

[3]. Wahyuningsih Sri , Theodora V.D Pandex, Vanessa Stefanny, “Implementasi Visible Watermarking Dan Steganografi Least Significant Bit Pada File Citra Digital”, Universitas Budi Luhur (INdonesia), September 2, 2016, pp. 140-145.

[4]. Jassim, Firas A., "A novel steganography algorithm for hiding text in image using five modulus method", arXiv preprint arXiv, Vol. 72, No. 17, PP. 39-44, 2013.

[5]. J.C. Ingemar, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, “Digital watermarking and steganography”, Burlington: Morgan Kaufmann; 2008..

[6]. Pamungkas, Friski Gatra. 2017. “Implementasi Teknik Steganalisis Menggunakan Metode Improvement Difference Image Histogram Pada Steganografi”. Skripsi. Universitas Telkom Bandung.

[7]. Mulyono, Ragil. 2015. “Pengamanan Pesan Text menggunakan Metode Steganografi Least Significant Bit dengan Media Digital Gambar”. Jurnal. Universitas Dian Nuswantoro Semarang.

[8]. A Hakim Muhammad, “Studi dan Implementasi Steganografi Metode LSB dengan Preprocessing Kompresi data dan Ekspansi Wadah “, 2016. .

[9]. Arora Aman, Singh Manish Pratap, Thakral Prateek, Jarwal Naveen, “ Image Steganography

[10]. Using Enhanced LSB Subsitution Technique”, 2016 Fourth Interntional Conference on parallel, Distributed and Grid Coumputing (PDGC), 2016

[11]. Thakur Ramesh Kumar, Saravanan Chandran, “Analysis of Steganography with Various Bits of LSB for Color Images”, International Conference on Electrical, and Optimization Techniques , 2016.

[12]. Chyquitha Danuputri, Teddy Mantoro, Mardi Hardjianto, “Data Security Using LSB Steganography and AESChiper in Androi Environtment”, Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic, 2015.

[13]. Monica, F Monica, F., & Surahman, A. (2016). Aplikasi Steganografi Pada Citra Digital Menggunakan Metode LSB (Least Significant Bit) Visual Basic 6.