"A Secure and Adaptive Approach for Image Steganography Using Data Inversion Technique"

Garima Agarwal, Vibor Agarwal* and Himanshu Sharma **
Dept. of Computer Science,
MACET, Gajraula, U.P., India.
* Senior Software Engineer
Mahindra Satyam, Hyderabad , India
**Dept. of Computer Science,
IFTM University, Moradabad, U.P., India.

Email: garimatalk2@gmail.com, vibhor.miet@gmail.com, cs.himanshu@gmail.com

Abstract:

Everyday day in life, the interpretation of sending the message secretly is difficult task. For sending any message secretly to another person we use steganography technique. It is the technique to hide furtive information in some other data without leaving any evidence of data adjustment. This technique consist of multifunctional program ,which sort out various problems like implementation of steganographic algo to hide the data in image file .Security for data broadcast is the most fundamental matter in modern communication system. We have discussed a new steganographic method. The effectiveness of the projected process is described through which plan of better security of data can be achieved. To hide data in a binary image, no key is needed relatively this algorithm is based on number of occurrence of 0s and 1s in data that has to hide and number of occurrence of 0s and 1s in the last bit of each pixel of binary image file. The algorithm assures the defense and the data hiding effect is relatively hidden. The security of the transformation of hidden data can be obtained by two ways: encryption and steganography. A combination of the two techniques can be used to increase the data security.

Keywords: Pixel, DataHiding, Encryption, Decryption

1. Introduction

Steganography" is a Greek origin word which means "hidden writing". Steganography word is divided into two parts: Steganos which means "secret or covered" (where you want to conceal the secret messages) and the graphic which means "writing" (text). However for hiding information the meaning of Steganography is hiding text or secret messages into another media file such as image, text, sound ,video.

Steganography ancient origins dates back to 440 BC. It was started by the Greeks by shaving the slaves hair heads and writing the message on their heads, after the hair had been grown, they were sent to their supporters in order to converse with them without the enemies awareness. As well as, the imperceptible ink used for hiding the secret messages by the American rebels during the

United States Revolution. Also it was used in both World Wars by German armed forces. Another Steganography technique is the Spam Mimic software which developed by Wayner in (2003), this software was developed to detect and hide the secret messages in text file based on set of code of behavior.

The intention behind developing image Steganography methods according to its use in various organizations to communicate between its members and it can be used for communication between participants of the military or intelligence operatives or agents of corporations to hide secret messages or in the field of reconnaissance. The main objective of using the Steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any modification in the sent message then this viewer will try to know the hidden information inside the message.

The main terminologies used in the Steganography systems are: the cover message, secret message, secret key and implanting algorithm. The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the info which is needed to be concealed in the suitable digital media. The secret key is usually used to insert the message depending on the hiding algorithms. The embedding algorithm is the way or the idea that is typically used to embed the secret information in the cover message.

In steganography, the potential cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information secreted and may be plain-text, cipher text, images, or whatsoever that can be embedded into a bit stream. Both the cover carrier and the embedded message form a stego-carrier. Hiding information may involve a stego key which is extra secret information as password required for embedding the information. For example, when a secret note is hidden within a cover image, the subsequent product is a stego-image.

A possible formula of the process may be represented as:

cover medium + embedded message + stego key = stego-medium .

Graphical Version of the Steganographic System

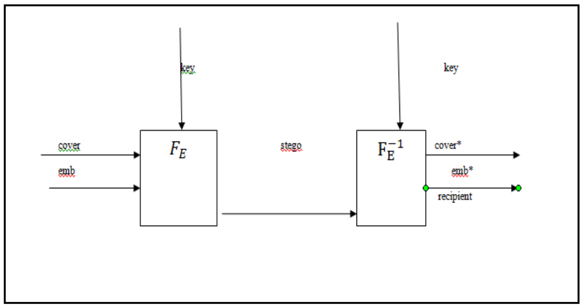


Fig 1: Generic Steganography Sceheme

fE : steganographic function "embedding"
fE-1 : steganographic function "extracting"
cover: cover data in which emb will be hidden
emb: message to be hidden
stego: cover data with the hidden message.

I. AIMS

The aims of this paper are three which are as follows :

i. To investigate the strength and limitations of current steganography schemes ,
ii. to mask the very presence of communication making the true message not apparent to the observer .
iii. To evaluate the new methods using application scenarios of copyright protection, security and authentication.

2. EVALUATION OF DIFFERENT STEGANOGRAPHIC TECHNIQUES

There are many techniques of steganography which are used , So through the following parameters we differentiate between them .

These parameters are as follows:

• Undetectability (imperceptibility): this parameter is the first and the primary requirement; it represents the ability to avoid detection, i.e., where the human eye fail to notice it. However, the techniques that do not alter the image in such a way to be perceptible to the human eye may still alter the image in a way that it is detectable by the statistical tests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.

• Robustness: it is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation (like cropping or rotating), data compression, and image filtering. Watermarks are an example of a robust steganographic technique.

• Payload capacity: it is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully. When compared with watermarking, that requires embedding only a small amount of copyright information, steganography is seen to hide communication and consequently a sufficient embedding capacity is required. Accordingly and by using this parameter, small amounts of data could be hidden without being detected by the human eye. Larger amounts of information, on the other hand, may detect artifacts by the HVS or statistical tests. The following paragraphs compare the previously mentioned steganographic techniques in terms of the competing parameters.

• LSB technique in the spatial domain is a practical way to conceal information but, at the same time, it is vulnerable to small changes resulting from image processing or lossy compression . Although LSB techniques can hide large quantities of information i.e., high payload capacity, they often compensate the statistical properties of the image and thus indicate a low robustness against statistical attacks as well as image manipulation.

• The promising techniques such as DCT, DWT and the adaptive steganography are not tended to attacks, especially when the hidden message is small. This can be justified in relation to the way they change the coefficients in the transform domain, thus, image distortion is kept to a minimum. Generally speaking, such techniques tend to have a lower payload when they are compared to the spatial domain algorithms . The experiments on the discrete cosine transform (DCT) coefficients have introduced some promising results and then they have diverted the researchers’ attention towards JPEG images. Working at some level like that of DCT turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding, especially in terms of compression survival .

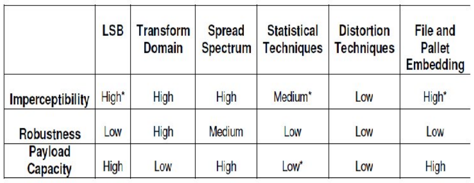
• Spread spectrum techniques are generally quite robust against statistical attacks, since the hidden message is spread throughout the image. However, a determined attacker is capable of compromising the embedded data using some digital processing, such as noise reduction filters, which are similar to the ones used in the decoding process to estimate the original cover. Spread spectrum encoding is extensively used in military communications due to its robustness against detection. When a message is embedded, an attacker cannot be easily recognized and it will be difficult to extract it without knowing the suitable keys. SISS is very good for steganography because of the reasonable high capacity and high difficulty proposed in the process of detection and extraction .

• The statistical techniques in most cases are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. Defenses could be considered to make the statistical techniques as robust as the watermarking scheme. The payload capacity and invisibility depends on the cover image selected.

• Unlike many LSB methods, distortion techniques do not upset any statistical properties of the image. In contrast, the need to send the cover image over a secure channel limits the worth of this technique. As in any steganographic technique, the cover image should never be used more than one time. If an attacker alters the stego-image by cropping, rotating, or scaling, the alteration can easily be perceived by the receiver and can fairly be reversed to the point where the message encoded with error correcting information can be fully recovered. Error correcting information also aids if the stego-image is filtered through a lossy compression scheme such as JPEG. Adopting this technique limits the hidden information capacity, since adding distortion to the cover image is the basis of embedding algorithm. As a result, the distorted image will be more vulnerable to the HVS.

• Techniques that modify image file formatting information have the following drawbacks: they have a large payload; however, they are easily detected and defeated; they are not robust against lossy compression and image filters, and the issue of saving the image one more time totally breaks the hidden data .

• Hiding information via steganographic techniques that modify the elements in the visual image results in a stego picture that will survive rotation, scaling and much lossy compression like JPEG. A reasonable payload capacity can be achieved with this technique as well. Table 5. 1 summarizes the evaluation of the mentioned techniques.



	LSB	Transform Domain	Spread Spectrum	Statistical Techniques	Distortion Techniques	File and Pallet Embedding
Imperceptibility	High*	High	High	Medium*	Low	High*
Robustness	Low	High	Medium	Low	Low	Low
Payload Capacity	High	Low	High	Low*	Low	High

Table 5.1 A comparison to image steganograhy technique

2. PROPOSED METHOD

The primary aim is to build an secure stego System that would affect visuality of the image so little that it is impossible to notice any change in image by human being eye interpretation. Here we take an image file where each pixel is represented by RED , GREEN & BLUE components of an image that define color of that pixel .

So pixel can be represented as

R	G	B
10010101	**00001101**	**11001001**

Whole image is viewed as the format of RGB components .

4. SECURE STEGO SYSTEM

The secure stego system is divided into three main stages : Cryptographic stages , Three component implementation and Single Component Implementation (only B). The description of each part is represented as follows . The overall system describes all three parts as the figure is illustrating below:

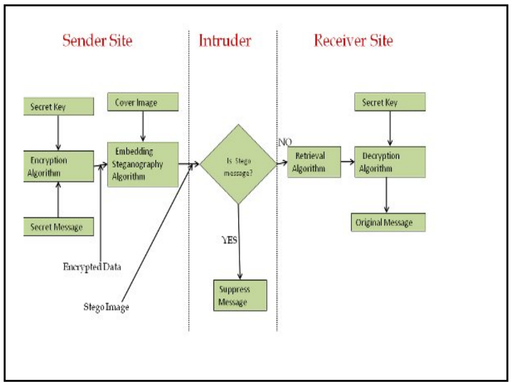


Fig 3: System Representation

4.1 Cryptographic Stage

For providing confidentiality by using key . In this part of the system the key first encrypt the data before hiding into the image for the high security. We X-OR the data with the key and if key is shorter than the message we repeat the key until the length of the message and then take the X-OR.

At the receiving side of our system perform the X-OR between key and the decrypted data to get the original one .

4.2 Three Component Implementation (RGB)

In this stage we hide the data in al three component of the image means Red ,Green and Blue . When this part of the algorithm is executed on the window it show the browse option to choose the image to hide the data then it will ask the key and secret data for hiding . After clicking on the hiding data option user save the stego image which is modified .

For getting the original data user have to click at extract button and insert the stego image with same key .

4.3 Single Component Implementation (only B)

In this stage we hide the data in single component of the image means blue . When this part of the algorithm is executed on the window it show the browse option to choose the image to hide the data then it will ask the key and secret data for hiding . After clicking on the hiding data option user save the stego image which is modified .

For getting the original data user have to click at extract button and insert the stego image with same key .

4.4 Algorithm:

1) Read the characters from the data file to be sent and convert the ASCII value of the characters into equivalent 8 bit binary representation and produce the blocks of 16 bits.

2) Encrypt each block using the secret key and produce encypted from tha data.

3)Calculate how many 0's and 1's are present in each block and save the cumulative sum into two integer variables suppose g0 and g1 which holds total number of 0's and 1's correspondingly. Repeat the step above for each block and find the values of g0 and g1 for each block.

4) From the image file , Read the RGB colour of each picture element (Pixel).

5) Read the last bit of each pixel from RGB 8+8+8 bits and read the blue colour 8 bits .

6) Now test for the last bit is 0 or 1 and store the result in two integer value a0 and a1.

7) If (a0>a1) and (g0>g1) or (a1>a0) and (g1>g0) then set the FLAG to 0 else set the FLAG value to 1.

8) Calculate FLAG for each block separately

Update the blocks –

If FLAG = 0 , we donot invert the bits of the block .

If FLAG =1 , we invert the bits of the block .

5. RESULTS

5.1Experimental Results

The algorithm is implemented and tested at random, one such example is explained here :

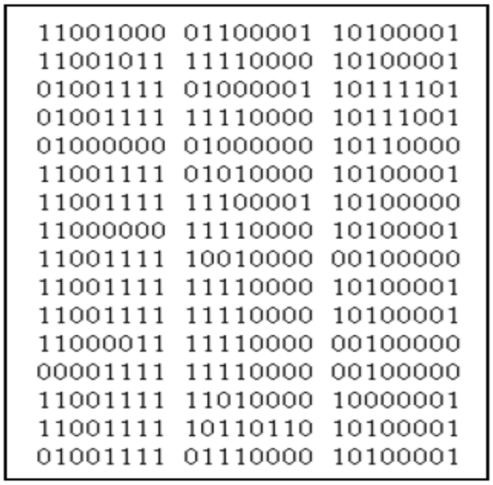
5.1.1 At sender site

Data File to be embedded : 01000100 00111000

Total number of 0s at data bit stream a0 =12

Total number of 1s at data bit stream a1= 5

Suppose the pixel information of RGB color of 16 pixels is as Table7.1



11001000	01100001	10100001
11001011	11110000	10100001
01001111	01000001	10111101
01001111	11110000	10111001
01000000	01000000	10110000
11001111	01010000	10100001
11001111	11100001	10100000
11000000	11110000	10100001
11001111	10010000	00100000
11001111	11110000	10100001
11001111	11110000	10100001
11000011	11110000	00100000
00001111	11110000	00100000
11001111	11010000	10000001
11001111	10110110	10100001
01001111	01110000	10100001

Table 5.1 Cover image

Here g0=5
Here g1=11

According to the algorithm
a0 = 12
a1 = 5
c0 = 5
c1=11
Here a1>a0 but g1>g0
Flag value will set to be 1 .
So data bits would be change and it would be as follows
Data File : 01000100 00111000
Inverted data file : 10111011 11000111

Table 5.1 will show the stego file without inverting data

10100000
10100001
10111100
10111000
10110000
10100001
10100000
10100000

00100000
10100000
10100001
00100001
00100001
10000000
10100000
10100000

Table 5.1 Stego file blue pixels with LSB algo

Number of bits changing without inverting data block =10

Table 5.2 will elaborate the stego file with modified algorithm.

FLAG

1010001**1**1
10100000
10111101
10111001
10110001
10100001
10100001
10100001
00100001
10100001
10100000
00100000
00100000
10000001
10100001
10100001

Table 5.3 Stego file with modified algorithm

Number of bits change using proposed system with inverting data =6

5.2 .2 At Receiver End

First Pixel’s bit before the last bit has been read and checkflag is detected as 1,
Reading the last bit of 16 pixel the which is data retrieved as follows:
10111011 11000111
Now according to checkflag’s data above value is inverted and finally original data has been retrieved that is 01000100 00111000
Visual effects also considered and checked which are explained here under –

Fig. 5.1 Simple Image

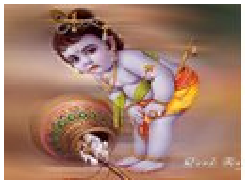


Fig. 5.2 Stego Image

CONCLUSION

The secure stego system developed is capable of sending the data with to another medium with security and affecting the quality of picture little .The system developed is capable of data into an image file . The message can then be extracted only by the same system running either on same system or different system. The key should be known to the receiver in order to extract correct message . This is the enhancement of security.

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the presence of a secret. Digital image steganography and its derivatives are growing in use and application. In fields where cryptography and strong encryption are being forbidden, citizens are looking at steganography to circumvent such policies and pass messages secretly. As with the other great innovations of the digital age: the battle between cryptographers and cryptanalysis, security experts and hackers, records, companies and pirates, steganography and Steganalysis will recurrently develop new techniques to counter each other.

ACKNOWLEDGMENT

We take this opportunity to express our sincere thanks and deep gratitude to the authors who extended their whole-hearted co-operation and have helped us in completing this research work successfully.

FUTURE DIRECTIONS

Stronger encryption algorithm (like RSA)could be applied to provide additional security . We can compress the data before embedding it into carrier file so as more data can be hidden in picture . We can select random pixels in the image for hiding the data so as to make brute force attack more feasible. We can concentrate more on internal structure of the image and try to find out the segments where if hidden , data will be least visible.

The proposed algorithm has been tested upon only monochrome images as of now. The further studies of this branch can be conducted upon the true-color images. Different dimensional images can be taken into consideration and an optimum number of hiding characters can be suggested that does not much affect the compression ratio. Straight forward cryptographic approach can be used upon the obtained bit stream of the location based compression algorithm for hiding characters without adding any extra bits so that the final compression ratio achieved remains same as with the focused compression algorithm.

Future research will contain the application to vessels other than 24-bit images, identifying and formalizing the customization parameters, and developing new applications.

References

Arvind Kumar , Km. Pooja (2010). Steganography – A data hiding technique . International Journal of Computer Applications. (Voulme No, Page No Missing)

Atallah M. Al – Shatnawi (2012). A new method in image steganography with improved image quality . Dept. of Information Systems Al-albat university , Jourden. (Voulme No, Page No Missing)

Atul Kumar , Vikas Tyagi (2012) . Image steganography using least significant bit with cryptography . Journal of global research in computer science. (Voulme No, Page No Missing)

Jagvinder Kaur , Sanjeev Kumar (2011). Study and analysis of various image steganography with mod-4LSR replacement methods using image contrast. (Voulme No, Page No Missing)

Miroslav Dobsicek .Modern steganography . Dept. of Computer Science and Engineering. (Voulme No, Page No Missing)

Muhamud Hesan , Kamruddin Md.Nun (2012).A novel compressed domain technique ofreversible steganography. International journal of advanced research in computer science and software engineering. (Voulme No, Page No Missing)

Muhalim Mohd. Amin (2003). Information hiding using steganography . Dept. of computer system & communication faculty of CS and University teknologi Malaysia.

N . Santoshi (2012). A secure and lossless adaptive image steganography with mod-4 LSR replacement methods using contrast. (Voulme No, Page No Missing)

Nagham Hamid , Abid yahaya , R. Budlishah Ahmad & Osamah M. Al Querashi . Image steganography Techniques : An overview university of Malaysia Perlis. (Voulme No, Page No Missing)

Pallavi Hemant Dixit (2013). Arm implementation of LSB algo of steganography . International Journel of Engineering and advanced Technology. (Voulme No, Page No Missing)