

An Optimistic Approach for Text Data Concealment in an RGB Image using CryptSteg Technique

Richa Singh

Computer Science & Engineering Department
PSIT, Kanpur

Amit Kumar Sharma

Assistant Professor
PSIT-COE, Kanpur

ABSTRACT

Cryptography is the science and art of encrypting and decrypting text data where Steganography is the science and art of hiding information. Steganography deals with composing hidden message so that only the sender and receiver know that the message even exists. A novel approach i.e. CryptSteg is introduced where sender embedding text message in the picture and send it to the receiver. In this approach the algorithm of cryptography and Steganography is combined. Firstly the text message is encrypted and this encrypted message is then embedded in an image using a new Steganography algorithm. The image are partitioned in the ten level block, and the text data will be embedded into ten diagonal or linear sub block values which is depend upon key. The quality of produced image is better using the median filter while using this algorithm.

Keywords

Cryptography, Steganography, Encryption, LSB

1. INTRODUCTION

Cryptography and Steganography are broadly used technique that encode and hide information. Cryptography is the jumbling of message so nobody can understand [1] and Steganography is the hiding of information so it cannot be seen by anyone. A study is to combine both techniques to provide better security.

Cryptography System is basically divided into two i.e. symmetric key and Asymmetric key. Symmetric key system uses a single key for encryption and decryption process whereas in asymmetric key two key are used, public key known to everyone and the private key that is known only to the receiver.

The main focus of this paper is to describe a method in which the Cryptography and Steganography are integrated together using some media such as image, audio, video etc.

In this paper, a new algorithm is proposed for RGB image. According to this algorithm, RGB image is divided into 10*10 blocks, and can take only diagonal blocks for data hiding using some rules.

Now a day's people uses digital picture to transmit over e-mail and other internet communication and the RGB image is one of them for sending secret message which is not affected by visual attack [2]. Visual Attack means intruder can easily detect the message on the low bit panel of an RGB image. For better security, Cryptography and Steganography techniques are combined in this paper. If the encoded data are send in an RGB image no one can easily detect the secret message. This technique is used to keep the data confidential.

2. RELATED RESEARCH

In [3], the LSB (Least Significant Bit) is the most popular technique to hide image in steganography. In LSB, place the embedded data at the least significant bit of each pixel in the image. The altered image is called Stego-image, which does not change the quality of an image. The least significant bit i.e. the eighth bit is changed with a bit of secret message inside an image.

ALGORITHM

1. Scan the image row by row and encode it in binary.
2. Encode the secret message in binary.
3. Check the size of image and secret message.
4. Select randomly one pixel of the image.
5. Divide the image into three parts i.e. red, green and blue
6. Hide bits of the secret message in each pixel of the least significant bits.
7. Set the image with the updated value

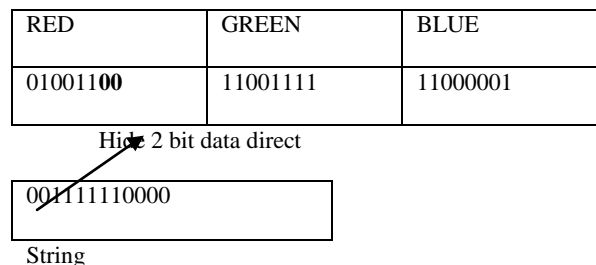


Fig1. Least Significant Bit Hiding Technique

3. THE PROPOSED METHOD

Steganography and Cryptography [4] are two different techniques. To assuring about the security is major issue for the computer users. Businessman, professionals and other user wants to make data secure. Both methods provide a good security but multiple layer security is always preferable by everyone. According to this combining technique the data are encrypted by software using a secret key and then embed the cipher text in an RGB image or any other media such as audio, video using the stego key. This combining technique provide the secure data transmission over an insecure environment i.e. internet.

The combined concept of cryptography and steganography is depicted by the diagram. In RGB image there are three data values for each pixel. To save the storage there are 24 bit representation for one pixel, so

hiding of data without significant distortion is very difficult for RGB image. On the basis of these criteria this paper introduces a new approach which consists of two parts: embedding process and extraction process.

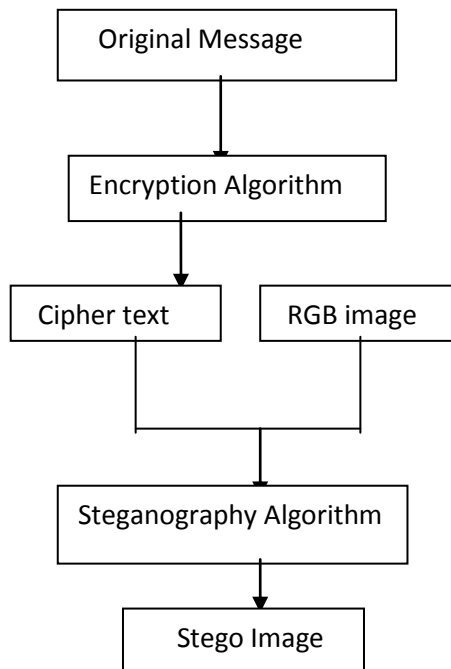


Fig2. Block diagram of algorithm

3.1 EMBEDDING PROCESS

In embedding process the original image is divided into blocks, calculating the binary values of each block and hiding the encrypted data on replacing the binary value of pixel.

Encryption Method

In encryption method we use the transposition technique to encrypt the data to become a cipher text.

3.1.1. TRANSPOSITION TECHNIQUE

In the transposition technique, the message are written in a matrix form, place the characters row by row, and read the message, column by column, according to the key value. The order of the column then becomes the key to the algorithms.

The transposition cipher [5] performing more than one stage of transposition of bits so it is more secure. The result gets complex permutation that is not easily decoded by anyone but this technique is quite useful to decrypt the text data. The encryption algorithms using transposition technique are as follows:

ALGORITHM FOR ENCRYPTION

1. Take the original message; place all characters of the message row by row in the matrices.
2. Read the message column by column, but permute the order of the columns. The order of the column then becomes the key to the algorithm.
3. Cipher text characters are generated, convert the cipher text into ASCII and take the binary values of all the encoded text.

For example, take the message 'GOOD', now place the message in a matrix. Read the message column by column according to the key. Now take the ASCII value of all the characters in the cipher text to convert it in binary.

PLAIN TEXT: "GOOD"

KEY=2

KEY=1

G	O
O	D

CIPHER TEXT = ODGO

ASCII value of cipher text is as follows:

Table1. ASCII value of cipher text

CT	O	D	G	O
ASCII	79	68	71	79

Now take the binary value of these ASCII values of all characters of the cipher text. Put all the binary values in the table as follows:

O	D
G	O

The binary value of the cipher text is as follows:

Table2. Binary value of cipher text

0	1	0	0	1	1	1	1	0	1	0	0	0	1	0	0
0	1	0	0	0	1	1	1	0	1	0	0	1	1	1	1

STEGANOGRAPHY

Steganography [6] is art of hiding information. In Steganography, firstly compare the size of the pixel with the size of text message and write all the pixel intensity value and changed in the binary format. In this paper two cases are discussed. Case 1 is discussed for less encoded message bit and case 2 is discussed for more encoded message bits.

For less message bit the RGB image hide the data and is same as the stego image because the intensity value of all pixel are not disturbed but for more message bit the RGB image is distorted. So due to the replacement of message bit the image are noisy, so median filter [7] are used to remove the noisy image. Two cases with result are as shown below.

CASE 1: If the bit of text document is too small then there is no effect on the stego image. The original image and the stego image both are looking same.



Fig.3 Original image of photographer

The pixel values are representing in the tabular form. Each block has some values and each value represents the pixel intensity value. These values lie between 0-255. Cipher data exist anywhere in the block depending on the arrangement of the pixel value.

Table3. Pixel values of photographer image

5	9	10	67	50	123
125	154	200	6	186	34
17	18	199	78	195	156
32	90	145	233	200	120
37	154	188	211	232	190
7	49	21	209	176	123

Now all values are the intensity value of each pixel. Take the binary value of each pixel and replace these binary values with the Cipher text binary values.

0	1	0	0	1	1	1	1	0	1	0	0	0	1	0	0
0	1	1	1	1	1	0	1	1	0	0	1	1	0	1	0
0	1	0	0	0	1	1	1	0	1	0	0	1	1	1	1
0	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0
0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0
0	0	0	0	0	1	1	1	0	0	1	1	0	0	0	1



 Image pixel block where cipher data exist.
 Original pixel value in binary

Fig4. Cipher data in image

3.1.2. EXTRACTING ALGORITHM

In the extraction process, same key is used for data decryption on receiver side. Receiver receives the Stego image and extracts the hiding data from the RGB image and decrypts the encoded data using the same key through which encryption process is done. The following algorithm provides for extracting the data from the image and decodes it using the help of key.

1. Receive the Stego image.
2. Convert the image into 10*10 pixel blocks as like as embedding algorithm.
3. Choose the edge pixels according to the data position array and collect the LSB [8] of the pixel value from the selected block and make cipher text.
4. The cipher text is then decrypted with the key and then gets the plain text message.

4. EXPERIMENTAL RESULT

The algorithm is implemented in MATLAB and run on window 7 platform. This method is applied to several RGB image. In this experiment the text message are 4 bytes (can take any byte of data) and 412*412 'Photographer' image. In fig 5.1 a 412*412 photographer image is the original image and hide 32 bit text document. The Stego image is shown here which is 412*412 and the encoded text document are hide in it using the proposed method [7]. The pixel in the photographer is uniformly distributed so it is very difficult to identify the hidden text document inside the RGB image. The hidden text content is not shown by the naked eye.



Fig5.1. Original image Fig5.2. Stego- image

CASE 2:

If the bit of text document is too large and the data are embedded in the original image then there is some possibility of noise in the image. Fig 6.1 shows the original image and fig 6.2 shows the noisy images in which the text data are hidden. To remove the noise in an RGB image, median filter [6] are used.

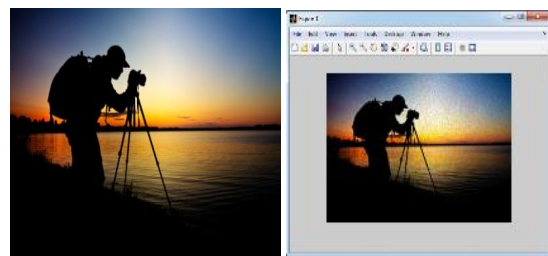


Fig6.1.Original image Fig6.2. Noisy Stego image

Now when the text data are hide the image gets noisy, because some intensity of pixels are changes due to the replacement of bits, so to remove the noise we use the Median filter to clear the RGB picture. The median filter clears the noisy image as its original RGB image. So the attacker does not find out that the image send to the receiver have data are not due to the picture quality. This method provides confidentiality of text document.



Fig7.1 Noisy Stego image Fig7.2. Stego image

After removal of noise, the data are sending to the receiver end. The receiver checks the RGB data and decrypts the cipher text embedded in the image by using the key.

Here there are the comparison between 'Lena', 'Baboon' and 'photographer'. Photographer provides the better capacity, robustness and PSNR as compared to 'Lena' and Baboon.

Table4. Test result of RGB image

Comparison of LSB with the experiment	Lena		Baboon		Photographer	
	LSB	PA	LSB	PA	LSB	PA
PSNR(dB)	36.3	41	35.1	37	37.7	43
Capacity (bits)	788	812	570	598	873	905
Robustness	.8	.7	1.6	1.4	.9	.8

In this paper, there is the comparison between original image and stego-image using their histogram. In both cases the histogram is almost same. The first histogram represents the original RGB image and the second histogram represents the stego image in which the text data are hiding.

The histogram is implemented in MATLAB coding and the output of the RGB image is shown here to compare easily. So using histogram, this shows that if the data are hiding in the RGB image there is no effect on the RGB image. It is same like as the original image. So the

attacker does not understand the data hide in the image, and this way the data are safe.

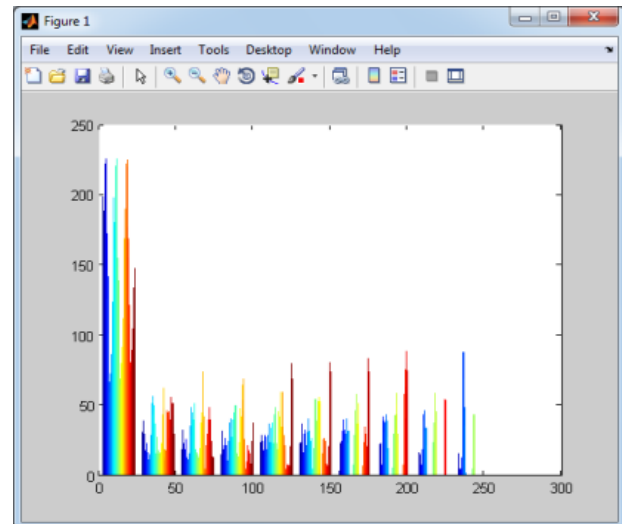


Fig8.1 Histogram of Original image

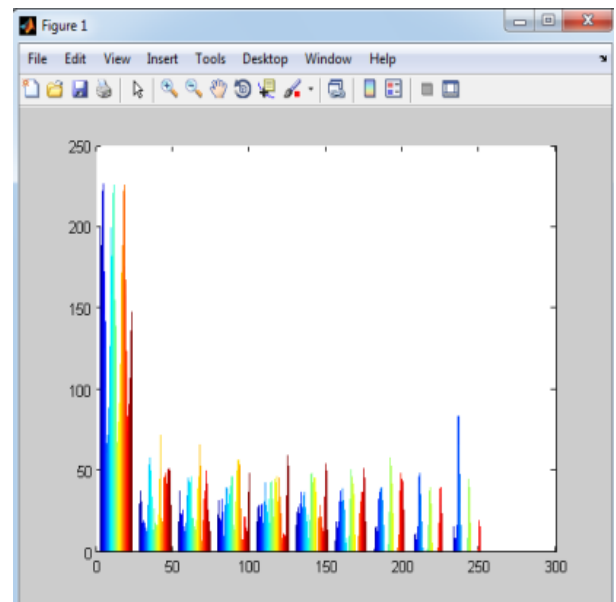


Fig8.2 Histogram of Stego image

5. CONCLUSION

This paper introduces a new method to hide the text document in the RGB image. This method has larger capacity to hide the text document in the RGB image. The experimental result shows the cases of noisy data and without noisy data. This method also provides more robustness.

6. FUTURE WORK

In this paper, the size of text document is very small. In future a large size of document may be used to hide the data, take the binary of the entire encoded text document and embedded it in a RGB image and send to the receiver.

7. ACKNOWLEDGEMENT

I give special thanks to Asst Prof. Mr. Amit Kumar Sharma for their constant support and guidance.

8. REFERENCES

- [1] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo M. Eghan, and Nii Narku Quaynor- “ A New Cryptographic Encryption Algorithm for Securing Digital Images”, *International Journal of Computer Applications (0975 – 8887)*, Vol. no. 94 – No. 19, May 2014.
- [2] Andreas Westfeld and Andreas Pfitzmann, “Attacks on Steganographic Systems Breaking the Steganographic Utilities” *EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned*.
- [3] Sakthisudhan K., Prabhu P., Thangaraj P., and “Secure Audio Steganography for Hiding Secret Information” *International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012) Proceedings published in International Journal of Computer Applications® (IJCA)*.
- [4] Sharmah Deepti Kapoor, Bajpai Neha, “Proposed system for data hiding using cryptography and steganography”, *International Journal of Computer Applications (0975 – 8887) Volume 8– No.9, October 2010*.
- [5] Omolehin J.O, Abikoye O.C, Bahej A.O , “Time Complexity of 4 Row Rail Fence Cipher Encryption Algorithm”, *International Journal of Mathematical science*, vol-1,nov-1,2009.
- [6] Anwar h.brahim, Waleed M. Ibrahim, “Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time”, *International Journal of Information Technology & Computer Science (IJITCS) (ISSN No: 2091-1610) Volume 7: No: 3: Issue on January / February, 2013*.
- [7] ABDESSAMAD BEN HAMZA, PEDRO L. LUQUE-ESCAMILLA, “Removing Noise and Preserving Details with Relaxed Median Filters”, *Journal of Mathematical Imaging and Vision* 11, 161–177 (1999) © 1999 Kluwer Academic Publishers. Manufactured in the Netherland.
- [8] V. Lokeshwara Reddy, Dr. A shubramanyam, Dr. P Chenna Reddy "A New LSB Matching Steganography Method Based on Steganography Information Table, *Int. J. Advanced Networking and Applications*, Vol: 02, Issue: 05, Pages: 868-872 (2011).