I.J. Intelligent Systems and Applications, **2012, 1, 32-38**
Published Online February 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2012.01.04

An Efficient Method of Steganography using Matrix Approach

Nirmalya Chowdhury
Department of Computer Science and Engineering,Jadavpur University,Kolkata-700032,India
nirmalya_chowdhury@yahoo.com

Puspita Manna
Department of OCLAN,Bharat Sanchar Nigam Limited,24 pgs(s) West Bengal,India
puspita3@yahoo.com

***Abstract*—** A large number of the world business is going on using "INTERNET" and the data over the internet which is vulnerable for attacks from the hackers. Thus, uses of highly efficient methods are required for sensitive data transmission over the internet to ensure data security. One of the solutions to data security is to use an efficient method of steganography. The goal of steganography is to hide messages inside other 'harmless' messages in a way that does not allow any enemy to even detect that there is a second message present. Steganography can be used with a large number of file formats most commonly used in the digital world of today. The different file formats popularly used are .bmp, .gif, .txt etc. Thus the techniques of steganography are going to play a very important part in the future of data security and privacy on open systems such as the Internet.

This paper presents an efficient method for hiding data into an image and send to the destination in a safe manner. This technique does not need any key for embedding and extracting data. Also, it allows hiding four bits in a block of size 5×5 with minimal distortion. The proposed algorithm ensures security and safety of the hidden information. The experimental results presented in this paper show the efficacy of the proposed method.

Index Terms- Steganography; data security; data hiding; Stego-image

I. INTRODUCTION

Steganography is the art of hiding information in such a way that prevents the detection of hidden messages [1,2]. In this technique, no one apart from the sender and the intended recipient even realize that there is a hidden message.

In steganography, the secret message is embedded into an image (or any media) called cover image, and then sent to the receiver who extracts the secret message from the cover message [3,4]. After embedding of the secret message, the cover image is called a stego-image. This image should not be distinguishable from the cover image, so that the attacker can not discover the presence of any embedded message[5]. Note that, the resulting stego-image will look identical to the cover image to human eyes.

Data security can also be achieved by cryptography. Sometimes these two techniques are used in a combined manner to increase the level of data security. The term steganography means "cover writing" whereas cryptography means "secret writing".

Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can only remove the disguise and read the message. The message we want to send here is called plain text and disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process i.e. recovering the plain text from the cipher text is called deciphering or decryption.

The encryption method protects contents during transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is clear. Steganography hides messages in plain sight rather than encrypting the message. The message is embedded in the data and does not require a secret transmission. In fact, the message is carried inside data. Steganography is therefore a better approach to data security than cryptography.

This paper proposes an efficient algorithm which has been developed by modifying an existing algorithm of steganography. The proposed algorithm has experimentally been found to give better performance compared to the existing one.

II. A BRIEF REVIEW OF EXISTING METHODS

Steganography helps to hide secret information which is to be protected using a digital object, also referred to as cover object, in such a manner that the information becomes a part of the cover object. The majority of today's steganographic systems uses multimedia objects like image[6], audio, video etc as the cover media

because people often transmit digital pictures over email and through other internet communications[7]. There are several methods of steganography[8,9]. Some of them are described below.

Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover object. For images as a cover object, the LSB of a pixel is replaced by one bit from the message. If we use 24-bit image file as the cover object, we can store 3 bits of information from the message in each pixel by modifying the LSB of the R, G, B components of the pixel. This will not make any difference between the visual appearance of the resulting stego image and that of the original cover image.

The Encrypt and Scatter technique is a method of image steganography to hide the data to be sent being embedded in an image. This technique of embedding message makes it appear more like noise and it is generally done using LSB modification. The demerits of this approach is that even if the message (encrypted version) bits are extracted successfully, it will be useless until we are able to decode the message using the appropriate stego-key[10].

An interesting method, proposed by G Sahoo and R K Tiwari in 2008, works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using steganography. Thus they have used a stego key for the embedding process[11].

Another method of steganography has been proposed by Ahmed Al-Jaber and Khair Eddin Sabri. This algorithm allows hiding four bits in a block of size 5 * 5 by changing a maximum of two bits. The selection of the bits to be changed in the block depends on the number of adjacent bits with the same value. The bit that has the least number of adjacent bits is selected[12].

III. PROPOSED TECHNIQUE

In this paper, we have presented an efficient method of steganography. This method is based on taking pixel information from the cover image and forming a matrix, each of size **5×5.** In each matrix, 4 bits from the secret message can be embedded.

For embedding of data the following steps are adopted :

Algorithm 1

Input : Cover image and secret message

Output : Stego-image.

Step1 : Divide the cover image into blocks (F) each of size 5×5.

Step2 : For each block, we proceed as follows

i. For every row in the first four rows of the block,
exclusive-or all the bits of that row to get
$r_1r_2r_3r_4$.

ii. For every column in the first four columns of
the block, exclusive-or all the bits of that
column to get $c_1c_2c_3c_4$.

Step 3: Exclusive-or the results from step i and ii to get $s_1s_2s_3s_4$ where $s_1 = r_1 \oplus c_1$, $s_2 = r_2 \oplus c_2$, and so on.

Step 4: Compare the results obtained from step 3 with the four embedded bits $b_1b_2b_3b_4$. If there is no difference, no change of bits in F is needed, otherwise, consider the following cases:

• if the difference is in one bit b_i, the bit $[F]_{i,5}$ or $[F]_{5,i}$ should be complemented

• else if difference in two bits b_i and bj, then the bit [F] i,j or [F]j,i should be complemented or bit $[F]_{5,i}$ and $[F]_{5,j}$ should be complemented.

• else if difference in three bits b_i, b_j and b_k, then the bits
(($[F]_{i,j}$ or $[F]_{j,i}$) and ($[F]_{k,5}$ or $[F]_{5,k}$)) or
(($[F]_{i,5}$ or $[F]_{5,i}$) and ($[F]_{k,i}$ or $[F]_{j,k}$)) or
(($[F]_{5,j}$ or $[F]_{j,5}$) and ($[F]_{k,i}$ or $[F]_{i,k}$))
should be complemented.

• else (if difference in four bits b_i, b_j, b_k and b_m) then the bits
(($[F]_{i,j}$ or $[F]_{j,i}$) and ($[F]_{k,m}$ or $[F]_{m,k}$)) or
(($[F]_{i,m}$ or $[F]_{m,i}$) and ($[F]_{k,i}$ or $[F]_{j,k}$)) or
(($[F]_{m,j}$ or $[F]_{j,m}$) and ($[F]_{k,i}$ or $[F]_{i,k}$))
should be complemented.

Note : The bit(s) to be changed is selected in such a way that the MSB and next two significant bits of the RGB values of each pixel of the cover image remain unaffected so that there is minimal distortion in the cover image.

Steps for Extracting the data from the stego image :

Algorithm 2

Input : Stego-image

Output : Secret message

The algorithm used for extracting the embedded data is similar to that used for embedding. The following steps are carried out to obtain the embedded data.

Step1 : Divide the cover image into blocks (F) each of size 5×5.

Step2 : For each block, we proceed as follows:

i) For every row in the first four rows of the block, exclusive-or all the bits of that row to get $r_1r_2r_3r_4$.
ii) For every column in the first four columns of the block, exclusive-or all the bits of that column to get $c_1c_2c_3c_4$.

Step 3 : Exclusive-or the results in 2.i. and 2.ii. to get the embedded bits $s_1s_2s_3s_4$ where $s_1=r_1\oplus c_1$, $s_2=r_2\oplus c_2$, and so on.

Step 4 : Stop.

Example : Suppose that we have the following cover image:

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

and the embedded data is : 11100101

Following the said necessary steps, for every row in the first four rows of the block, we exclusive-or all the bits of that row to get $r_1r_2r_3r_4$ on the given block and the following result is obtained :

$1\oplus 1 \oplus 1 \oplus 1 \oplus 1 = 1$
$1\oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$
$0\oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0$
$1\oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0$

The result is 1000

Following the said necessary steps for every column in the first four columns of the block, we exclusive-or all the bits of that column to get $c_1c_2c_3c_4$ on the same block to get the following result:

$1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0$
$1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 = 0$
$1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 1$
$1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 = 1$

The result is 0011

Now we exclusive-or the results obtained in 1 and 2 to get the embedded bits $s_1s_2s_3s_4$ where $s_1=r_1\oplus c_1$, $s_2=r_2\oplus c_2$, and so on for the same block to get the following result:

$1 \oplus 0 = 1$
$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$0 \oplus 1 = 1$

The result is 1011 and the embedded data is 1110.

It can be seen that the bits number 2 and 4 in the result are different form those in the embedded data. So there should be a change in either the bit $[F]_{2,4}$ or $[F]_{4,2}$. To minimize its effect on the cover image, bit $[F]_{4,2}$ should be changed. In the other block, if the same operation is repeated, the following results are obtained:

$r_1r_2r_3r_4 = 0101$ $c_1c_2c_3c_4 = 0010$ $s_1s_2s_3s_4 = 0111$
The embedded data is 0101.

Therefore, the bit that should be changed is either $[F]_{3,5}$ or $[F]_{5,3}$. Again due to the same reason as stated above $[F]_{3,5}$ is to be changed.

IV. Experimental Results

The proposed algorithm has been applied on different images for different data. The same image-data combinations have been used for experimentation with the existing algorithm for comparision. The following computations were performed for each stego-image:

Average : It is computed for each pixel depending on its neighbors. Then the average of pixel average values is also computed to test the consistency between each pixel and its neighbors.

Standard Deviation : Compute the average for each pixel depending on its neighbors, and then compare it with the original image.

Here we have considered three .bmp files as the cover images and three text files to be embedded in those cover images. The output consists of three stego images which are .bmp files.

Experiment No. 1:
In this experiment we have used the following cover image as shown in Fig1.1. The text to be embedded is presented in Table 1. The stego image is shown in Fig 1.2 . It is found that the proposed method can successfully embed the given text into the cover image and is also able to extract the given text (secret message) from the stego image. It may be noted that here all the words of the secret message are successfully extracted in the right order without any error.

Fig 1.1 Original Image

Table 1 Text to be embedded

India is our motherland, Its the land of our love, We are proud to be an Indian. We serve our life for our beloved country.

Figure 1.2 Stego Image

Experiment No. 2:

In this experiment we have used the following cover image as shown in Fig2.1 . The text to be embedded is presented in Table 2. The stego image is shown in Fig 2.2 . It is found that the proposed method can successfully embed the given text into the cover image and is also able to extract the given text (secret message) from the stego image. It may be noted that here all the words of the secret message are successfully extracted in the right order without any error.

Fig. 2.1 Original Image

Table 2 Text to be embedded

```
//   bmp in C
#include <stdio.h>
#include<stdlib.h>
#include<math.h>
#include<ctype.h>
#include<conio.h>

typedef struct tagBITMAP
{
        unsigned short bfType; //might
need to be a char
        unsigned long size;
        unsigned short bfReserved1;
        unsigned short reserved2;
        unsigned long offset;
        unsigned long sizeofstruct;
        unsigned long width;
        unsigned long height;
        unsigned short planes;
        unsigned short bits;
        unsigned long compression;
        unsigned long imagesize;
        unsigned long xresolution;
        unsigned long yresolution;
        unsigned long ncolors;
        unsigned long impcols;
} BITMAP;
```


Figure 2.2 Stego Image

Experiment No. 3:

In this experiment we have used the following cover image as shown in Fig3.1 . The text to be embedded is presented in Table 3. The stego image is shown in Fig 3.2 . It is found that the proposed method can successfully embed the given text into the cover image and is also able to extract the given text (secret message) from the stego image. Here also all the words of the secret message are successfully extracted in the right order without any error.

Figure 3.1 Original Image

Table 3 Text to be embedded

260320 Nirmalendu mondal Near kalikapur hospital Haanpur,Champahati,pin-743330
261803 Smt Bijoli Mondal Sahebpur Champahati, Pin-743330
260545 Sri Debabrata Chatterjee vill_p.o.-Champahati, Pin-743330
260317 Sri Netai Charan Maity Kalikapur Pin-743330
260163 Sri someswar Banerjee Vill+ P.O.-South Garia Pin-743618
260855 Sri Sovan Chatterjee Vill+P.O. South Garia
260856 Sri Barendra nath Roychoudhury Vill+P.O. South Garia
260447 Sri Subal Ghosh Champahati Main Road,Champahati
261726 Sri Lalit Bhattacharjee Vill+P.O. South Garia
260821 Sri Anil Kr Naskar Vill+P.O. South Garia
261651 Sri Ranjan Banerjee South Garia PIN-73613
260432 Sri Sujan Chakraborty O/O The CAO(TR) GM,CAL SSA

Figure 3.2 Stego Image

It may be noted that in all of the above three experiments, no difference in the visual appearance between the cover image and the stego image is observed. This is important since if any difference in appearance between the cover image and the stego image is introduced due to the embedding of the secret message, then someone may doubt or even decipher the embedded text from the stego image.

Table 4. and Table 5. show the comparision of the existing and the proposed method in terms of the average and standard deviation respectively. The said comparisons are also graphically demonstrated in Fig. 4 and Fig. 5. It can be clearly seen that the proposed algorithm shows a better performance in terms of both the average and standard deviations between the original image and stego-image.

Table 4 Average using existing and proposed algorithm

File size(KB)	Average using Existing Algorithm	Average using Proposed Algorithm
1	25.80	23.59
2	39.42	26.99
3	22.69	21.16
4	25.80	21.91
6	28.07	21.16
7	23.59	15.86
9	22.69	18.87
10	20.43	14.98
15	28.07	18.87
16	29.00	22.69

Table 5 Standard deviation using existing and proposed algorithm

File size(KB)	Standard Deviation using Existing Algorithm	Standard Deviation using Proposed Algorithm
1	24.37	21.60
2	35.10	34.18
4	35.33	34.47
6	37.91	37.10
7	36.83	35.92
9	39.55	39.19
10	31.62	30.92
16	33.78	32.32

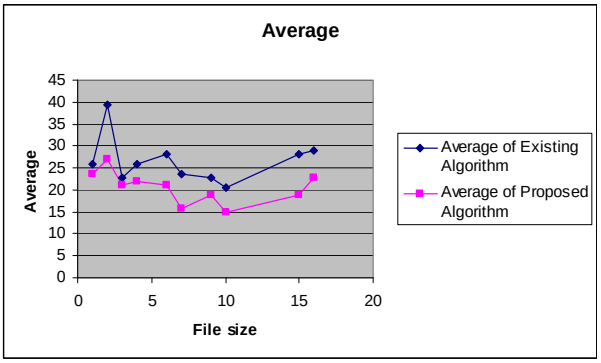

Figure 4 Average using existing and proposed algorithm

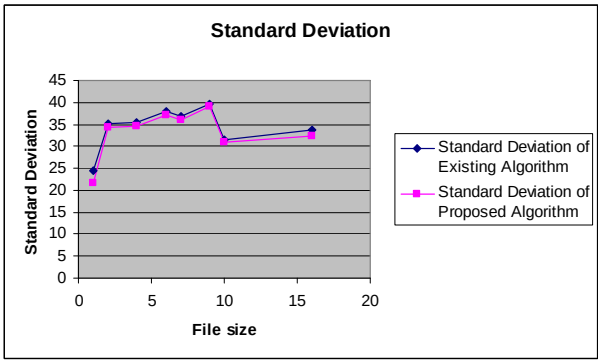

Figure 5 Standard deviation using existing and proposed algorithm

V. CONCLUSIONS

In this paper, the technique which has been proposed to hide data within a color image is secure and the hidden information is quite invisible. The advantages of the proposed technique are:

- The proposed algorithm shows a better performance in terms of both the average and standard deviations between the original image and stego-image.
- The proposed algorithm does not need a secret key. It needs only an agreement between the embedding and extracting agents.
- The proposed algorithm ensures that the MSB and the next two bits of any pixel value of the original image will not be modified. So the distortion of the image will be less compared to that of the existing algorithm.

A comparison of the proposed algorithm with the existing scheme shows that the proposed algorithm gives a better performance in terms of the average and standard deviation factors.

References

[1] Y. Chen, H. Pan, and Y. Tseng, “A secure Data Hiding Scheme for Two-Color Images,” IEEE Symposium On Computers and Communications, 2000.

[2] C.Cachin, ”An Information-Theoritic Model for Steganography”, Proc. of the 2nd International Workshop on Information Hiding, Portland, Oregon, USA,15-17 Apr 1998, Lecture notes in CS, Vol.1525, Springer-Verlag.

[3] N. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen,” IEEE Computer, pp. 26-34, February 1998.

[4] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques",2001 International Conference on Image Processing, October 7-10, 2001, Thessaloniki, Greece, Vol. 3, pp. 1019-1022.

[5] 1. Johnson, N. F. and Jajodia, S. (1998). Exploring steganography:Seeing the unseen. Computer,31(2):26–34.

[6] C.T.Hsu and J.L.Wu., ”Hidden Singatures in Images”, *Proc. IEEE International Conf. on Image Processing, ICIP-96*, Vol.3, pp.223-226.

[7] Niels-Provos, Peter Honeyman, Hide and Seek: Introduction to steganography(2003).

[8] K. Curran and K. Bailey, "An Evaluation of Image Based Steganography Methods," International Journal of Digital Evidence, vol. 2, issue 2, pp. 1-40, Fall 2003.

[9] Luis von Ahn, Nicholas J. Hopper., Public Key Steganography.

[10] Robert Krenn. Steganography and steganalysis.

[11] G Sahoo, R K Tiwari “Designing an Embedded Algorithms for Data Hiding using Steganographic Technique by File Hybridization” , IJCSNS, vol 8, No 1,pp-226-233, January 2008

[12] Ahmed Al-Jaber , Khair Eddin Sabri “Data Hiding in a Binary Image”

