ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

A New Approach in Steganography using different Algorithms and Applying Randomization Concept

U. Rizwan[1] and H. Faheem Ahmed[2]

Department of Mathematics, Islamiah College, Vaniyambadi, India[1]

Department of Computer Science, Islamiah College, Vaniyambadi, India[2]

ABSTRACT: **In this paper, we have given an overview of the image steganography, its uses and techniques. We have proposed some new techniques of embedding a text message in an image in every odd, even, prime number memory location of image pixel values. We have also compared the actual and embedded images with histograms and computed the Mean Square Error(MSE) and Peak to Signal Noise Ratio (PSNR). We also compute the Structural SIMilarity (SSIM) index of all our images and make a comparative study. SSIM is a method for measuring the similarity between two images. It is an improved version of the universal image quality index proposed before. SSIM gives a much better indication of image quality.**

Keywords: **Cryptography, Steganography, DFT, DCT, DWT,SSIM**

I. INTRODUCTION

Since the rise of the internet, one of the most important factors of information technology and communication has been the *security of information. Cryptography* was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called *Steganography*. In short, the science of securing a data by encryption is Cryptography whereas the method of hiding secret messages in other messages is Steganography, so that the secret's very existence is concealed.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words *stegos* meaning *cover* and *grafia* meaning *writing* defining it as *covered writing*. Steganography has been used since ancient times, for example people practiced it by etching messages in wooden tablets and covered with wax. They used tattooing a shaved messenger's head, letting his hair grow back and then shaving it again when he arrived at his contact point to reveal the message. Different types of stenographic techniques have been used that employ invisible inks, microdots, character etc. Digital steganography uses the digital objects such as image, video, music or any other computer file for hiding the data. The idea was first given by Simmons in 1983. Steganography is different from cryptography; the latter is about concealing the content of message whereas former is about concealing the existence of message itself. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect military messages, E-mails, credit card information, corporate data, personal files, etc.

There are two methods of performing steganography, one in *spatial domain*, and the other in *frequency domain*. Each technique has its own advantage and disadvantage. In the spatial domain, we can simply insert data into host image by changing the gray levels of some pixels in the host image, but the inserted information may be easily detected using computer analysis. In the frequency domain, we can insert data into the coefficients of a transformed image, for example, using discrete Fourier transform (DFT), Discrete Cosine Transform (DCT) and

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

Discrete Wavelet Transform (DWT). But we cannot embed too much data in the frequency domain because the quality of the host image will be distorted significantly. The convolutional codes are the good error detection and correction code, which is using the concept of the interleaving.

A most popular and oldest technique for hiding data in digital image is the *Least Significant Bit Method* Technique. One of the major disadvantages associated with LSB techniques is that the hidden message can be destroyed by the intruder by changing the LSB of all image pixels. In this way, hidden message can be destroyed but the change in image quality is in the range of +1 to -1 at each pixel position.

II. Traditional Least Significant Bit Substitution

LSB substitution is the most popular method used for Steganography due to its ease of application and less perceptual impact. The current embedding process uses LSB Steganography as the basis to implement a more robust technique. The secret message is converted to a bit stream and each bit of the message is embedded into the LSB of the pixels of the image. This ensures that the pixel value changes almost by one, which does not result in a significant change in the image quality perceptually. The word almost used here is significant as probabilistically there is 50% chance the LSB to be changed is already the one desired, and, hence no change to the image is made.

First LSB algorithm
1 0 0 1 0 0 0 1

Here only the last bit of the pixel is modified to hide the data. It is implemented highly because of its simplicity and good picture quality.

Second LSB algorithm
1 0 0 1 0 0 0 1

Here last two bits are subjected to change to increase the amount of data to be hidden. Eventually the picture quality is less than our first LSB algorithm.

III. Integration of Algorithms

The improvement of LSB information hiding algorithm mainly aims at the images of BMP type. Research revealed that, the reaction of human eyes to Red, Blue and Green is different. According to the brightness formula:

$$I = 0.3R + 0.59G + 0.11B$$

And the theory of the human visual cells sensitivity of colour, human eyes are most sensitive to the green, the next is to the red, and the least is to the blue. Therefore, the different least bits of brightness components of the red, green, and blue of each pixel can be replaced by the hiding data. And according to the basic principle of the Least Significant Bits Information Hiding algorithm, the effect of replacing the least bit on original data is only 1, the second least bit replacement's effect is 2, and the third's is 4, and so on, the nth is $2n-1$. The higher the bit, the greater effect is. By taking advantage of the less eyesight relevance to the lower bits, the data to be hidden are embedded into the lower (first few least) bits of each pixel. If the least bit is changed in green component of the colour, the resulting effect on the brightness is $20 \times 0.59 = 0.59$. If the same change is made to red component, the effect on the brightness is $20 \times 0.3 = 0.3$. If the first 2 least bits of the blue component are altered, the effect on the brightness is $(20 + 21) \times 0.11 = 0.33$. So, all effects are not greater than the maximum change in brightness the traditional LSB algorithm brings about: $20 \times 0.59 = 0.59$, which cannot be perceived by human eyes. Thus, for each 3-byte in the bitmap, $1 + 1 + 2 = 4$ bits can be used for replacement. This means an increase in the hiding efficiency by about 17%, a great improvement by this improved LSB algorithm, compared with using the tradition LSB method. Moreover, there is no impact on the hiding result.

IV. Proposed Technique for Embedding Text Message in Image

The *Mean Square Error (MSE)* and the *Peak Signal to Noise Ratio (PSNR)* are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed/reconstructed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower is the error.

To compute the PSNR, the block first calculates the mean-squared error using the following equation:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

V. Embedding Text Message in Every Odd Memory Location of Image

Let cover image be

51	3	106	213	128
50	190	215	5	180
153	113	133	173	109
69	237	51	96	77
50	118	171	212	48

Let the message be ‘hello’ ie the value to be embedded is

104 101 108 108 111

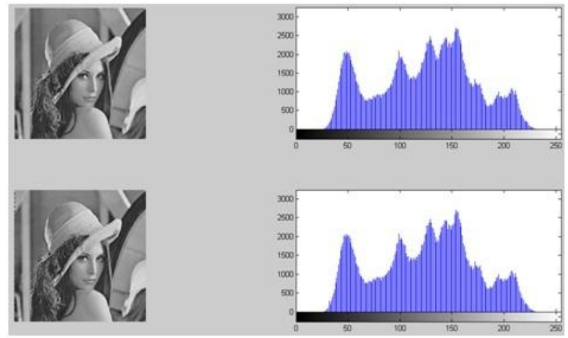
Replacing the values with the message bytes at every odd location we get

104	3	106	213	128
50	108	215	5	180
101	113	133	173	109
69	111	51	96	77
108	118	171	212	48

Now extracting from above from each odd locations

[104 101 108 108 111]

we get, ‘hello’. The original image and its stego image embedded in odd pixel memory locations along with their histograms are presented in Fig. 1.



MSE = 0.3004 PSNR_Value = 53.3531

Fig. 1 Original and Stego Image embedded in odd pixel locations with histograms

VI. Embedding Text Message in Every Even Memory Location of Image

Let cover image be

51	3	106	213	128
50	190	215	5	180
153	113	133	173	109
69	237	51	96	77
50	118	171	212	48

Let the message be ‘hello’ ie the value to be embedded is

104 101 108 108 111

Replacing the values with the message bytes at every even locations, we get

51	108	106	213	128
104	190	215	5	180
153	108	133	173	109
101	237	51	96	77
50	111	171	212	48

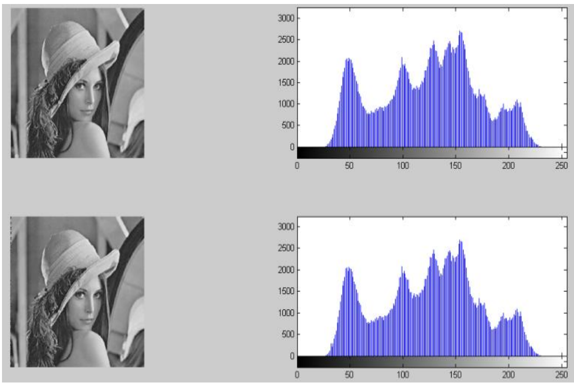
Now extracting from above from each odd locations

[104 101 108 108 111]

we get, ‘hello’. . The original image and its stego image embedded in even pixel memory locations along with their histograms are presented in Fig. 2.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012



MSE = 0.2992 PSNR_Value = 53.3707

Fig. 2 Original and Stego Image embedded in even pixel locations with histograms

VII. Embedding Text Message in Every Prime Number Memory Location of Image

Let cover image be

51	3	106	213	128
50	190	215	5	180
153	113	133	173	109
69	237	51	96	77
50	118	171	212	48

Let the message be 'hello' ie the value to be embedded is

104 101 108 108 111

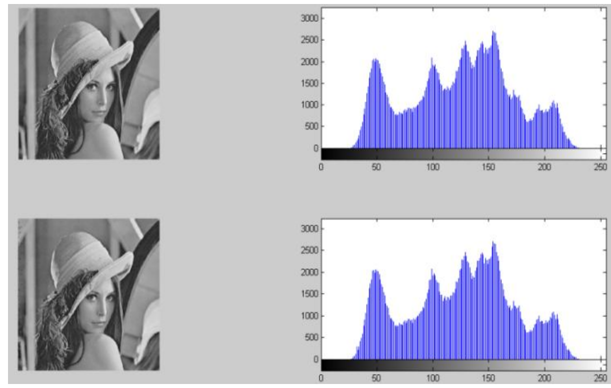
Replacing the values with the message bytes at every prime number locations like 2, 3, 5, 7, 11, 13, 17, 19 , ….. we get

51	3	106	213	128
104	108	215	5	180
101	113	133	173	109
69	111	51	96	77
108	118	171	212	48

Now extracting from above from each prime memory locations

[104 101 108 108 111]

we get, 'hello'. The original image and its stego image embedded in prime number memory locations along with their histograms are presented in Fig. 3.



MSE = 0.2841 PSNR_Value = 53.5953

Fig. 3 Original and Stego Image embedded in prime number memory locations with histograms

VIII. Embedding Text Message in Every Minimum Value in Each Column of Image

Let cover image be

51	3	106	213	128
50	190	215	5	180
153	113	133	173	109
69	237	51	96	77
50	118	171	212	48

Find minimum gray level in each column.

50 3 51 5 48

Let the message be 'hello' ie the value to be embedded is

104 101 108 108 111

Replacing the minimum values with the message bytes we get

51	101	106	213	128
104	190	215	108	180
153	113	133	173	109
69	237	108	96	77
50	118	171	212	111

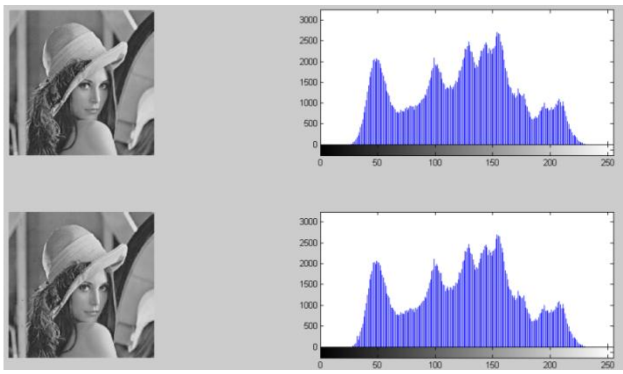
Now extracting from above from each column from each minimum location

[104 101 108 108 111]

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

we get, 'hello'. The original image and its stego image embedded in each column minimum value of memory locations along with their histograms are presented in Fig. 4.



MSE = 0.1017 PSNR_VALUE = 58.0556

Fig. 4 Original and Stego Image embedded in column minimum value with histograms

IX. EMBEDDING TEXT MESSAGE IN EVERY MAXIMUM VALUE IN EACH COLUMN OF IMAGE

Let cover image be

51	3	106	213	128
50	190	215	5	180
153	113	133	173	109
69	237	51	96	77
50	118	171	212	48

Find maximum gray level in each column.

153 237 215 213 180

Let the message be 'hello' ie the value to be embedded is

104 101 108 108 111

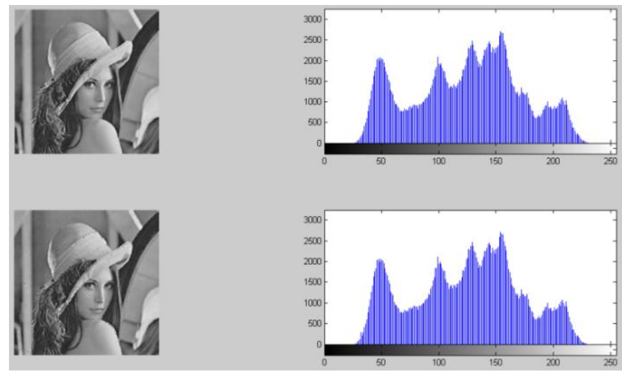
Replacing the minimum values with the message bytes we get

51	3	106	108	128
50	190	108	5	111
104	113	133	173	109
69	101	51	96	77
50	118	171	212	48

Now extracting from above from each colum from each maximum location

[104 101 108 108 111]

we get, 'hello'. The original image and its stego image embedded in each column maximum value of memory locations along with their histograms are presented in Fig. 5.



MSE = 0.7929 PSNR_VALUE = 49.1386

Fig. 5 Original and Stego Image embedded in column maximum value with histograms

X. EMBEDDING TEXT MESSAGE IN EVERY SPIRAL MATRIX COORDINATES OF IMAGE

Let cover image be

51	3	106	213	128
50	190	215	5	180
153	113	133	173	109
69	237	51	96	77
50	118	171	212	48

Construct a 5x5 spiral matrix.

21	22	23	24	25
20	7	8	9	10
19	6	1	2	11
18	5	4	3	12
17	16	15	14	13

Let the message be 'hello' ie the value to be embedded is

104 101 108 108 111

Replace the image with the message bytes at locations equal to diagonal elements of spiral matrix as shown above to get the stego image.

108	3	106	213	128
50	101	215	104	180

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

108	113	111	173	109
69	237	51	96	77
50	118	171	212	48

Now extracting from each diagonal elements of spiral matrix [21,7,1,3,13] we get

[104, 101,108,108,111]

which is 'hello'. The original image and its stego image embedded in every spiral matrix value of memory locations are presented in Fig. 6.

MSE= 0.28529 PSNR =53.57794

Fig. 6 Original and Stego Image embedded in spiral matrix coordinates

XI. Embedding Text Message at First Row of Magic Square Matrix Coordinates of Image

Let cover image be

51	3	106	213	128
50	190	215	5	180
153	113	133	173	109
69	237	51	96	77
50	118	171	212	48

Construct a 5x5 magic square matrix.

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

Let the message be 'hello' ie the value to be embedded is

104 101 108 108 111

Replace the image with the message bytes at first ray locations of magic square matrix as shown above to get the stego image.

108	3	106	213	128
50	190	215	104	180
153	108	108	173	109
69	237	51	96	101
50	118	111	212	48

Now extracting from each diagonal elements of spiral matrix [17, 24, 1, 8,15] we get

[104, 101,108,108,111]

which is 'hello'. The original image and its stego image embedded in the first row of the magic square matrix coordinates value of the memory locations are presented in Fig. 7.

Original Image Stego Image

MSE= 0.25089 PSNR =54.13599

Fig. 7 Original and Stego Image embedded in magic square matrix coordinates

Comparison of MSE, PSNR and SSIM index for the various techniques are given in Table 1.

Image	: Lena512.bmp
Pixels	: 512x512
Hidden Message Size	: 512 bytes

The hidden and the retrieved text message from the stegoimage of all above procedures is:

Steganographic techniques have been used with success for centuries already. However,since secret information usually has a value to the ones who are not allowed

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

toknow it, there will be people or organisations who will try to decode encrypted informationor find information that is hidden from them. Governments want to know whatcivilians or other governments are doing, companies want to be sure that trade secretswill not be sold to competitors and most persons are naturally curious. Many differentmotives exist to detect the use of steganography, so techniques to do so continue to bedeveloped while the hiding algorithms become more advanced Secrets can be hidden inside allhide information inside images, as this is relatively easy to implement. However, there aretools available to store secrets inside almost any type of cover source.

Table 1. Computed values of MSE, PSNR and SSIM indices

No.	Embedding Technique	MSE	PSNR	SSIM index
1	Odd memory locations	0.3004	53.3531	0.9999
2	Even memory locations	0.2992	53.3707	0.9999
3	Prime number locations	0.2841	53.5953	0.9980
4	Minimum gray level	0.1017	58.0556	0.9948
5	Maximum gray level	0.7929	49.1386	0.9682
6	Spiral matrix locations	0.28529	53.57794	0.9917
7	Magic Square locations	0.25089	54.13599	0.9999

XII. MATLAB CODING (MAXIMUM VALUE TECHNIQUE)

```
clc
cover=imread('lena512.bmp');
cover1=reshape(cover,256,1024);
[m,x]=max(cover1)
m1='Steganographic techniques have been used with success for centuries already. However,'
m2='since secret information usually has a value to the ones who are not allowed to'
m3='know it, there will be people or organisations who will try to decode encrypted information'
m4='or find information that is hidden from them. Governments want to know what'
m5='civilians or other governments are doing, companies want to be sure that trade secrets'
m6='will not be sold to competitors and most persons are naturally curious. Many different'
m7='motives exist to detect the use of steganography, so techniques to do so continue to be'
m8='developed while the hiding algorithms become more advanced Secrets can be hidden inside all '
m9='sorts of cover information: text, images, audio, video and more. Most steganographic utilities nowadays,'
m9='hide information inside images, as this is relatively easy to implement. However, there are'
m10='tools available to store secrets inside almost any type of cover source.'
    message=strcat(m1,m2,m3,m4,m5,m6,m7,m8,m9,m10);
    msgnum=double(message);
    l=length(message);
    for i=1:l
        cover1(x(i),i)=msgnum(i);
    end
    for i=1:l
        text(i)= cover1(x(i),i);
    end
    cover1=reshape(cover1,512,512);
    disp(char(text));
    subplot(2,2,1),imshow(cover)
    subplot(2,2,2),imhist(cover)
    subplot(2,2,3),imshow(cover1)
    subplot(2,2,4),imhist(cover1)
    [rows columns] = size(cover);
    % Calculate mean square error .
    mseImage = (cover - cover1) .^ 2;
    mse = sum(sum(mseImage)) / (rows * columns);
    % Calculate PSNR (Peak Signal to noise ratio).
PSNR_Value = 10 * log10( 255^2 / mse);
```

XIII. CONCLUSION

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective merits and demerits. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. We have given an overview of image steganography, its uses and techniques. Some new techniques of embedding a text message in a digital image are given. We have also compared the actual and embedded images with histograms and calculated MSE and PSNR (Mean Square Error and Peak to Signal Noise Ratio).

REFERENCES

[1] Adam Turcotte, *More efficient MATLAB implementation of SSIM* at http://ssim.rivetsforbreakfast.com

[2] Bhabdhosh, C., *Digital Image Processing and Analysis*, 8th Edn., Prentice Hall, India, 2006

[3] Bret, D., *A detailed look at Steganographic Techniques*. SANS Institute, Infosec Reading Room. 2002.

[4] Eric, C., 2003. Hiding in Plain Sight, Steganography and the art of Covert Communication. Wiley Publishing, US.

[5] Rizwan. U and Faheem Ahmed. H, *An Alternative Technique in Data Embedding*, Advanced Materials in Physics, pp 233 – 242, 2012.

[6] Rudra, P., *Getting Started With MATLAB: A Quick Introduction for Scientists and Engineers*, Version 6, Oxford Press, India, 2002.

[7] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, *Image quality assessment: From error visibility to structural similarity*, IEEE Transactions on Image Processing, vol. **13**, no. 4, pp. 600-612, 2004.

Biography

U. Rizwan earned his Ph.D. degree in Mathematics from the University of Madras. He is currently the Head of the Department of Mathematics, Islamiah College, Vaniyambadi and is serving the Institution for the past 26 years. He has published 40 research articles in journals of international repute. He has authored 5 books and is also the editor of two international journals. He has guided 30 M.Phil. scholars and one M.Tech. (IT) candidate. Presently he is guiding Ph.D. research scholars in Mathematics and Computer Science. His research interest includes Image Processing, Hacking algorithms, Stochastic Processes, Fuzzy Logic, etc. He is the member of the board of studies in PG Mathematics of Thiruvalluvar University, Vellore. He is also an academic auditor.

H. Faheem Ahmed earned his M.Tech. degree in Information Technology from Punjabi University and M.Phil. degree in Computer Science from Manonmaniam Sundaranar University. He is pursuing Ph.D. in Computer Science. He has guided 50 M.Phil research scholars in Computer Science. He is currently the Head of the Department of Computer Science and Applications, Islamiah College, Vaniyambadi and is serving the institution for the past 28 years. His research interest includes Steganography and Image processing. He has published 7 research articles and authored one book.