Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Image Steganography

[1]K. S. Sadasiva Rao*, [2]A. Damodaram
[1]Dept.of Informatics, Sri Indu PG College, India
[2]Professor, JNTUH, India

Abstract— Steganography is a branch of science where the secret information can be transmitted in a carrier file, example text, image, audio and video files. Cryptography is a branch of science where secret information is transmitted on the channel by encrypting into coded form. The mere existence of secret information is visible in case of cryptography, where as in the case of steganography, existence of secret information is not visible. Embedding of the secret data in image carrier file is called as an image steganography. Much of the research was carried out in gray scale images to embed data without disturbing the quality of the image. Where as in color image steganography, it is a bit difficult to embed data on color image without disturbing the quality of the image. Hence this paper presents a survey on various methods of steganographic techniques available.

Keywords— Steganography, Cryptography, Least Significant Bit Method

I. INTRODUCTION

'Steganography' is a greek word. 'Steganos' means covered and 'graphia' means writing. According to the history of Greek, Steganography is 'covered writing' and is used to send the messages in secured way. In ancient days, a slave's hair was removed and the secret message is tattooed on his scalp and after hair grew slave will be sent to the destination. Once he reaches destination, slave's hair will be removed and message can be retrieved.

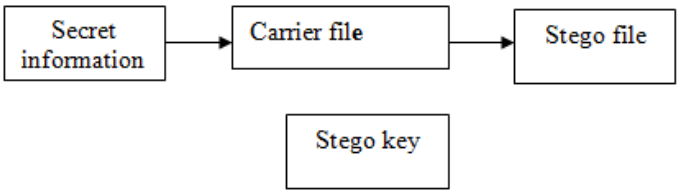

Figure1: Process of Steganography

From Figure(1), Original file is to be transferred in secured way is called as 'Secret information'. Secret information can be text file, audio file, video file or any other files. The secret information bits are embedded in various positions in carrier file (it can be text file, audio file, video file etc) depending on the stego key. Stego key is chosen by sender and is to be informed about that key to the receiver. After embedding the secret information bits in the carrier file, the carrier file is called as stego file. The process of hiding secret information in carrier file with stego key is called as steganography.

There are various forms of steganography:

- Text steganography
  Text file is used as a carrier to embed secret data.
- Audio steganography
  Audio file is used as a carrier to embed secret data.
- Image steganography
  Image file is used as a carrier to embed secret data.
- Video Steganography
  Video file is used as a carrier to embed secret data.

II. IMAGE STEGANOGRAPHY

The process of hiding secret information in the image file is called as Image steganography [1]. The image file which is used to carry the secret data is called *carrier file*. It may be gray scale image or color image. Each pixel is represented with 24-bits in color image and 8-bits for gray scale image [6]. After embedding the secret data bits on the carrier image file is called as *stego image*. There are two categories of the process of Steganography:

A. Spatial domain Techniques

Here secret data will be embedded in the pixel values of the image directly. These techniques are easy to implement. But less tolerant to attacks. Least Significant Bit techniques and variations on LSB methods will be under these techniques.

LSB Technique:

The more simple and flexible algorithm of steganography is Least Significant Bit (LSB) algorithm [4]. The original data bits will be inserted into the least significant bit position of the pixel.

24-bit images*:* We can store 3 bits of information in each pixel, one in each LSB position of the three 8 bit values in 24 bit value.

For example suppose 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

The Secret number is 200(11001000)

The result is as follows: (00101101 00011101 11011100) (10100110 11000101 00001100) (11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the image, only the 3 bits needed to be changed according to the embedded message. On average, LSB requires that only half the bits in an image be changed to hide a secret message. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. Still, human eye would not be able to discover these changes thus we can say that the message is successfully hidden.

8-bit images: In these images 1 bit of information can be hidden in each pixel. The color variation may occur and therefore, care should be taken in selecting the cover image. For example, a simple four-color palette of white, blue, green and red has corresponding palette position of 00, 01, 10 and 11 respectively. The raster values of four adjacent pixels of white, white, blue, and blue are 00, 00, 10, and 10.

The secret number is 01 (0001)

It will change the raster data to 00,00,10,11, which is white, white, and green, red. These changes in the color of image are visible and clearly highlight the weakness of using 8-bit images.

B. Transform domain Techniques

The cover image is transformed into other domain. The coefficients of the transformed domain will be used to place the secret data. Again the modified coefficients are transformed back into the spatial domain to obtain the stego image. These following are the advantages of transform domain techniques comparing with frequency domain techniques.

- These techniques are more sustainable to attacks.
- Transform domain techniques will embed data in frequency domain where as spatial domain techniques will embed data directly on the image.
- Transform domain techniques are stronger than spatial domain techniques.
- Most of the steganographic algorithms are using transform domain techniques as they are less exposed to compression, cropping and image processing.

There are two types of transform domain techniques are available.

C. Orthogonal Transform Techniques:

It uses sinusoidal functions [3].

- Discrete Fourier Transform Technique (DFT)
- Discrete Cosine Transform Technique (DCT)
- Discrete Wavelet Transform Technique (DWT)

- **DFT (Discrete Fourier Transform) Technique:**

DFT is used to transfer an image from spatial domain into frequency domain.

DFT is defined by the following equation:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y)\, e^{-j2z\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

$$u = 0, 1, 2, ..., M-1 \; and \; v = 0, 1, 2, ..., N-1$$

M and N are the size of image.

Inverse Discrete Fourier Transform (IDFT):

Fourier Transform (FT) methods introduce round off errors, thus it is not suitable for hidden communication.

The difference between a Discrete Fourier Transform and a Discrete Cosine Transform is that the DCT uses only real numbers, while a Fourier transform can use complex numbers.

$$f(x,y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v)\, e^{j2z\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

$$x = 0, 1, 2, ..., M-1 \text{ and } y = 0, 1, 2, ..., N-1$$

- **DCT (Discrete Cosine Transform) Technique:**

It represents an image as a summation of sinusoidal waves of varying frequencies and magnitudes [7]. For any input image 'x, calculate the DCT coefficients of the transformed output image 'y' by using the following equation.

For an input image for N x M pixels,

y(u,v) is DCT coefficient in u[th] row and v[th] column of the DCT matrix and x(m,n) is the intensity of the pixel in m[th] row and n[th] column of an image matrix.

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} x(m,n)\ \cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \quad \text{-------} \quad (1)$$

Where α_u and α_v are given by:

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{2}} & if\ u = 0 \\ 1 & if\ u = 1, 2.....N-1 \end{cases}$$

$$\alpha_v = \begin{cases} \frac{1}{\sqrt{2}} & if\ v = 0 \\ 1 & if\ v = 1, 2.....N-1 \end{cases}$$

The image is recreated by applying inverse DCT operation according to Eq. 2:

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} x(m,n)\ \cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \quad \text{------} \quad (2)$$

- **DWT (Discrete Wavelet Transform) Technique:**

A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena [5]. A signal can be better expressed as a linear decomposition of sums of products of coefficient and functions. A system with two-parameters is constructed, with one having a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal.

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image steganographic model is that the wavelet transform separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is always preferred over Discrete Cosine Transforms (DCT) because at various levels image in low frequency can offer corresponding resolution needed.

The use of DWT transforms mainly address the capacity of the Information-hiding system features and robustness. The hierarchical nature of the Wavelet representation allows multi-resolution detection of the hidden message, which is a Gaussian distributed random vector added to all the high pass bands in the Wavelet domain.

The Forward DWT Eq. is:-

$$W_\varphi(J_O, K) = \frac{1}{\sqrt{M}} \sum_n f(n)\varphi_{j\ o,k}(n)$$

$$W_\Psi \sum_n (j,k) = \frac{1}{\sqrt{M}} \sum_n f(n)\Psi_{J,K}(n) \quad for\ j \geq j_o$$

The complementary inverse DWT Equation is:-

$$f(n) = \frac{1}{\sqrt{M}} \sum W\varphi(J_O, K)\varphi j_{o,k}(n) + \frac{1}{\sqrt{M}} \sum\sum W_\Psi(j,k)\Psi_{J,K}(n)$$

Advantages:

- These methods hide messages in more significant areas of the cover-image, which make them more robust to attack than LSB.
- Transformations can be applied to the entire image, to block throughout the image, or other variants.

Disadvantages:

- Methods of this type are computationally complex.

D. Non-Sinusoidal Transform Techniques:

1) Haar transforms

1. Find the order N. Let n=log N
2. Determine p and q.

a. P ranges from 0 to n-1.

b. If p=0, then q=0 or q=1.
Else, $1 \le q \le 2^p$

3. The value k is determined as
$k=2^p+q-1$ and Z=0/Z,1/Z,2/Z…,(N-1)/Z
4. If k=0, then

$h_0(z)=h_{00}(z)= \frac{1}{\sqrt{N}}$ for Z ϵ(0,1)

Else

$$h_k(z)=h_{pq}(z)= \frac{1}{\sqrt{N}}\left[2^p \; if \; \frac{q-1}{2^p} \le z < \frac{(q-1)/2}{2^p}\right]$$

$$= \frac{1}{\sqrt{N}}\left[-2^{p/2} \; if \; \frac{q-1/2}{2^p} \le z < \frac{(q)}{2^p}\right]$$

= 0 for Z ϵ [0, 1]

2) Walsh transforms

The Walsh transforms is given as

$$w(u)=\frac{1}{N}\sum_{x=0}^{N-1} f(x)\prod_{i=0}^{n-1}(-1)^{[b_i(x)b_{n-1-i}(u)]}$$

The term h(x,y) is given as

$$h(x,y) = \frac{1}{N}\prod_{i=0}^{n-1}(-1)^{[b_i(x)b_{n-1-i}(u)]}$$

h(x,y) is called the kernel of Walsh transform.

3) Hadamard transforms

Like the Walsh transform the bases function Hadamard transform is +1 and -1. The 1D Hadamard transform kernel is given as

$$g(x,u)=\frac{1}{N}(-1)^{\sum_{i=0}^{n-1} b_i(x)b_i(u)}$$

The 1D Hadamard transform H(u) is given as

$$H(u)=\frac{1}{N}\sum_{x=0}^{N-1} f(x)(-1)^{\sum_{i=0}^{n-1} b_i(x)b_i(u)}$$ where $N=2^n$

III. CONCLUSION

There are many steganographic algorithms existing such as spatial domain and transform domain techniques. But according this study, transform domain techniques are more suitable for steganographic process as these techniques are resistant towards attacks.

REFERENCES

[1] Niels Provos and Peter Honeyman, Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy, 2003.

[2] Saiful Islam, Mangat R Modi, Phalguni Gupta, Edge-based Image Steganography, Springer 2014.

[3] Gurmeet Kaur, Aarti Kochhar, Transform Domain Analysis of Image Steganography, International Journal for Science and Emerging Technologies with Latest Trends, 2013.

[4] Anil Kumar, Rohini Sharma, A Secure Steganography Based on RSA Algorithm and Hash-LSB Technique, International Journal of Advanced Research in Computer Science and Software Engineering, July, 2013.

[5] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, A Secure Color Image Steganography In Transform Domain, International Journal on Cryptography and Information Security, Volume 3, No 1, March 2013.

[6] Deepesh Rawat, Vijaya Bhandari, A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image, International Journal of Computer Applications, Volume 64, 2013.

[7] Suchitra B, Priya M, Raju J, Image Steganography Based On DCT Algorithm for Data Hiding, International Journal of Advanced Research in Computer Engineering& Technology, Volume 2, November 2013.

[8] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital Image Steganography: Survey and Analysis of Current Methods, Elsevier, 2010.

[9] Hardik Patel, Preeti Dave, Steganography Technique Based on DCT Coefficients, International Journal of Engineering Research and Applications, Volume 2, 2012.

[10] Wien Hong And Tung-Shou Chen, A Novel Data Embedding Method Using Adaptive Pixel Pair Matching, IEEE Transactions On Information Forensics And Security, Volume 7, No. 1, February 2012.

[11] Niel F Johnson, Sushil Jajodia, Exploring Steganography: Seeing The Unseen, IEEE, 1998.

