Exploring the Techniques of Data Embedding in Images: A Review

Amanjot Kaur
(Student M.Tech IT)
CEC Landran Mohali, Punjab, India

Bikrampal Kaur, Ph.D
(Prof. IT Department)
CEC Landran Mohali, Punjab, India

ABSTRACT

Steganography is defined as the invisible communication between two communicating parties. For hiding communicated data many carrier file formats are present but the most commonly used are images. The data can be hidden by using Least Significant Bit(LSB)**,** *k*-Modulus Method(k-MM), Discrete Wavelet Transform(DWT) and Discrete Cosine Transform(DCT). The LSB and *k*-MM algorithms are implemented under spatial domain in which secret data is directly embedded in the bits of cover image whereas the DCT and DWT algorithms are under transform domain in which firstly images are transformed and then the message is embedded in the image. The comparison and performance of these techniques depend upon different parameters: MSE(Mean Squared Error), PSNR(Peak Signal to Noise Ratio), BER(Bit Error Rate), Capacity. This paper explains the different Steganography techniques for hiding the information in an image.

General Terms

LSB, DCT, DWT, MSE(Mean Squared Error), PSNR(Peak Signal to Noise Ratio), BER(Bit Error Rate), Steganography.

Keywords

LSB, DCT, DWT, MSE(Mean Squared Error), PSNR(Peak Signal to Noise Ratio), BER(Bit Error Rate), Steganography.

1. INTRODUCTION

Steganography is the art of sending confidential information in which communication takes place. According to R. Anderson et.al [1], the origin of "Steganography" derives from Greek and it means "cover writing". To hide secret information there can be different approaches, such as cryptography and steganography. In cryptography, data is less protected because it attracts the attention of attacker, whereas in steganography, the data is more secure than the cryptography because it hides the existence of information. The most common method is to use images to hide the data from the methods of steganography. Hiding the information in an image is called image steganography.

In this method, to hide the secret data the pixels of the images are altered so as unviewable to the others and the changes applied in the image are intangible. The image in which secret data is embedded called the cover image and the cover image in which the secret data has embedded is called the stego image. Over all the multimedia types most popular cover files are images for steganography. Many different image file formats exist in image steganography. According to A. Cheddad et.al [3], there are different steganographic algorithms which are used for different image file formats. There are two types of compression: lossy and lossless. In both compression types, they save space of storage, but their procedures are different. Lossy compression creates short files as it discards excess image data from the original image and also deletes details. Therefore, an outer person made close approximations of the original image, but do not made an exact duplicate. Joint Photographic Experts Group (JPEG) is an example of an image format that uses this compression technique, on the other side, Lossless method makes the message more robust and also hide messages in more significant areas of the cover image. In this way, the most suitable method for image steganography is lossless image formats. Because of redundancy the image files are very commonly used as a medium for steganography. Audio files contain less inessential information than image files. To use images as cover objects there are two techniques proposed. These techniques can be classified into the following two ways:

(1) Spatial domain techniques

(2) Transform domain techniques.

(1) Spatial domain techniques directly embed secret information in the intensity of the pixels, while in transform domain, images are transformed firstly and then the message is embedded in the image. A steganographer modifies the secret data and the cover medium in the spatial domain. In this method, encoding is at the level of the Least Significant Bit (LSB) or *k*-Modulus Method (*k*-MM).

(2) Transform domain techniques using Discrete Cosine Transformation (DCT) or Discrete Wavelet Transformation (DWT) the cover images are transformed firstly and after that data is hide inside them. In transform domain techniques, data is hidden in mathematical functions.

The image steganography embedding process can be understood from Figure 1.1 given below.

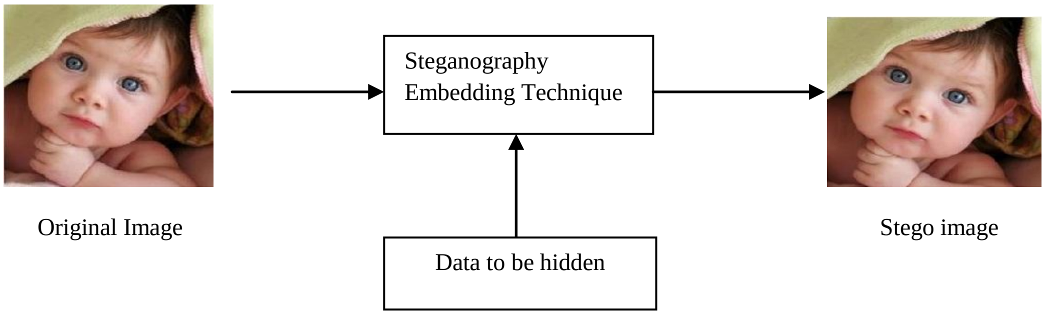

Figure 1.1:- Block diagram of a simple Image Steganography Embedding Process

The image steganography extraction process can be understood from Figure 1.2 given below

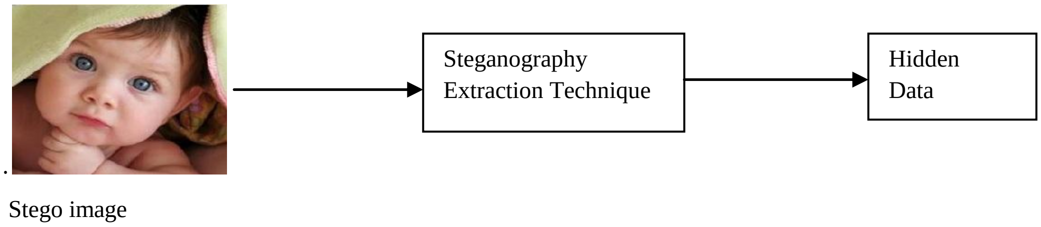

Figure 1.2:- Block diagram of Steganography Extraction from a Stego image

The remaining paper structured as follows: 2. Steganography Techniques, 3. Evaluation of image quality, 4. Conclusion.

2. STEGANOGRAPHY TECHNIQUES

To hide confidential information in an image there are many steganography techniques. In this section, different steganography techniques are discussed.

2.1 Least Significant Bit(LSB)

Least significant bit (LSB) based steganography is one of the techniques of spatial domain that hides secret information in the LSBs of pixel values without demonstrable deformations. According to T. Morkel et.al [2] to human eye, alterations in the value of the LSB are untraceable. Message bits can be embedded either simply or randomly in image. The least significant bit of several or all of the bytes inside an image is changed to a bit of the secret message. Digital images are primarily of two types (i) 8 bit images and (ii) 24 bit images. Three bits of information are embedded in each pixel in 24 bit images, in each LSB position of the three eight bit values one bit is embedded. According to A. Cheddad et.al [3], rising or declining the value by changing the LSB does not change the appearance of the image; much so the resulting stego image looks almost same as the cover image. One bit of information can be hidden in 8 bit images.

Assume the first three pixels (P1, P2, P3) of the cover image have the following binary values: [1 0 0 1 0 11 0], [1 0 1 0 0 0 1 0] and [1 0 1 1 0 1 1 1], correspondingly. To hide the secret message M whose binary value is [1 1 0], we replace the LSBs of P1, P2, P3 with bit stream M. These P1, P2 and P3 stego pixels have the following new values: [1 0 0 1 0 1 1 1], [1 0 1 0 0 0 1 1] and [1 0 1 1 0 1 1 0].

2.2 *k*- Modulus Method(*k*-MM)

k- Modulus Method (*k*-MM) steganography is under the spatial transformation. *k*- MM was primarily suggested by F. A. Jassim[4]. The radical aim behind *k*-MM is to transform the original image pixels into multiples of *k* (any positive integer value). According to F. A. Jassim et.al [5], the difference between the original image and the transformed image is hardly noticed by human eye. As said by [4], if the value of the *k* is upto 10 then the original image does not influence the Human Visual System (HVS).

Assume *k*- 2, the pixels value of the image lies between 0 to 255 then these values will be transformed as the multiples of 2 i.e. 0,2,4,6,8,….,254. In the same way, any integer value of *k* is multiples of that value but as the value of *k* is increasing the quality of the output image is decreasing in accordance with F. A. Jassim[6].

2.3 Discrete Cosine Transformation (DCT)

Discrete Cosine Transformation algorithm comes under the transformation domain techniques. In this technique, image of the spatial domain is firstly converted into frequency domain. According to Mamta Juneja et.al [7], it can extricate the original image into different frequency components in the manner of high frequency components, middle frequency components and low frequency components.

Assume that there is a 512×512 pixels image, the DCT technique firstly transformed the 512×512 image into 256×256 pixels blocks and then the data is hidden into low, middle and high frequency components as said by Krenn. R. [8].

2.4 Discrete Wavelet Transformation (DWT)

Discrete Wavelet Transformation algorithm comes under the transformation domain techniques. In DWT algorithm, it renovates spatial domain data into frequency domain data. Discrete Wavelet Transform lucidly dissections the low frequency data and high frequency data on a pixel by pixel basis that is why wavelets are used in the image steganographic model. As said by Prabakaran. G et.al [9], DWT principally concentrates on the capacity and robustness of the message hiding system.

Contemporary, a new DWT based algorithm is proposed by Vijay Kumar et.al [10] for hiding a secret message CH band of cover image is used. In this algorithm, secret information is embedded in the different bands of cover image.

3. EVALUATION OF IMAGE QUALITY

To evaluate the quality of the image there are different parameters, commonly used are Peak Signal to Noise Ratio(PSNR), Mean Squared Error(MSE), Bit Error Rate(BER), capacity and security. In this section, different parameters are discussed.

3.1 Mean Squared Error

According to K. B. Shiva Kumar [11], Mean-squared error between the original image and stego image is measured by:

$$MSE=\sum_{M,N}[I1(m,n)- I2(M,N)]^2/ M*N$$

In the input images, M, N is the number of rows and columns, correspondingly.

3.2 Peak Signal-to-Noise Ratio

By scaling the MSE according to the image range, Peak Signal-to-Noise Ratio (PSNR) avoids this problem [12]:

$$PSNR=10 \log_{10} 256^2/ MSE$$

The PSNR is deliberated in decibels (dB). As the value of the PSNR increasing the quality of the image is also increasing.

3.3 Bit Error Rate

Bit Error Rate (BER) is the reciprocal of the Peak Signal-to-Noise Ratio[13]:

$$BER=1/PSNR$$

If the value of BER is closer to zero it means the quality of the image is good.

3.4 Capacity

It refers to the how much secret information can be hidden into an image. Higher the capacity of the image to hide data better will be the technique. According to K Suresh Babu [14], capacity represented by bpp that is bits per pixel and MHC (Maximum Hiding Capacity) in terms of percentage.

3.5 Security

It refers to how much the information is secure from the steganalysis.

Comparison table of the parameters

Table 1.1:- Comparison Table of parameters

PARAMETERS	LSB	K-MM	DCT	DWT
MSE	0.000507	0.00043	0.00107	446.319
PSNR	81.077	50.7787	77.815	21.6343
BER	0.01233	0.19693	0.01285	0.04622
CAPACITY	LOW	MORE	MORE	LESS
SECURITY	HIGH	HIGHEST	HIGH	HIGHER

4. CONCLUSION

In foregoing years, for data hiding, steganography has become fascinated and vital field. In these past years, many researchers gave many techniques of data hiding. In this paper, foremost steganographic techniques are reviewed. In this paper, the quality estimation parameters are also reviewed. The above discussed techniques gratify these most significant parameters of steganography architecture.

5. REFERENCES

[1] Anderson, R. and Petitcolas, F. 1998. On the limits of steganography, IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, May 1998, pp. 474-481.

[2] Morkel, T. , Eloff, J.H.P. , Olivier, M.S. 2005. An overview of image steganography, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa, June 2005 pp. 1-11.

[3] Cheddad, A., Condell, J., Curran, K. and Kevitt, P.M. 2010. Digital image steganography: survey and analysis of current methods, Signal Processing Elsevier, vol. 90, no. 3, 2010, pp. 727-752.

[4] Jassim, F. A. 2013. k-modulus method for image transformation, International Journal of Advanced Computer Science and Applications, vol. 4, no. 2, 2013, pp. 267–271.

[5] Jassim, F. A. and Qassim, H. E. 2012. Five modulus method for image compression, Signal & Image Processing: An International Journal, vol. 3, no. 5, 2012, pp. 19-28.

[6] Jassim, F. A. 2013. A Novel Steganography Algorithm to Hide a Grayscale BMP Image in Two Grayscale BMP Images for Dual Secrecy, 2nd National Conference on Information Assurance(NCIA), vol. 4, no. 8, 11 Dec 2013, pp. 73-77.

[7] Juneja, M., Sandhu, P.S.2009.,Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305.

[8] Krenn. R. 2004. Steganography and Steganalysis, Internet Publication, January 2004. Stuti Goel, Arun Rana, Manpreet Kaur, “A Review of Comparison Techniques of Image Steganography,” Global Journal of

Computer Science and Technology Graphics & Vision, vol. 13, no. 4, 2013, pp. 9-14.

[9] Prabakaran. G, Bhavani. R. 2012.A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform, International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 2012, pp. 1096-1100.

[10] Kumar, V. and Kumar, D. 2010. Performance Evaluation of DWT Based Image Steganography, IEEE 2nd International Advance Computing Conference, 2010, pp. 223-228.

[11] Shiva Kumar, K. B., Raja, K. B., Chhotaray, R. K. and Pattnaik, S. 2010. Coherent Steganography using Segmentation and DCT, Computational Intelligence and Computing Research(ICCIC), IEEE-978-1-4244-5967-4/10, Dec 2010, pp. 1-6.

[12] Ming, C., Ru, Z., Xinxin, N., Yixian, Y. 2010. Analysis of Current Steganography Tools: Classifications & Features, International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), IEEE-0-7695-2745-0/06, Dec 2006, pp. 384-387.

[13] Beram Fariba Ghorbany. 2014. Effective Parametersof Image Steganography Techniques, International Journal of Computer Applications Technology and Research, vol. 3, no. 6, 2014, pp.361-363.

[14] Suresh Babu, K., Raja, K.B., Kiran Kumar K, Manjula Devi T H, Venugopal K R, Patnaik,L.M. 2008. Authentication of Secret Information in Image Steganography, TENCON 2008-2008 IEEE Region 10 Conference, 2008, pp. 1-6.