IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol-6, Special Issue-3, Apr 2018 E-ISSN: 2347-2693

Image Steganography using Edge Based Data Hiding in Dct Domain: An Overview

Nadish Ayub[1*], Arvind Selwal[2]

[1*] Department of Computer Science & IT, Jammu, India
[2] Department of Computer Science & IT, Jammu, India

*Corresponding Author: nadishbangi@gmail.com, Tel.: +91-7889-678423

Available online at: www.ijcseonline.org

***Abstract*—** Steganography is the art of concealing secret information in some given information. Steganography hides the existence of the message unlike cryptography which keeps the contents of message secret. Image steganography is the branch of steganography where secret information is hidden inside an image. There are various techniques of image steganography i.e., spatial domain and frequency domain. In this paper, a review of image steganography techniques is presented using qualitative parameters like robustness, embedding capacity and quantitative parameters like PSNR, SNR, MSE are taken into consideration for analyzing the efficiency of various techniques of image steganography. The study reveals that transform domain techniques are more robust than spatial domain techniques even though are more complex than spatial domain techniques. Furthermore, it is observed that edge based data hiding in DCT domain has more embedding capacity and is more robust than spatial domain techniques.

***Keywords*—** Imagesteganography,DCTdomain,datahiding.

I. INTRODUCTION

Steganography[1] is the art and science of communicating in such a way which hides the existence of the communication. Steganography is different from cryptography in the sense that cryptography keeps the content of message secret while as steganography keeps existence of message secret. There are various kinds of steganography i.e., image, text, video, audio, protocol. Digital images are most frequently used on the internet and hence images are the most popular cover objects for steganography.

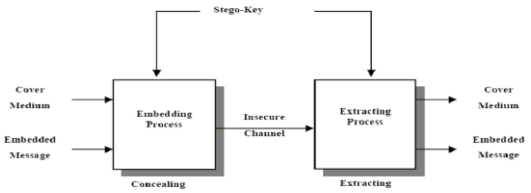

Fig. 1: The General Steganography System

Image Src:Samir Bandyopadhyay et al[2010]

A. *Image steganography Techniques*

The steganography algorithms have been classified as spatial/image and transform/frequency domain. Spatial domain techniques are applied on the pixels directly. The transform domain methods hide messages in more significant areas of the cover image, so this scheme seems to be robust than spatial domain.

1) Spatial Domain Scheme

All of these process some bits of the pixel or directly conceal the secret data by processing some bits. Some common spatial domain methods are based on PVD (Pixel value differencing) Based, LSB (Least significant bit) Based, Texture Based, Pixel Intensity Based, Edge Based Embedding Schemes,etc.Usually, the spatial domain methods are effective and complexity is medium. This creates less change in the medium and hides more data. But they are not that robust and could be destroyed by attacks more easily.

2) Transform Domain Scheme

Transform domain method is better than spatial domain method as these schemes hide the secret data in the particular region of the medium that is more robust. But this technique is more complex than the spatial domain method. "DWT" (Discrete Wavelet Transform), "DFT" (Discrete Fourier Transform), "DCT" (Discrete Cosine Transform), etc are transform domain methods.

3) Hybrid Scheme

This technique uses the combination of both spatial and transform domain. Although it provides good security but the complexity gets increased.

B. *Performance measures*

A steganography technique may be evaluated by a set of performance metrics, that are listed below[15] :

1) PSNR (Peak Signal to Noise Ratio):

It is the fraction between the maximum possible power of a signal and the power of corrupting noise .

$$\text{PSNR}=10\log_{10}\frac{(PV)^2}{MSE} \quad (1)$$

here *PV*=Peakvalue and *MSE*=Mean square error.

2) MSE (Mean Square Error): Mean Squared Error gives the average squared difference between a given image and a distorted image.

$$\text{MSE}=\sum_{i=1}^{n}\frac{(carr(i)-stego(i))^2}{A+B} \quad (2)$$

3)SNR (Signal to Noise Ratio): It gives the ratio of signal power to the noise power.

$$\text{SNR}=10\log_{10}\frac{\sum_{i=1}^{n}(carr(i))^4}{\sum_{i=1}^{n}(carr(i)-stego(i))^2} \quad (3)$$

In above equations, carr represents the carrier signal and stego represents the stego signal which is obtained after encoding. A and B represents the dimension of the input signal vector.

This paper has been divided into 4 sections. Section 1 gives the brief introduction of image steganography .Section 2 is the explanation of the literature review. Furthermore, in Section 3 comparative analysis of various image steganography is given in a tabular form. The Section 4 gives the conclusion.

II. BACKGROUND

Vijaya Raghava Kukapalli et al [12]have proposed an image steganography by using Enhanced pixel indicator method using most significant bit (MSB) compare .This paper presents an pixel indicator method by comparing three MSB bits at each pixel to conceal the data .They have used blowfish algorithm for encryption.

Terence Johnson et al[13] have presented a method of steganography in which they are using K Strange Points clustering algorithm. The authors have compared the results of this algorithm with K Means clustering algorithm. Results have shown that it works well with K Strange algorithm rather than K Means clustering algorithm.

Gurinder Singh et al[14] have presented a study of Magnetic Resonance Imaging(MRI) , its advantages and disadvantages, various types of MRI and comparative analysis of image steganography techniques to hide sensitive patient information into the stego medical image to ensure confidentiality. They segment the image using segment growing in order to find anatomical and non-anatomical regions. Anatomicals regions are those that contain sensitive information so for hiding the data they use non-anatomical by using LSB they could provide large embedding capacity.

Sounak Lahiri et al [15] have developed a robust approach for steganography in colored images in which they had used edge based data hiding in DCT domain .They have made use of various edge detectors and computed the performance parameters using all edge detectors. A high SNR and PSNR values were obtained. Data hiding in edges here is done using mathematical expressions. The encryption is performed on DCT coefficients and as such increases performance and prevents attack by an adversary. The proposed system had large capacity for embedding because color images are used.

Monika Gunjal et al[16] have proposed image steganography using Discrete Cosine Transform(DCT) and blowfish algorithm. This is the combination of cryptography and steganography to increase security of system. this approach calculates LSB of each DC coefficient and replace with each bit of secret message. Blowfish is an improvement over DES , 3DES, etc. designed to increase security and to improve performance.

Sherin Sugathan et al [17] have presented an improved LSB embedding technique for image steganography for RGB images .The results had shown that proposed method performs well when embedding secret data at higher LSB bit positions but this method had reduction in embedding capacity.

Champakamala et al[18] have presented a use of LSB algorithm for image steganography in which he had used modified LSB embedding algorithm as in conventional LSB technique, which requires eight bytes of pixels to store 1 byte of secret data but in proposed LSB technique, four bytes of pixels hold one message byte and remaining bits in the pixels are same.

Smitha GL et al [19] have made K.Naveen et al [2] have presented an approach to hide the data in different regions like edges because it is not detected easily by an attacker as edge pixels appear brighter or dimmer than other pixels in neighbourhood. The authors have used a technique in data can be embedded in edge pixels by using LSB approach. In simpleLSB and randomLSB an attacker can detect the presence of hidden message but this method is more secure than simpleLSB and randomLSB. They had used canny edge detector to detect edges and use LSB method to hide secret message.

Abdelhamid Awad Attaby et al [3] have presented a new methodology for transform domain JPEG image steganography technique that provides high embedding performance with less change in cover image. The algorithm used is DCT-M3 which uses modulus three of the difference between two DCT coefficients to embed two bits of the

compressed form of secret message. This algorithm has improved the embedding capacity by 16.7% approximately. message which is based on the modulus three of the difference between DCT coefficients of the cover image during JPEG compression process.

Sahar A.El_Rahman et al [4] have presented a comparison of image steganography based on DCT algorithm and steganography tool to conceal nuclear reactors sensitive information. The authors have used DC components of DCT for hiding secret bits in LSBs .The results indicated that the middle frequency has the more hiding capacity and gives less distortion.

Solomon O.Akinola et al [5]have presented a system in which they use hybrid technique of LSB and MSB algorithms. In this approach two bits LSB and MSB of cover images are replaced with a secret message. Then comparisons on the basis of PSNR , MSE and encoding time were made and the proposed technique produced a stego-image which shows less distortion in quality of image than "MSB" technique.

G.T. Shrivakshan et al [6] have proposed a comparison between edge detection techniques in image processing. The authors have made a comparison between Gradient-based (Robert, Prewitt and Sobel operators) and Laplacian (Marr-Hildreth, Gaussian Gabor filter and Gaussian canny) based edge detection techniques by taking case study of identifying a shark fish type .Laplacian based filters are found to be less sensitive to noise as compared to gradient based methods.

Shreya Gupta et al [7] have developed a hybrid technique including both steganography and cyptography in which the sensitive data is first encrypted using AES encryption algorithm and then this encrypted data is embedded in the coloured Cover image by using a hash based algorithm (MD5).This proposed system does not corrupt the image quality in any form. This algorithm was suitable for almost all image formats e.g., jpeg/jpg, Bitmap, TIFF & GIFF.

Saiful Islam et al [8] have proposed a technique which conceals sensitive message in the carrier image. To get the genuine edges, Canny edge detection has been used. The proposed system can withstand various types of structural and non-.structural attacks. This method uses 2-bit LSB for embedding, and decreases number of pixels to be distorted. Since there is significant change intensity of pixels but this change cannot be detected due to sharp difference in intensity of edge and non-edge pixel and thus embedding does not produce distortion.

Sudhanshi et al [9]have presented a review of transform domain techniques i.e., DCT and DWT for steganography. The authors have made a comparative analysis between the two techniques on the basis of various quantitative parameters like MSE, PSNR. The comparisons show that DCT has higher PSNR than DWT but DWT was more robust than DCT.DCT also gave best quality of image.

The proposed algorithm is applied to embed the compressed

Mamta jain et al[10] have presented a comparative analysis of LSB and LSB array method which is used usually in spatial domain. In the LSB techniques, substitution is performed upto 4 LSBs. The LSB techniques have larger capacity, but give moderate security as compared to techniques of other categories of digital image steganography. This review paper will help researchers to recognize the idea sand difference of LSB and LSB array methods in image steganography.

Ashley S. Kesley et [11]al have proposed a discrete wavelength transform approach for enhanced security in image steganography. The system proposed by them has low impact on quality of image and making it difficult to be detected by the attacker. The proposed system had provided good encryption also and improves the overall imperceptibility, security, data embedding capacity and robustness.

Sobel edge detection technique for image steganography in which they had used Edge Adaptive based on Least-Significant-bit Matched Revisited (LSBMR) approach using Sobel edge detection. In this paper they are proposing the latest Steganography algorithm-Edge Adaptive based on Least-Significant-bit Matched Revisited (EALSBMR) approach with the help of Sobel edge detection. The presented technique uses image-processing technique to detect edges. Sobel edge detection technique was applied on cover images to determine edges. Then sharper edges were exploited for embedding secret bits.

Aditi Sharma et al [20] have proposed a secure steganography technique using MSB. In this proposed method they had used pixel indicator method to hide secret information. In addition to this they have used central portion of image to hide secret information for security reasons. Red channel of RGB image is used as an indicator .To hide the secret message in 5^{th} and 6^{th} bits of either green channel or blue channel for embedding. Green channel is used if there are even number of 1's in Red channel else blue channel is used.

Ammad Ul Islam et al[21] have proposed an improved Image steganography technique based on MSB Using Bit Differencing in which bit 5 is used to store secret message bits based on the difference of bit no 5 and bit no 6 .Proposed system has improvement over SNR and is also secure because attackers cannot guess information is stored in MSB.

Table I: Comparative analysis of various image steganography techniques

YEAR	NAME OF TECHNIQUE	PERFORMANCE	AUTHOR	Ref.
2017	MSB	PSNR=54.646	Aditi Sharma	[20]
2017	Sobel edge detection technique	SNR=39.632 PSNR=43.616	Smitha GL	[19]
2017	Improved LSB	PSNR=52.17 MSE=0.39	S. Sugathan	[17]
2016	Edge Based Data Hiding In DCT Domain		S. Lahiri	[15]
2016	MRI Medical Image and Steganography		G. Singh	[14]
2016	k strange points clustering	Purity (with Iris Dataset=0.86	T. Johnson	[13]
2016	DWT		A. S. Kelsey	[11]
2016	LSB and LSB Array	MSE=0.41 PSNR=51.93	M. Jain	[10]
2016	Hybrid technique of spatial domain		C. H. Shreya Gupta	[7]
2016	DCT-M3		A. A. Attaby	[3]
2016	DCT LSB		Sahar A.El_Rahman	[4]
2015	Review of transform domain techniques	DCT PSNR=High DWT PSNR=Low	S. Sharma	[9]
2015	Combined LSB-MSB		S. O.Akinola	[5]
2014	Edge based image steganography	Accuracy=51.196	S. Islam	[8]
2014	MSB with PIM		V. R. Kukapalli	[12]
2014	DCT and Blowfish algo		M. Gunjal	[16]
2014	LSB		B. S. Champakamala	[18]
2012	Comparision of various edge detection techniques		G. T. Shrivakshan	[6]
2012	EDGE Based Steganography		K. N. Brahmateja	[2]

III. COMPARATIVE ANALYSIS

As shown in Table 1, a comparative analysis of various image steganography techniques is presented in a tabular form. After going through literature it may be revealed that most of the image steganography techniques were evaluated using only one or two performance metrics. LSB technique proposed by S. Sugathan [17] results in low embedding capacity. Futhermore, the simple LSB technique exhibits low security. The MSB image steganography technique shows a tradeoff between security and quality of image. Furthermore, it is also revealed that transform domain image steganography is more robust than spatial domain image steganography techniques and edge based data hiding have good embedding capacity .

IV. CONCLUSION:

After going through literature it may be revealed that most of the image steganography techniques were evaluated using only one or two performance metrics. Furthermore, the simple LSB technique exhibits low security. The MSB image steganography technique shows a trade-off between security and quality of image. Furthermore, it is also revealed that transform domain image steganography is more robust than spatial domain image steganography techniques and edge based data hiding have good embedding capacity.

ACKNOWLEDGMENT

We are thankful to the authorities of Central University of Jammu for providing necessary platform and all the facilities for carrying out the work.

REFERENCES

[1] T. Morkel, M. S. Olivier, and S. Africa, "AN OVERVIEW OF IMAGE STEGANOGRAPHY."

[2] K. N. Brahmateja, G. L. Madhumati, and K. R. K. Rao, "Data Hiding Using EDGE Based Steganography," vol. 2, no. 11, pp. 285–290, 2012.

[3] A. A. Attaby, M. F. M. Mursi Ahmed, and A. K. Alsammak, "Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3," *Ain Shams Eng. J.*, 2016.

[4] S. A. El Rahman, "algorithm and steganography tool to hide nuclear reactors," *Comput. Electr. Eng.*, vol. 0, pp. 1–20, 2016.

[5] S. O.Akinola and A. A.Olatidoye, "On the Image Quality and Encoding Times of LSB, MSB and Combined LSB-MSB Steganography Algorithms Using Digital Images," *Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. 4, pp. 79–91, 2015.

[6] G. T. Shrivakshan and C. Chandrasekar, "A Comparison of various Edge Detection Techniques used in Image Processing," *Int. J. Comput. Sci. Issues*, vol. 9, no. 5, pp. 269–276, 2012.

[7] C. H. Shreya Gupta, Akshay Kalra, "A Hybrid Technique for Spatial Image Steganography," *3rd Int. Conf. onComputing Sustain. Glob. Dev.*, pp. 643–647, 2016.

[8] S. Islam, M. R. Modi, and P. Gupta, "Edge-based image steganography," *EURASIP J. Inf. Secur.*, vol. 2014, no. 1, p. 8, 2014.

[9] S. Sharma and U. Kumar, "Review of Transform Domain Techniques for Image Steganography," *Int. J. Sci. Res. ISSN (Online Index Copernicus Value Impact Factor*, vol. 4, no. 5, pp. 194–197, 2015.

[10] M. Jain and S. K. Lenka, "A Review of Digital Image Steganography using LSB and LSB Array," vol. 11, no. 3, pp. 1820–1824, 2016.

[11] A. S. Kelsey and C. M. Akujuobi, "A Discrete Wavelet Transform Approach for Enhanced Security in Image Steganography," vol. 5, no. 1, pp. 10–20, 2016.

[12] V. R. Kukapalli, B. T. Rao, and B. S. Reddy, "Image Steganography by Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare," vol. 15, no. 3, pp. 97–101, 2014.

[13] T. Johnson *et al.*, "Improved steganography using enhanced k strange points clustering," *Int. J. Appl. Eng. Res.*, vol. 11, no. 9, pp. 6881–6885, 2016.

[14] G. Singh, "MRI Medical Image and Steganography," vol. 4, no. 2, pp. 2–5, 2016.

[15] S. Lahiri, P. Paul, S. Banerjee, S. Mitra, A. Mukhopadhyay, and M. Gangopadhyaya, "Image Steganography On Coloured Images Using Edge Based Data Hiding In DCT Domain," *Inf. Technol. Electron. Mob. Commun. Conf. (IEMCON), 2016 IEEE 7th Annu.*, 2016.

[16] M. Gunjal and J. Jha, "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm," *Int. J. Comput. Trends Technol.*, vol. 11, no. 4, pp. 144–150, 2014.

[17] S. Sugathan, "An improved LSB embedding technique for image steganography," *Proc. 2016 2nd Int. Conf. Appl. Theor. Comput. Commun. Technol. iCATccT 2016*, no. 4, pp. 609–612, 2017.

[18] B. S. Champakamala, K. Padmini, R. D. K. A. Professors, and D. Bosco, "Least Significant Bit algorithm for image steganography Overview of Steganography," *Int. J. Adv. Comput. Technol.*, vol. 3, no. 4, p. 5, 2014.

[19] T. Nadu, "Sobel edge detection technique implementation for image steganography analysis .," pp. 1–7, 2017.

[20] "A Secure Steganography Technique Using MSB," vol. 9359, no. 6, pp. 208–214, 2017.

[21] Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan , Toqeer Mahmood3, Adnan Khan Usman Ali2, Muhammad Naeem" An Improved Image Steganography Technique based on MSB using Bit Differencing",IEEE awe 978-1-5090-2000,2016.

Authors Profile

Nadish Ayub has completed Bachelor of Technology from University of Kashmir,Jammu and Kashmir in 2015 and is currently pursuing Master of Technology from the department of computer science and IT from Central University of Jammu.Her area of interst is Image processing and Neural Networks.

Arvind Selwal is presently working as Assistant Professor in Department of Computer Science and IT in Central University of Jammu, J&K, India. He holds B.Tech., M.Tech. and Ph.D. degrees in Computer Science and Engineering. He has authored two books on the topic theory of computation and database systems. He has published more than 14 research publications in reputed international journals indexed in popular databases like SCI, Scopus and DBLP. He has more than 13 years of experience in teaching.

