Working and Comparative Analysis of Various Spatial based Image Steganography Techniques

Dimple Anandpara[1]
Ph.D. Scholar
School of Computer Science,
R.K. University,
Rajkot

Amit D. Kothari[2], Ph.D
HOD and Associate Professor,
ITM Universe,
Vadodara

ABSTRACT

Steganography is the technique to the fact that communication is taking place, by hiding secure information in other information. Secret data can embed in different types of objects like text file, audio, image or video but image is commonly used as carrier file for steganography. For hiding secret information a large variety of image steganography techniques are available with their respective pros and cons. Some algorithm provides more payload capacity while some provide more robustness against attack. This paper provides working and comparative analysis of some of the existing spatial based image steganography techniques.

General Terms

Data Hiding

Keywords

Steganography, spatial domain, LSB

1. INTRODUCTION

Now a day internet is widely used for information transfer. So the security of the information is the prior concern. There is a need to hide information within other object.

There are two ways to hide secret message, like ***Cryptography*** and ***Steganography***. Cryptography makes the data unreadable to outsiders by various transformations, whereas the methods of steganography hide the existence of messages.

The word **Steganography** is derived from the Greek words ***"stegos"*** meaning "cover" and ***"grafia"*** meaning "writing" defining it as **"covered writing"**. **Steganography** used by the military, revolutionaries, spies and perhaps terrorists.

Steganography can be used in a large amount of data formats in the digital world of today. The most common data formats used are .txt, .doc, .bmp, .gif, .jpeg, .mp3, .avi and .wav etc. Text steganography techniques are easy to implement but the lacking of using text as carrier for sending message is that it is less robust from attack and less amount of redundant data for embedding secret message.

One can hide secret messages in "noise" (and in frequencies which humans can't hear) part of audio, but to use audio as cover object is less robust because of the sensitivity of the Human Auditory System(HAS). While using video steganography, the effect on video quality has to be kept in mind to achieve a secure communication. Human Visual System [HVS] and Human Auditory System [HAS] both affecting to the video steganography techniques robustness. The scope of using image as stego object is more because user can use any file format like BMP, JPEG, PNG, and GIF for embedding secret data. Advantage of using image as cover objects for transferring information is that it provides good payload and more robustness then other media but still there is a need for developing a technique which provides good tradeoff between robustness and payload capacity.

This paper is intended to provide an overview of the different spatial based algorithms used for image Steganography. The paper is structured as follows:

In section no.1 working of the most popular spatial based image steganography algorithms is discussed. Section 2 provides comparative analysis of all these techniques based on different parameters and in Section 3 conclusion and future scope is reached.

2. TYPES OF IMAGE STEGANOGRAPHY TECHNIQUES

The image steganography techniques can divide into two groups.

- **Spatial Domain based Image Steganography:**

The intensity of pixels used for embedding secret message in this technique. Advantages of spatial domain based steganography techniques are high payload capacity, less complex to implement and imperceptibility of hidden data. But the major drawback is its vulnerability to various simple statistical analysis methods.

- **Transform Domain based Image Steganography**:

This technique, first transforms the cover-image into its frequency domain then the secret data is embedded in frequency coefficients. Advantage includes more robust against simple statistical attacks but less payload capacity.

The common spatial domain Image steganography techniques are:

- Least significant bit substitution method (LSB)
- Random pixel embedding method (RPE)
- LSB Matching Technique
- Color component based method
- SLSB Technique
- Pixel value differencing (PVD) method
- Edges based data embedding method (EBE)
- Pixel indicator based method
- Pixel Intensity based method
- Palette based technique
- GLM (Gray level modification) technique
- BPCS method
- Patchwork method

2.1 Working of Spatial based Image Steganography Techniques

2.1.1 LSB substitution Technique

LSB substitution technique [4] which simply substitutes LSB of image pixels sequentially with message bit.

Eg. **10101011** message stream

Image pixels are…..

10101111 10101011 11111111 10101010 101010101 11111110 11010101 11001100

New image pixels after inserting message stream

10101111 10101010 11111111 10101010 101010101 11111110 11010101 11001101

This method is easy to implement but provide less payload capacity because only one bit of message embeds per pixel and less robust because message bits are added in sequence of the image pixel so easily known by the intruder. To improve robustness new LSB based image steganography technique [5] proposed in which the message bits not embedded sequentially to the image pixels but the cover image divided into fixed size blocks and embeds the secret bits into each block. To improve payload capacity and robustness of LSB substitution technique in the proposed image steganography technique [6] the secret data first encrypted and then compressed using LZW compression technique. The Knight Tour algorithm, used for embedding compressed data so it will spread out to the image and increase the robustness of the method.

2.1.2 Random Pixel Embedding Technique (RPE)

The RPE technique[12] not embed secret message bits sequentially like LSB substitution technique[4] added into random position for increasing robustness against attack. Last two bits of each random position pixel used for embed message.

2.1.3 LSB Matching Technique

In LSB matching technique[10] not like LSB substitution in which LSB of the image replaced with the secret data bit but the message bits are embedded to cover image by adding 0 or 1 or-1 to the pixel of cover image.

2.1.4 Color Component Based Technique

In Color component based technique [7] color cycle algorithm is used. In this algorithm all the three colors are used for embedding data. Maximum 4 bits can added to each color. And all the colors are treated in same manner. Message bits are added sequentially to the pixels of image. This technique used for color image but the main drawback of this technique is that it treats all the three colors of the pixel equally for embedding secret bits which is less robust against statistical attack.

2.1.5 SLSB (Selective LSB) Technique

In SLSB color component based technique [8] all the color component of pixel are not used for embedding secret message bits but using sample pair analysis only one color component selected for embedding secret data. LSB matching technique is implemented after embedding secret data to reduce the distance of color between stego color and original color.

2.1.6 Pixel Value Differencing (PVD) Technique

The PVD method [13, 14] first find difference between two non overlapping neighborhood pixels, then on the base of difference value decide the pixel belongs to edge or smooth area. The number of bits embeds per pixel on the base of difference value. The secret data bits are embedded more into edge pixels then non-edge pixels. But both the methods [13, 14] can use for gray scale image only. For RGB color image bi- directional Pixel Value Differencing method [15] can used in which difference between two pixels found in both the side .That will improve both payload capacity and security of message.

2.1.7 Edge based Data Embedding Technique

In edge based data hiding technique [16] edge pixels are found using canny edge detection technique and then the secret data are stored in the 3 LSBs of every color channel of edge pixels only. The edge area can tolerate more changes then smooth area so the robustness will increase by this technique but the payload capacity is less because non-edge area pixels are not used for embedding data. To improve payload capacity hybrid edge detector technique [17] is developed in which the combination of both canny and fuzzy edge detection techniques is used. In this technique different amount of data bits embedded to edge-pixels and non-edge pixels but this technique apply only to gray scale image not the color image.

2.1.8 Pixel Indicator Technique

In RGB channel based pixel indicator technique[18] out of three color channels one color channel is used as indicator channel and other two channels are used as data channel. The indicator channel indicates whether data bits embed to both of data channels or not. In this technique image is divided into number of blocks and for each block decide indicator channel according to the color whose total value in particular block is maximum. To improve robustness in RGB channel based image steganography technique[19] same indicator channel not used for all the pixels but the image first divided into 4 sub images then use either default (i.e. red color) or user defined pixel indicator channel in zing zang manner.

2.1.9 Pixel Intensity based Technique

The color intensity based image steganography technique [20]. used for color image. In this technique out of 3 color channels one channel is used as a indicator channel and other two channels used to store secret message. Unlike pixel indicator based technique in this technique any channel is used as indicator channel no sequence is maintain so robustness will increase. In this technique number of bits added depend upon color intensity, if intensity is less then more number of bits are added and vice versa.

2.1.10 Palette based Technique

The palette based image steganography technique [21] support only GIF or PNG format with maximum 256 colors. In this technique message bits not directly embed to the image pixel but palette table of the image used for data embedding. In this technique by quantizing two similar colors a and b create new color entry then assign binary choice 0 or 1 for the selection of color a and b. This technique reduces distortion of image after embedding data. Payload capacity of this technique is low.

2.1.11 Gray Level Modification (GLM) Technique

Gray level modification technique [1] modifies gray level values of the image pixels for mapping secret data. This is a very simple method to implement.

2.1.12 BPCS Technique

In BPCS technique [3] the image divided into bit-planes and then it replace complex regions of each bit-plane of with random binary pattern. Use B-W border based complexity measure for region segmentation.

2.1.13 Patchwork Technique

In patchwork technique [2] the researchers proposed a statistical approach for data hiding. In this technique two patches are chosen randomly that is X and Y. All the pixels in patch X is lightened while the pixels in patch Y are darkened. The intensity of the pixels in the one patch is increased and in another patch decreased by a constant value. This technique is more robust against image manipulation because two copies of secret data stored in image.

2.1.14 Separable Reversible Data Hiding Technique (SRDH)

In Separable Reversible Data Hiding Technique [11] two keys are used one is encryption key and another is data hiding key. First the image is encrypted using encryption key then the image is compressed using data hiding key to embed secret data bits. Four positions (5, 6, 7, and 8) bits of randomly selected pixel are used for embedding secret data. In this technique secret data embedded to the image in lossless manner so that the image can extract as it is without any minor distortion that occurs due to data embedding. Another advantage is that data can extract from an encrypted image separately without decrypting the image. Both the extraction of image and data can separate at receiver side.

3. COMPARATIVE ANALYSIS OF SPATIAL BASED IMAGE STEGANOGRAPHY TECHNIQUES:

All the above mentioned algorithms for image steganography have different strong and weak points. There are many parameters that are used for define the imperceptibility of an algorithm. These parameters are as follow.

Payload Capacity: Payload capacity indicates amount of secret data that can embed to the cover media.

Robustness against statistical attack [9]: Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. For the performance measurement of image Pick- Signal-to-Noise Ratio (PSNR) will calculate. If the PSNR ratio is high then it indicates less distortion of image after embedding secret data that will increase robustness against statistical analysis.

Complexity: The complexity of encoding and decoding the message is another consideration. If more complex algorithm then more time require for both encoding and decoding operation.

Image Type Supported: There are different types of image formats like GIF, JPEG, JPG, PNG, BMP etc. There is a need of steganography technique which supports different types of image format.

On the base of above parameters comparative analysis of different image steganography techniques is given in Table-I.

Table 1: Comparative analysis of Spatial Based Image Steganography Techniques

Method	PSNR Value (in Db)	Payload Capacity	Complexity	Image Type Supported
LSB Substitution Method[5]	67.3	1 bit per 8 pixels	Low	Gray scale image
Enhanced LSB Substitution Method[6]	59.86	1 bpp	Low	Gray scale image
LSB Matching Technique [23]	50.13	1.583 bpp	Medium	Gray scale image
Color component based Method[7]	31.49	Maximum 4 bpp	Low	BMP -24
Edge Based Data Embedding Method[16]	51.1	0.5bpp	Low	Gray scale image
Pixel Indicator Based Method[18]	50.31	Maximum 4 bit per pixel of data channel	Low	BMP-24
Intensity Base Method[20]	49.66	Maximum 4 bits per pixel per data channel	Low	BMP-24
DHPVD Method[13]	49.45	Maximum 6 bits in difference of two pixels	Medium	Gray scale image
Bi-Directional PVD method for	52.25	1 bpp	Medium	BMP-24

color image[15]				
Palette based Method[21]	37.51	Maximum 2.7 bits when all colors are grouped	High	Palette based image format (GIF,PNG)
Separable Reversible Data Hiding Method[11]	45.85	3 bpp	High	Any image format (jpg, jpeg, gif, png, bmp etc.)
GLM Method[22]	50	1 bpp	Low	Gray scale image

The performance of steganography techniques cam mainly measure by its robustness against steganalysis. So, the comparative analysis of above given techniques on the base of PSNR value is given below in fig 1.

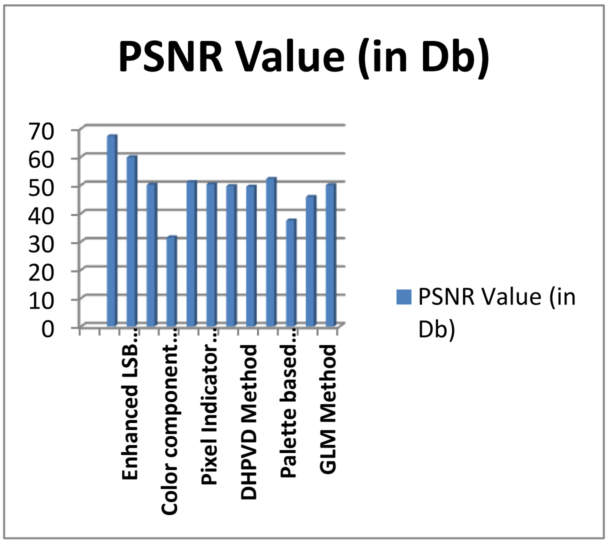

Fig 1: Comparative analysis on the base of PSNR value

4. CONCLUSION AND FUTURE SCOPE

This paper discuss certain popular spatial based image steganography techniques and also give comparative analysis of these techniques on the base of four parameters payload capacity, PSNR value, complexity and type of image format supported.. After analysis the author reveal that there is a tradeoff between mainly two parameters payload capacity and robustness of the technique. The PSNR ratio obtain by LSB based technique is high then other techniques discuss in this paper and also easy to implement but the payload capacity and robustness against statistical attack is very low. While the Separable reversible data hiding technique is more robust against attack by intruder because in this technique image first encrypted and then data embed in lossless manner. Author also analyze that the techniques based on grayscale image have less payload capacity then color component based techniques.

Main object of this study is to know what the lacking aspects of current spatial based image steganography techniques. So, in future this study can use as a base to develop some new techniques which provide more robustness and good embedding capacity by removing the loopholes associated with the existing techniques.

5. REFERENCES

[1] Potdar, V., and Chang, E "Gray Level Modification Steganography for Secret Communication" IEEE International Conference on Industrial Informatics, Berlin, Germany, 2004.

[2] W. Bender, D. Gruhl,N. Morimoto and A. Lu "Techniques for data Hiding" IEEE IBM System Journals, Vol. 35, 1996.

[3] E. Kawaguchi, R.O. Eason "Principal and Applications of BPCS Steganography", Proc of SPIE, Vol. 3528, pp. 464-473, 1998.

[4] Chin-Chen Chang, Min-Hui Lin, Yu-Chen Hu "A Fast And Secure Image Hiding Scheme Based on LSB Substitution" International Journal of Pattern Recognition and Artificial Intelligence, 2002.

[5] Omer Kurtulud ,Nafiz Arica "A New Steganography Method Using Image Layers" IEEE Computer and Information Sciences, 2008.

[6] Morteza Bashardoost, Ghazali Bin Sulong and Parisa Gerami "Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression" International Journal of Computer Science, 2013.

[7] Lip Yee Por, Delina Beh,Tan Fong Ang and Sim Ying Ong "An Enhanced Mechanism for Image Steganography Using Sequential Color Cycle Algorithm" The International Arab Journal of Information Technology, 2013.

[8] Juan José Roque, Jesús María Minguet "SLSB: Improving the Steganographic Algorithm LSB" Universidad Nacional de Educación a Distancia (Spain).

[9] T. Mokel, J.H.P.Eloff, M.S.Olivier "An Overview Of Image Steganography" in proceedings of the fifth annual Information Security, South Africa , 2005.

[10] Shang-Kuan Chen, Ja-Chen Lin "Image hiding by LSB matching of higher payload" IEEE, Sixth International Conference on Genetic and Evolutionary Computing, 2012.

[11] Vinit Agham, Tareek Pattewar "A Novel Approach Towards Separable Reversible Data Hiding Technique" IEEE, 2014.

[12] B. Karthikeyan, V. Vaithiyanathan, B. Thamotharan, M. Gomathymeenakshi and S. Sruti "LSB Replacement Steganography Using Psudoranomise Key Generation" Research Journal of Applied Sciences, Engineering and Technology, 2012.

[13] J. K. Mandal, AKhamrui "A Data-Hiding Scheme for Digital Image Using Pixel Value Differencing (DHPVD)" IEEE Electronic System Design (ISED), 2011.

[14] X. Liao, Q. Y. Wen, and J. Zhang "A steganographic method for digital images with four-pixel differencing

and modified LSB substitution" journal homepage: www.elsevier.com/ locate/ jvci.

[15] Himakshi, Harsh Kumar Verma, Ravindra Kumar Singh, Charan Kamaljit Singh "Bi-Directional pixel-value differencing approach for RGB Color Image" IEEE 2013.

[16] Youssef Bassil "Image Steganography based on a Parameterized Canny Edge Detection Algorithm" International Journal of Computer Applications, Vol. 16, No.4, December 2012.

[17] Wen-Jan Chen, Chin-Chen Chang, T. Hoang Ngan Le "High payload steganography mechanism using hybrid edge detector" journal homepage www.elsevier.com/locate/eswa.

[18] Gandharba Svalin, Saroj Kumar Lenka "A Novel Approach to RGB Channel Based Image Steganography technique" International Arab Journal of Technology, 2012.

[19] P.Mahimah, Mrs.R.Kurinji "Zigzag Pixel Indicator based Secret Data Hiding Method" IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[20] M.Shobana, R.Manikandan "Efficient Method for hiding data using color intensity" International Journal of Engineering and Technology (IJET), Vol 5 No 1, Feb-Mar 2013.

[21] Xuefeng Wang, Zhen Yao and Chang-Tsun Li "Palette Based Image Steganographic Method Using Color Quantization" IEEE Image Processing, 2005.