International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

An Improved Noise Resistant Image Steganography Technique Using Zero Cross Edge Detection Method

Mohan Singh Kachera[1], Gaurav Gupta[2] and Neeraj Jain[3]

[1]*M.Tech. Scholar, Department of Electronics and Communication, Rajasthan Technical University, India*

[2]*Assistant Professor, Department of Electronics and Communication, Rajasthan Technical University, India*

[3]*Assistant Professor, Department of Electronics and Communication, Rajasthan Technical University, India*

Abstract— *Steganography is derived from two Greek words i.e. 'Stegno' and 'Graphy'. 'Stegno' means 'cover' and 'graphy' means 'writing'. It is an essential part of information security which secures the secret data from eavesdropper. Steganography hides the existence of secret data in order to secure it. Least Significant Bit Insertion technique is applied to hide the secret information. This method modifies the least significant bit of each pixel of cover image. An interesting feature of randomization is that it provides improved image parameters i.e. Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Tamper Assessment Function (TAF). At the retrieval side, retrieve the bit stream from LSB of the edge pixels of the stego image for extracting the secret message from the cover image. De-randomization is applied to the bit stream using the same stego keys which were used for randomization. The proposed method gives much better results in terms of PSNR, MSE and Robustness against various noises like Salt & pepper noise, Poisson noise, Gaussian noise and Speckle noise.*

Keywords— Least Significant Bit (LSB) Technique, Mean Square (MSE), Peak Signal to Noise Ratio (PSNR), Tamper Assessment Function (TAF), Region of Interest (ROI).

1. Introduction

Steganography is the art and science of imperceptible communication. This is accomplished through hiding secret information in other information, thus hiding the survival of the communicated information. The word Steganography is derived from Greek words "stegos" means "cover" and "grafia" means "writing" defines it has "covered writing". In image steganography the secret information of data is hidden exclusively in images. Steganographic technology thus embeds hidden information in unreadable cover media so as not to stimulate an auditor's suspicion. In the past, people used invisible ink or hidden tattoos to convey steganographic data. Today, computer and internet technologies provide easy to use communication channels for steganography. Essentially, the information hiding process starts by identifying a cover medium's redundant bits (those that can be changes without destroying that medium's integrity).The embedding process generate a stego medium by replaced these redundant bits with data from the secret message.

2. Literature review

Aruna Mittal [1] proposes a new method for embedding secret information within skin and as well as in the edge area, as it is not much sensitive to Human Visual System. Firstly, skin tone detection method is performed on input image using HSV (Hue, Saturation and Value) color model. Second the cover image is transferred in frequency domain. It is performed by using double density discrete wavelet transform. After that the payload is calculated. Finally the secret information embedding is performed of high frequency sub band by tracking skin pixels. Before performing all steps cropping on input image is performed. Then cropped image region embedding is done. In which the embedding process affects only certain Region of Interest other than entire image. Then DD-DWT stego image is produced. Thereafter IDD-DWT image is merged with original image and final stego image is produced. This paper gives a review of steganography and its various techniques, its advantages and disadvantages, applications and comparison with cryptography techniques. Nowadays, data communication with security is basic necessity in

this internet era and this is most important factor in today's world. For protecting our secret data from an unauthorized person, it is very important to give security to information. By using steganography techniques secret message can be hidden inside a cover and the cover may be text, image, audio and video file. Vandana M. Ladwani et al. [3] categorized the Steganography techniques on the basis of spatial and frequency domain techniques. For authentication of the image paper presents a modulus technique with cryptography. To send a secret message from the sender to the receiver the message is firstly encrypted using DES encryption algorithm then using proposed embedding algorithm. At the receiver side, the secret message is retrieved using the proposed method. Image is divided into blocks of two pixel size after that critical function is evaluated. Intensity of any one of the pixel is modified based on the value of the critical function to hide the message information. Proposed work provides better PSNR. Saiful Islam et al.[4] proposes Steganography technique in which canny edge detection method is used for calculating the edge map. The selection of edges for embedding is dependent on the size of payload and the image. As the size of payload increases, a weak threshold are selected for getting edge pixels so that more edges can be selected to accommodate the increased amount of information. For a payload size, the sharpest edges are selected to embed the message. Anant M. Bagade et al. [5] proposed morphing concept for image steganography is used to overcome the limitations of the LSB that is less embedding capacity, poor quality of stego image, and imperceptibility. Author considers the image performance parameter like the PSNR to improve stego image quality and standard deviation as a measure to morphed image selection, respectively. The stego keys are generated and used to embed and extract the secret image. Author used a method of image morphing to improve steganography method by enhancing the hiding capacity, stego image quality, and imperceptibility. Sneha Arora et al. [7] proposed a technique to hide the text data into the color images using edge detection method. The changes in edges cannot be differentiated well so edges can hide more data without losing quality of an image. In this technique, edges are detected by scanning using 3x3window of the cover image and then text message is concealed in edges of the image. The proposed method achieved high embedding capacity and high quality of encoded image. K. Naveen BrahmaTeja et al. [8] gives an idea to embed data into random pixels instead of data embedding sequentially in pixels. The edge based Steganography is to embed secret data in the position of edge pixels, which meets the requirements of both in perception and robustness, but proposed method causes speckles in the image. An attacker has less suspicion of the existence of information bits in edges, because pixels in edges appear to be either much brighter or dimmer than their neighbors. So, author proposed a novel technique to hide data in the edge pixels of the image by extending the least significant bit embedding. Author hides data in the edge pixels and thus ensures better security against attackers.

3. Proposed Method

In this paper edge pixels were selected using zero cross edge detection in order to hide the secret message. One simple method to hide the data is "Least Significant Bit Insertion". The selection of pixels in which the secret message will be embedded is very essential part because modified pixels of the image where there are pixels that are most like their neighbors are much more noticeable to the naked eye. For embedding data, edge map is created for selected edge pixels. Here secret message is in the form of 8-bit gray scale image of peppers with size of 30 x 30 and all 8-bit pixels of that image are converted into bit stream. In this method adding the different types of noise like Gaussian noise, Speckle noise, Poisson noise, Salt & pepper noise etc. It gives the improved image parameter i.e. PSNR, MSE and TAF. At the retrieval side, the extraction method is considered as the inverse of the embedding method, although the embedding and extraction algorithms may be created such that extraction is not absolutely mathematical inverse of the embedding method.

Embedding and Retrieval Algorithm

This method aims to select the edge pixels in the image. In order to increase the embedding capacity 1 to 2 bit

LSB substitution is performed. Since 1 to 2 bit embedding is done in the smooth region there will be minor difference between the stego-image and the actual image. The resultant will be having high randomness and robustness. Due to these qualities the image will be invisible to the human visual system.

A. Embedding Algorithm

Step 1 Read the cover image.

Step 2 Apply Zero Cross Edge Detection Method to find the Edge Pixels.

Step 3 Convert the edge pixels in 8-bit binary data.

Step 4 Read the image information.

Step 5 Set the Size of payload data according to number of edge pixels.

Step 6 Convert the edge pixels into 8-bit binary data.

Step 7 Convert 8-bit binary data into bit stream.

Step 8 Randomize the bit stream using stego key 1.

Step 9 Randomize the bit stream using stego key 2.

Step 10 Insert bit stream into 1st and 2nd LSB of each edge pixels.

B. Retrieval Algorithm

To extract the secret information from stego image following steps are followed

Step 1 Read the stego image.

Step 2 Retrieve the bit stream from 1st and 2nd LSB of stego image edge pixels.

Step 3 De-randomize the bit stream using secret key 2.

Step 4 De-randomize the bit stream using secret key 1.

Step 5 Convert the bit stream into 8-bit binary pixels.

Step 6 Convert 8-bit binary data into decimal.

Step 7 Recover the image information.

4. Results

In this section we demonstrate simulation results for proposed method. To detect the edge pixels of cover image of eight with size of 256 x 256, shown in Fig. 4.1, Fig. 4.2 shows secret image to hide inside cover image. To getting the edge pixels of cover image Zero Cross Edge Detection Method is used. Zero Cross edge detection method provides highest number of edge pixels at lower threshold. It also shows that Zero Cross method has better embedding capacity than all other methods.

Fig. 4.1 Cover image

Fig. 4.2 Secret image

The stego image after addition of different noises (like Speckle, Salt and pepper, Gaussian and Poisson) are shown in Fig. 4.3 to Fig. 4.6

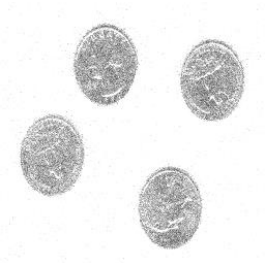

Fig. 4.3 Stego image after adding Gaussian Noise

Fig. 4.4 Stego image after adding Salt and Pepper Noise

Fig. 4.5 Stego image after adding Speckle Noise

Fig. 4.6 Stego image after adding Poisson Noise

It is observed from table 4.1, that the proposed method provides better results as compared to the results of Aruna Mittal[1].The proposed method is providing PSNR of considered image after addition of different noises (like Speckle, Salt and pepper, Gaussian and Poisson). Thus the proposed method are providing better improvement in PSNR over the results of Aruna Mittal[1].

Table 4.1 Comparison of the proposed method with Aruna Mittal [1]

S. No.	With or Without Noise	Aruna Mittal [1]	Proposed Method		% Improvement in PSNR over [1]
		PSNR	PSNR	MSE	
1	Without Noise	51.9769	60.1246	0.0632	15.67
2	Gaussian Noise	48.6234	56.9572	0.1310	17.13
3	Salt and Pepper Noise	56.3243	59.3892	0.0748	5.44
4	Speckle Noise	49.3423	53.2356	0.3087	7.89
5	Poisson Noise	58.6758	60.4955	0.0580	3.10

5.conclusion

In this paper, zero cross edge detection based Steganography is proposed which focus on hiding and extracting the data inside a cover image. Zero cross detection is used for detecting the edge pixels of cover image.

Experimental study points out that the proposed method gives better result as compared to the results of Aruna Mittal [] in terms of higher visual quality, high PSNR values of hiding secret data in the image thus reduces the chance of the confidential message being detected and enables secret communication. It is also found that the hidden message can be extracted perfectly.

Acknowledgment

I would like to express my sincere thanks to Mr. Gaurav Gupta for giving me the opportunity to explore this field of image Steganography. He has always motivated and supported me at all stages of the project work. Also I would like to thank our Department of Electronics & Communication Engineering for providing me all the help as and when required.

References

[1] Aruna Mittal, "A highly secure skin tone based optimal parity assignment steganographic scheme using double density discrete wavelet transform." *international journal of advanced research in computer and communication engineering* 1.9 (2012).

[2] Rashi Singh & Gaurav Chawala," A Review on image Steganography", International Journal of Advanced Research in Computer Science & Software Engineering, Vol.- 04, Issue. 5, ISSN- 2277 128X, May 2014.

[3] Vandana M.Ladwani, Srikanta Murthy K, "A New Approach to Securing Image", International Journal of Advance Research in Computer and Communication Engineering, Vol.- 4, Issue- 1, pp. 2319-5940, January 2015.

[4] Saiful Islam, Mangat R Modi and Phalguni Gupta, "Edge Based Image Steganography", EURSAP Journal on Information Security, pp. 1-14, 2014.

[5] Anant M.Bagade and Sanjay N.Talbar, "A High Quality Steganographic Method Using Morphing" Vol.-10, No. 2, pp. 256-270, June 2014.

[6] Nitin Jain, Sachin Meshram, Shikha Dubey, "Image Steganography Using LSB and Edge – Detection Technique", International Journal of Soft Computing and Engineering, Vol. -02, Issue- 03, pp. 2231-2307, July 2012.

[7] Sneha Arora, Sanyam Anand, "A Proposed Method for Image Steganography Using Edge Detection", International Journal of Emerging Technology and Advanced Engineering, Vol.-03, Issue- 2, pp. 2250-2459, February 2013.

[8] K. Naveen Brahma Teja, Dr. G. L. Madhumati , K. Rama Koteswara Rao, "Data Hiding Using Edge Based Technique", International Journal of Emerging Technology and Advanced Engineering, Vol.-02, Issue- 11,pp. 2250-2459, November 2012.

[9] Jasleen Kour and Deepankar verma,"Steganography Techniques – A Review Paper", International Journal of Emerging Research in Management and Technology, Vol. - 03, Issue. 5, ISSN- 2278 9359, May 2014.

[10] Ratnakirti Roy, Anirban Sarkar, Suvamoy Changder, "Chaos Based Edge Adaptive Image Steganography", International Conference of Computational Intelligence Modelling Techniquies and Applications, Vol.-10, pp. 138-146, 2013.

[11] Da -Chun Wu & Wen-Hsiang Tsai, "A Steganographic Method for Images by Pixel-Value Differencing", Pattern Recognization Letters 24(2003), pp. 1613-1626.

[12] R. Rejani, D. Murugan and Deepu V. Krishnan, "Pixel Pattern Based Steganography on Images", ICTACT Journal on Image and Video Processing, Vol. - 05, Issue: 03, pp. 0976-9102, 2015.

[13] Shamim Ahmed Laskar and Kattamanchi Hemachandran, "High Capacity Data Hiding Using LSB Steganography and Encryption", International Journal of Data Base Management System, Vol. - 4, Issue– 6, December 2012.

[14] R.S. Gutte, Y.D. Chincholkar and P.U. Lahane, "Steganography for Two and Three LSBs Using Extended Substitution Algorithm", ICTACJ journal on communication technology, Vol. -04, Issue- 01, pp. 2229-6948, March 2013 Security and Its Applications (IJNSA), Vol.- 07, No.- 2, March 2015.