International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Data Hiding using Edge-based Image Steganography

Neelam Jaiswal[1], Rekhansh Rao[2]

[1]M. Tech. Scholar, Department of Computer Science and Engineering, RCET, Bhilai, Durg (CG) India

[2]Asistant Professor, Department of Computer Science and Engineering, RCET, Bhilai,Durg (CG) India

Abstract: ***This paper proposed a new method for data hiding within a digital image by using edge based steganography. Steganography is an art and science of hiding secret data by embedding message into an innocence looking cover media in such a way that no one can suspect its existence. In this proposed method we embed the text data in the edges of the digital image, Canny edge detection algorithm is used for detecting the edges of an image. Here amount of data plays an important role on the selection of edges i.e. higher the payload weaker selection of threshold value and for lower payload stronger threshold value will be selected. Then we use 2 LSB plane for embedding the text data on the pixels of the edges. And at the receiver end we extract the text data from stego image by simply applying the reverse process of proposed algorithm. Experiment result shows that we achieve high capacity and higher quality of stego image under HVS (human vision system) due to use of edge detection method.***

Keywords: Steganography, cover image, Canny edge detection, Edges, stego image

1. Introduction

Steganography derives from the Greek Words: Stegano means Covered or secret and Graphic means Writing [2]. Steganography means secret writing and is used for secret communication. Steganography offers us covertly communication and it takes cryptography a step farther by hiding an encrypted message so that no one suspects it existence. The main goal of steganography is to communicate securely in a completely undetectable way and to avoid drawing suspicion to the transmission of a hidden data. Steganography and cryptography are cousins in the spy craft family [1]. Cryptography is the study of hiding information, while Steganography deals with composing hidden messages into a cover media so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Generally the sender writes an innocuous message and then conceals a secret message into the cover media like audio, video or digital image. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists.

The ancient form of Steganography has been reported by the Chinese as the secret message was written in very fine silk or paper, and then rolled it into a ball and covered with wax. The communicator would either swallow the ball or hide it in his parts. A king "Histiaeus" encouraged the Aristagoras of Miletus to revolt against the Persian king. He used to shave the head of his most trusted servants and tattooed the scalps with secret message and waited for the hair to grow. The servants could travel between the borders freely. At the reception end his head would be shaved again and the message will be conveyed [3].

Steganography can be used for wide range of applications such as, in defense organization for safe circulation of database, in military and secret agencies, medical record and prescription of patients should be kept as secret so that it can't abused by illegal people as these are sensitive data of human life. Copyright protection mechanisms that prevent data, usually digital data, from being copied. The term "copyright protection" is occasionally seen in this usage, but is an error; copy protection or Digital Rights Management is the usual term. To protect owner's data, embed the vital information within the digital cover host file.

Steganography techniques uses various types of cover media for embedding process. All digital file format is used to as a cover medium for embedding secret message that may be inside an audio file, video file, with in text, digital image or within a network protocol such as TCP that's called protocol steganography[5][6].

There are two classifications of image steganography methods: spatial domain and frequency domain. The techniques in the spatial domain embed the secret messages directly into the intensity values of the image pixels. The spatial domain based steganography use the LSB algorithm for embedding and extraction process. In the frequency domain, images are first manipulated with algorithms and transforms, and then the message are embedded in the image. The methodsin thespatial domain are considered simplest but also more susceptible to steganalytic attacks, less robust. The frequency domain is also known as the transform domain. Transform domain methods includes discrete Fourier transform(DFT), discrete cosine transform(DCT), and discrete wavelet transform(DWT) [7].

2. Performance Evaluation Parameters

There are so many parameters to be considered while learning steganographic system. They are Robustness, Capacity and Security. They are interdependent to each other and in order to improve one element we have to

sacrifices one or both of the other two element. For example in order to improve security we have to sacrifice capacity and so on.Steganography triangle is best way expressing the relationship between these parameters as shown in Figure 1 it represents the relationship between the three parameters [1][9].

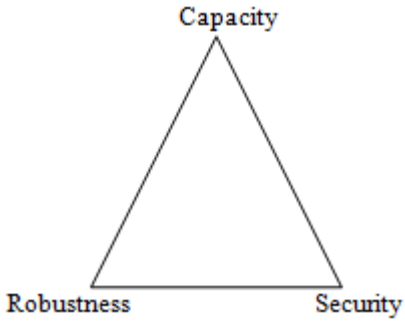

Figure 1: Steganography Triangle

- Robustness: It refers to the potential of the secret message to survive in the process of embedding and extraction of steganographic system. Along with the process of moderation degradation compression, filtering, rotating and cropping of stego image. The robustness of steganographic system checked, if the payload has ability to endure when a cover image gradually decade. However, it is most expected that the embedded content be fragile, so as to lower the chance that an interceptor would be able to reassemble the embedded message.
- Capacity: Capacity of stegonographic system states that, the maximum number of bits which could be inserted or embedded in the cover image, and at the same time the quality of stego image should be high and human visual system unable to detect the difference between stego image and cover image[10]. In steganography the cover image is act like a carrier which carries embedded information. So care should be taken for channel capacity i.e. stego image like other communication channel at the maximum achievable rate and at the same time undetectability should be achieved.
- Security: The fundamental characteristic of steganograpic system is its ability to offers a means of communication without suspicion of the third party other then sender and receiver. Security is the ability of an embedding carrier to remain undiscovered, undetectable. The communication carrier between sender and receiver should be so robust that it does not create any suspicion to the eavesdropper. So undetectability is main motto of steganographic system while taking security as one of the performance parameter. Therefore, proper care should be taken, so that the intruder will unable to distinguish between stego image and cover image.

3. Proposed Technique

3.1 Canny Edge Detection

Fundamentally, edge detection is the process of identifying pixels in a computer image at which image brightness changes abruptly, images are preferred medium for the current steganography techniques [11]. Content adaptability, visual resilience, and smaller size of images make them good carrier to transmit secret message over the internet. Security of any steganography techniques depends on the selection of pixels for embedding. Pixels in noisy and textured area are better choice for embedding because they are difficult to model. Pixels in edges can be seen as noisy pixels because their intensities are either higher or lower than their neighbouring pixels due to sudden change in the coefficient gradient. Due to these sharp changes in the visual and statistical properties, edges are difficult to model in comparison to pixels in smoother area. Therefore, edges make a better option to hide secret data than any other region of an image where a small distortion is much more noticeable.

This paper proposes a new image steganography technique based on Canny edge detection algorithm. The Canny edge detector is an edge detection operator that uses a multi-stage algorithm to detect a wide range of edges in images. It was developed by John F Canny in 1986.In essence Canny edge detection is a technique to extract useful structural information from vision objects and dramatically reduce the amount of data to be processed. Canny edge detection is a multistage algorithm which has the following steps:

1) Noise reduction: Since edge detection is susceptible to noise in the image first step is to remove noise by applying Gaussian filter.
2) Finding intensity Gradient of the image: Smoothened image is then filtered with a edge detection operator like Roberts, Prewitt, or Sobel kernel in both horizontal and vertical direction in horizontal direction (G_x) and vertical direction (G_v). From these we can find edge gradients and direction for each edge pixels as follows

$$G = \sqrt{Gx^2 + Gy^2}$$
$$\Theta = tan^{-1}\frac{Gy}{Gx}$$

3) Non- maximum suppression- After getting gradient magnitude and direction, a full scan of image is done to remove any unwanted pixels which may not constitute the edge.
4) Double thresholding: This stage decides which are all edges are really edges and which are not. For this, we need two threshold values, minVal and maxVal. Any edges with intensity gradient more than maxVal are sure to be edges and those below minVal are sure to be non-edges, so discarded. Those who lie between these two thresholds are classified edges or non-edges based on their connectivity. If they are connected to "sure-edge" pixels, they are considered to be part of edges. Otherwise, they are also discarded.
5) Edge linking: Final edges are found by discarding all edges that are not connected to strong edges.

3.2 Gaussian filter

Since all edge detection results are easily affected by image noise, it is essential to filter out the noise to prevent false detection caused by noise.So Gaussian filter is used in the first step of canny edge detection algorithm to smooth the image and reduce the noise and unwanted details. It is important to understand that the selection of the size of the

Gaussian filter will affect the performance of the detector. The larger the size is, the lower the detector's sensitivity to noise. Additionally, the localization error to detect the edge will slightly increase with the increase of the Gaussian filter kernel size. Here we use 5×5 size of Gaussian kernel, it is a good size for most cases.

3.3 Threshold Selection

The selection of edges for embedding is dependent on length of the text message or payload and the size of the image. As the payload size increases a week threshold for the selection of edges is used so that more edges can be selected to accommodate the increased amount of text data. And if the payload size is less a strong threshold value will be selected.

Canny edge detection algorithm returns the edges of digital image on the basis of three parameters namely high threshold t_h , lower threshold value t_l and width of Gaussian kernel. Threshold t_h is used to identify strong edges and t_l used for weaker edges. The t_h value is dynamically adjusted on the basis of message size in such a way that enough number of edges in the cover image are selected to embed the secret message.

4. Proposed Algorithm

The proposed algorithm is performing two task: the embedding process which hides the secret text message into digital image turning it into a stego image, and the extracting process which extract the secret text message out of the stego image. The embedding process has several steps to be executed and they are as follows:

1) At first we mask our input or cover image I through LSB replacement which does not modify any bit other than LSB and we get clearer and sharper edges of cover image.
2) The algorithm calculate the length of augmented message M, which is a combination of N and C, where N = secret text message and C = message size.
3) The algorithm obtain edge map e by calling Canny edge detection algorithm.
4) Canny edge detection algorithm is used for detecting edges of cover image I, it has three parameter high threshold t_h low threshold t_l and width of Gaussian kernel w. Embedding is done by computing edge map e based on threshold value.
5) Theedge map e is obtained through the Canny edge detector is randomly arranged using stego key P by calling randomPermute(e,P). It ensure that only the intended user can extract data from the stego image.
6) The secret message M is embedded in the randomly permuted S using edge map e by modifying the least two bits of pixel $S_{x,y}$ to the corresponding two consecutive message bits $M_{index+1}$ and M_{index} .
7) The thresholdvalueisembeddedinnon-edgepixelsof the stego image.Non-edge pixel mape' is obtained by taking complement of eforminimum values of t_h andw.The thresholdvalueisembeddedinthefirst32bitsofS correspondingto e.ImageSisreshuffledtogetthestego image.
8) To retrieve the augmented message from the given stego image.The threshold value is extracted from the non-edge pixels of the stego image. Stego key has been used as the seed to permute the set of edge pixels.
9) Extraction is similar to the embedding process. The least two significant bits of the stego image S is masked and edge map e is computed. It is permuted using stego key P to retrieve the message in the same order as it has been embedded.
10) The value corresponding to the least message, and few extra bits. Message size msg_size is extracted from the first C bits of the payload which is used to retrieve the actual message M[C+1:msg_size]. Extra bits beyond msg_size are discarded, and the secret message M is returned.

5. Experimental Result

Algorithm describe in our proposed work have been applied on any size of images. The result were evaluated both qualitatively and quantitatively. Two metrics are MSE (mean square error) and PSNR (peak signal to noise ratio) are calculated for all the standards images, these are used for measures of image quality.

1) MSE - The MSE also called as mean square deviation is cumulative squared error between the compressed and the original image.[4]

$$\text{MSE} = \frac{1}{MN}\sum_{I=0}^{M-1}\sum_{J=0}^{N-1}(x(i,j) - y(i,j))^2$$

Where: i, j refer to the position in the image
M, N refer to number of rows and columns in the input image respectively.

2) PSNR – Peak Signal to noise ratio, often abbreviated as PSNR. It is applied to images as a quality metrics, it is an expression for the ratio between the maximum possible value (power) of signal and the power of distorting noise that affects the quality of its representation. The PSNR is usually expressed as logarithmic decibel scale.

$$\text{PSNR} = 10 \log \frac{R^2}{MSE}$$

Where R is the maximum value in the input image data type.[8]

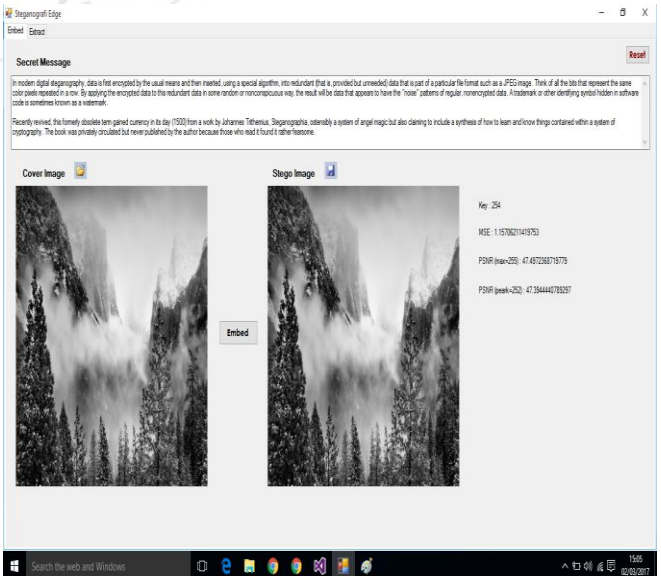

Figure 2: Embedding data into the image 1

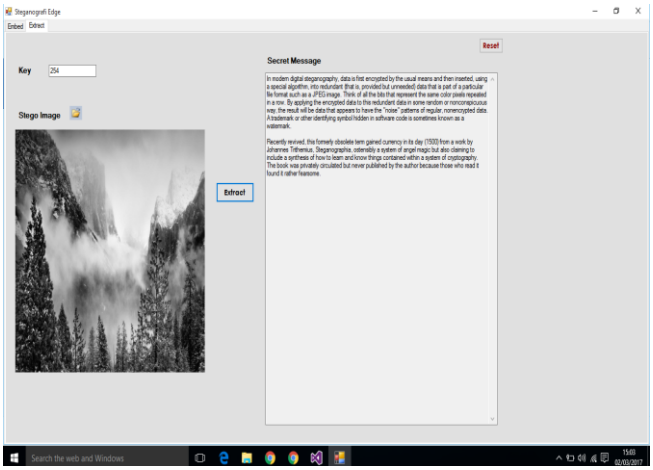

Figure 3: Data Extraction from image 1

In Fig.2we embedding some text data into the gray scale image, image 1 and Fig.3 shows that we get the exact same data after extraction, and from these we can say that we achieved 100 percent accuracy. The MSE and PSNR value of original and stego image of image 1 are 1.15706, 47.49723 respectively.

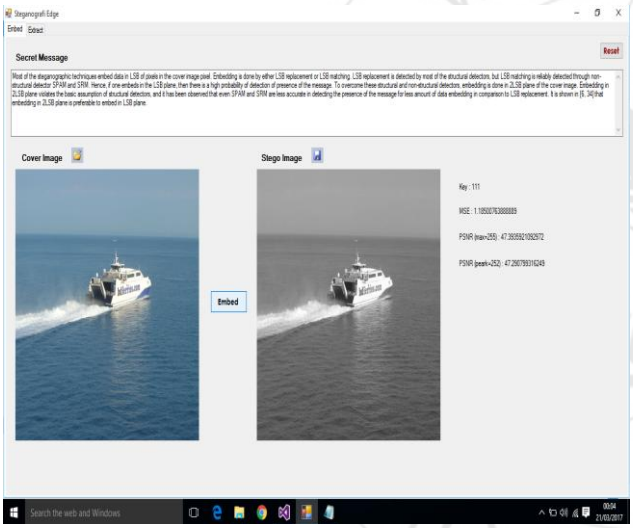

Figure 4: Embedding data into image 2

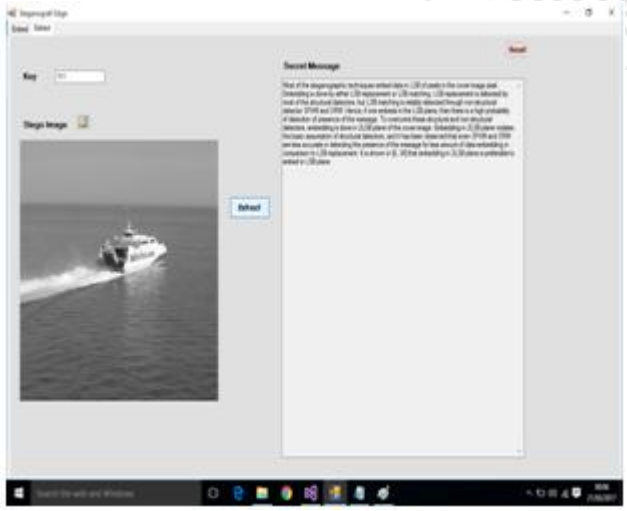

Figure 5: Data Extraction from image 2

In Fig.4 we embedding some text data into the bitmap image, image 2 and Fig.5 shows that we get the exact same data after extraction, and from these we can say that we achieved 100 percent accuracy. The MSE and PSNR value of original and stego image of image 2 are 1.18500, 47.39359 respectively.

Table 1: Proposed algorithm result

Image	MSE	PSNR
Image 1	1.15706	47.49723
Image 2	1.18500	47.39359

Table 1 shows the MSE and PSNR values of images.

6. Conclusion

The proposed method using the edges of image for hiding the text data. Advantage of edge detection technique is to be taken to increase capacity, because embedding data in the edges of digital image can't be detected well by human eye but embedding in smooth areas can be detected easily. From the experimental result we can conclude that proposed algorithm has good results. The performance of proposed algorithm has been illustrated by embedding text messages within the Original images to produce stego images. When these stego-images are decoded, the text messages are completely recoverable. The proposed algorithm produces high capacity and higher quality stego images under HVS(human vision system) due to use of edge detection method. Experimental results show that the proposed work is successful in not only achieving a high embedding payload but also in obtaining a stego image of satisfactory quality.

The future work of this proposed method is dealing with gray scale images and with high dimension to avoid distortion to hide maximum number of character.

As future work, the proposed method is to be optimized for other types of digital files such as jpeg, jpg format of digital image, audio files and video files. Moreover, investigating how other image processing techniques such as brightness and contrast adjustment can be exploited in steganography so as to give the communicating parties more options to control their secret communication.

References

[1] Ge Huayong, Huang Mingsheg, Wang Qian,"SteganographyandSteganalysisBasedonDigitalImage", IEEE Internal Congress On Image and Signal Processing, Vol 4 2011
[2] K. Naveen BrahmaTeja, Dr. G. L. Madhumati, K. Rama Koteswara Rao "Data Hiding Using EDGE Based Steganography" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 11, November 2012)
[3] Sneha Arora, Sanyam Anand "A New Approach for Image Steganography using Edge Detection Method " International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2013
[4] Nasseer M. Basheer, Ashty M. Aaref, Dhafer J. Ayyed "Proposed Method of Text Hiding in Image Edges" International Journal of Computer Applications (0975 – 8887) Volume 126 – No.11, September 2015

[5] Saiful Islam ,Mangat R Modi and Phalguni Gupta "Edge-based image steganography" Springer open Journal
[6] Sachin lawande, Aniket Pawar, Kishor Dhumal "Data Security using Image Steganography and Processing "International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015 ISSN2091- 2730
[7] Mayra Bachrach and Frank Y. Shih "Image steganography and steganalysis " Department of Computer Science, New Jersey Institute of Technology, Newark, NJ, USA DOI: 10.1002/wics.152
[8] Rafael C Gonzalez , Richard E Woods (2002), "Digital Image Processing", Tom Robbins, 2nd Edition
[9] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi "Image Steganography Technique: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6) Issue (3) 2012
[10] Mayra Bachrach and Frank Y. Shih "Image steganography and steganalysis " Department of Computer Science, New Jersey Institute of Technology, Newark, NJ, USA DOI: 10.1002/wics.152
[11] Youssef Bassil "Image Steganography based on a Parameterized Canny Edge Detection Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 60– No.4, December 2012