

A New Approach for Image Steganography using Edge Detection Method

Sneha Arora¹, Sanyam Anand²

Post Graduate Student, Dept. of CSE, Lovely Professional University, Jalandhar, India¹

Assistant Professor, Dept. of CSE Lovely Professional University, Jalandhar, India²

ABSTRACT: This paper proposed a new technique for image steganography using edge detection for RGB images. There are lots of algorithms to hide data with precision level but they are also decreasing the quality of the image. In this proposed study, edges of an RGB image will be detected by scanning method using 3x3 window, and then text will be embedded in to the edges of the color image. By doing this not only high embedding capacity will be achieved, it also enhances the quality of the stego image from the HVS (human vision system).

Keywords: Decoding, Edges, Encoding, Steganography.

I. INTRODUCTION

Steganography is the method for secret communication. The word “Steganography” derives from Greek and it means “cover writing” [1]. Steganography is method of invisible communication between two parties and it is opposite to cryptography. Its goal is to hide the content of a message. Steganography uses a media like an image, video, audio or text file to hide information in it in such a way that it does not attract any attention and looks like an innocent medium. Images are the most popular cover files used for steganography. In image steganography, many different image file formats exist. For different image file formats, different steganographic algorithms are there. There are two types of compression: lossy and lossless [2]. Both methods save storage space, but the procedures are different. Lossy compression creates smaller files by discarding excess image data from the original image. It deletes details that are too small for the human eye to differentiate. As a result, close approximations of the original image are made, but not an exact duplicate. An example of an image format that uses this compression technique is JPEG, whereas lossless method hides messages in more significant areas of the cover image, making it more robust. So the lossless image formats are most suitable for image steganography [3]. Image steganography uses images as the cover file to hide the secret data. Images are the most widely used cover files as they contain a lot of redundancy. Redundancy or redundant information can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display [4]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [5].

II. EVOLUTION OF STEGANOGRAPHY

Steganography has been derived from Greek word “Stego” which means “Covered” and “Graphia” which means “writing”. Steganography is an old technique of invisible communication. 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. Herodotus “the father of history” has mentioned in one of his seminal works of history, about the tradition of secret writing. He has mentioned about the conflicts between Greece and Persia. 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. During the World War II, the Germans invented the use of microdots. Today there are lots of techniques, methods and algorithms for image steganography. We can use any of them according to our requirements. Least significant bit insertion method is most commonly used method to hide the data in images and audio files. In spite of all still there is need of improvement in steganographic systems. Because we have also strong steganalysis algorithms which retrieves the secret messages very easily.

III. PROPOSED WORK

A. Proposed Algorithm For Encoding Data In Image

Step 1: Read the 24 bit RGB image I of size rxc.

Step 2: Detected the edges of the input image by 3x3 scanning method using different orientations and use these edge pixels as the key (K).

Step 3: Read the notepad file (.txt) and store the message in an array list (M).

Step 4: The key (K) is sorted to randomize the pixels and generate a pattern i.e sequence of values those are the position of the pixels where data will be stored.

Step 5: The pattern is stored in the array list (K1).

Step 6: The ASCII value of M[i] is replaced with blue component of K1[i].

Step 7: The output is the image containing secret data [I1].

B. Proposed Algorithm For Decoding Data From Image

Step 1: Read the encoded image [I1].

Step 2: Input shared key (K1), the pattern where data has been stored.

Step 3: Values of blue-byte at K1[i] are read. As each byte contains the ASCII value of the character, the each ASCII value is converted to the character and each character is written to notepad file.

Step 4: The output is the notepad file that contains the secret data decoded from the image.

IV. EXPERIMENTAL RESULTS

All the algorithms described in proposed work section have been applied on standard images of size 512x512 pixels. The results were evaluated both qualitatively and quantitatively. Two metrics are: PSNR (peak signal to noise ratio) and MSE (mean square error) are calculated for all the standard images.

MSE – The MSE is the cumulative squared error between the compressed and the original image.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|I(i, j) - K(i, j)\|^2$$

PSNR – Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$

Figure 1 shows original image of lena of size 512x512 pixels and figure 2 shows the edge detected of the lena image and figure 3 shows the encoded image of lena with text data.



Fig.1 Original image of Lena



Fig.2 Edge detected image of lena



Fig.3 Encoded image of lena

We evaluated both qualitatively and quantitatively results of the proposed algorithm and their evaluated results are shown in Table 1. By analyzing visual and quantitative results, it is seen that proposed algorithm has good results.

Table 1 PSNR and MSE Results of Lena image		
Text Data Encoded in Bytes	PSNR	MSE
100	56.1306	0.1597
200	52.4540	0.3725
400	48.8006	0.8638
849	45.4802	1.8555
1698	42.0073	4.1281
2547	40.2644	6.1665

V. CONCLUSION

This work proposed an algorithm that is combination of edge detection method and data hiding method for encoding. From the above iii and iv sections 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 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.

ACKNOWLEDGMENT

I wish to express my heartfelt gratitude to Assistant Prof. Sanyam Anand for bestowing on me the opportunity to undergo my thesis work under his guidance. I would also like to thank all the faculty members of my Computer Engineering Department of Lovely Professional University. I am deeply indebted to my parents for their inspiration and ever encouraging moral support, which enabled me to pursue my studies. I am also thankful to the authors whose works I have consulted and quoted in this work. Last but not the least I would like to thank God for not letting me down at the time of crisis and showing me the silver lining in the dark clouds.

REFERENCES

1. Morkel T et al, “An overview of image steganography”, Proceedings of the fifth annual information security South Africa conference (ISSA2005).
2. Moerland. T, “Steganography and steganalysis”, Leiden institute of advanced computing science.
3. Madan lal, Jagtar singh, “A novel approach for message security using steganography”, 3rd International conference of advance computing & communication technologies, November 08-09, 2008, APIIT, Panipat, India.
4. Abolfazl diyanat, Farshid Farhat, Shahrokh ghaemmaghami, “Image steganalysis based on SVD and noise estimation: improve sensitivity to spatial lsb embedding families”, IEEE, 978-1-4577-0255-vol-6, 2011.
5. Piyush marwaha, Paresh marwaha, “Visual cryptographic steganography in images”, IEEE, 978-1-4244-6589-vol-7, 2010.

BIOGRAPHY



Sneha Arora is a post graduate student. She is doing M.Tech in CSE from Lovely Professional University Jalandhar. She has worked as a Lecturer in the department of Computer Science for two years in **S.R.P.A.A.B college under G.N.D.U(Asr.)** from July 2007 to April 2009, in **S.D college for women under G.N.D.U(Asr.)** from Nov 2009 to Feb 2010, in **Apeejay College Of Fine Arts under G.N.D.U(Asr.)** from July 2010 to May 2011, in **Apeejay College Of Fine Arts under G.N.D.U(Asr.)**. from July 2011 to August 2011.