

Adaptive Method of Data Hiding using Edge Detection

Harpreet Kaur

M.E. Student

ECED, Thapar University, Patiala
Punjab, India

Ajay Kakkar

Assistant Professor

ECED, Thapar University, Patiala
Punjab, India

ABSTRACT

Data security is of utmost importance for an institution, organization and many government sectors to keep the confidential information protected from different competitors. It will help to make sure that the security of user's data is maintained. In today's time most of the information is first received, processed and finally is get saved within the computers and further transmitted across different networks, therefore, it is required to preserve the data in order to maintain confidentiality. Keeping in mind the importance of steganography for transmission of secret data a data hiding algorithm using edge detection and clustering mechanism is proposed. Data is embedded using LSB scheme. Also, comparison using two edge detection algorithms has been done. Simulation results of the proposed algorithm show good value of PSNR as well as an acceptable quality of the stego image which makes it difficult to detect any presence of embedded data in the cover image and hence make it secure for transmission.

Keywords

Steganography; Fuzzy Edge detection; Clustering; Data Embedding

1. INTRODUCTION

The progress of computer technology and the increasing awareness of public network among the users make it easier for users to get access and exchange different kinds of multimedia files. So, these types of files like audio, video, image etc. may become more susceptible to attack by any user on the internet. Therefore, it has become important to protect this kind of sensitive data. One of the techniques used for hiding the information over the public network is Steganography. The word steganography is acquired from the Greek words "stegos", signifying "cover", and "grafia", signifying "composing", which collectively mean a "secured composition" [1-3]. Steganography is a practice of concealing communication; a steganographic framework in this way hides secret information with the help of a cover media, so that, a hacker or an unauthorized user may not feel the presence of the secret data. Steganography is a process of concealing different types of content such as text, image, audio or any video in some other multimedia file like audio, image or video [4-5]. Steganography can be distinguished by cryptography in the viewpoint that in case of steganography's the key point is that the secret data is covered up and no person can think that there is any hidden information, while in cryptography anyone can realize that there is a hidden message. It incorporates an immense range of secret communications strategies that hide the message's extremely presence [6-8]. Image steganography, is a method in which secret information is inserted inside any picture, as a cover medium which is generally examined among the most recent decades [9]. Content flexibility, visual versatility, small dimension of pictures and furthermore the shortcomings of the human visual system (HVS) make it a great conveyer to transfer confidential information through the web [10-11]. For

the process of image steganography here emphasis on spatial domain technique is given, as secret information is hidden in pixel value straightforwardly though transformation domain techniques accomplish inserting by first changing over the image from spatial to frequency space [12]. There are two primary ways to attain embedding in spatial space that are classified as Least-Significant-Bits (LSB) substitution, and Pixel-Value-Differencing (PVD). LSB substitution is the most normally utilized strategy specifically substituting the LSBs of pixels in the cover picture with secret bits to get the stego picture. PVD technique gives great imperceptibility by figuring the difference of two sequential pixels to decide the depth of the hidden bits [13-14]. Safety of every steganography strategy relies on upon the choice of pixels for hiding. Noisy pixels as well as pixels found in finished regions are preferred decisions for inserting on the grounds that they are hard to design [15-16].

2. RELATED WORK

A novel two-description image coding algorithm using steganography and least-significant bit (LSB) steganographic method was presented [1-2]. Xin Liao *et al.* worked to enhance the hiding limit while yielding an undetectable optical standard, and proposed a new steganographic technique which depends on four-pixel differencing and modified least significant bit substitution [3]. Chung-Li Hou *et al.* worked on a significant problem in steganography which is to reduce distortion between the cover and stego image. Due to ease of the tree based parity check technique, it is used to embed a secret data in the cover picture [4]. Sunita Bhati *et al.* presented novel encryption algorithm "Byte-Rotation Encryption Algorithm (BREA)" which also includes "Parallel Encryption Model" this improved both privacy and speed of the encryption technique [5]. A discussion on the various types of image encryption and decryption schemes and investigation on already existing various steganography schemes for data hiding is done [6-8]. Hamidreza Rashidy Kanan *et al.* proposed an adjustable visual picture superiority as well as information lossless practice in spatial domain which depends on a genetic algorithm (GA). Simulation outputs, in comparison to other recently well-known steganography methods, show that the introduced technique which can attain high hiding capacity in addition to this also improves the PSNR of the stego image [9]. A new approach for generating keys from the available data was introduced [10-11]. Frequency domain steganography based data embedding scheme deploying Fresnel transform (FT) was proposed [12]. Similarly another procedure for steganography Pattern Discovery (SPD) to have high recognition precision was proposed by Hedieh [13]. Steganography technique by utilization of interval valued intuitionistic fuzzy edge identifying strategy and in addition the modified LSB substitution strategy which makes it possible to standardize the picture quality and also to enhance the capacity was proposed [14]. Text steganography by employing LZW compression technique and color coding based approach was proposed. This algorithm first compresses secret data and then

concealed the compressed confidential information into the electronic mail addresses and also in the cover message of the email [15-16].

3. PROPOSED SCHEME

In this section the proposed method which is the Adaptive method of embedding is discussed. The brief description of the above algorithm is given below:

3.1 Adaptive method of embedding

The proposed technique is based on variably embedding the pixels of the cover image i.e. the undisclosed message that has to be hidden would be embedded variably in each pixel of the cover image. The main emphasis is to get better image quality of stego image and also to enhance capability of data that can be hidden. This has been done by differentiating edge pixels and smooth pixels. Edge pixels may be viewed as noisy pixels in light of the fact that their intensities may be higher or may be lower than their adjoining pixels because of abrupt transform in the coefficient angle. Because of these abrupt transforms in the visual and geometric properties, edges are hard to display in contrast with pixels of smoother zone. Hence a potential edge recognizing strategy is required. The flow diagram of this adaptive embedding process is shown in figure 1. Firstly, a gray scale image is taken as a cover image. Now the second step is to detect the edges of this cover image. This is done by technique considering full or fractional participation and connection among one value to other of the pixels of the image. For this, a fuzzy inference system (FIS) toolbox in MATLAB R2013a is used using which input membership functions and the output membership functions have to be defined. Accordingly various rules or conditions based on if, else or and rules are applied, on the basis of these rules the edge detection is done. This would separate the edge pixels from smooth pixels. Before embedding the data (that is the last step) the clustering of the pixels of the image has been performed.

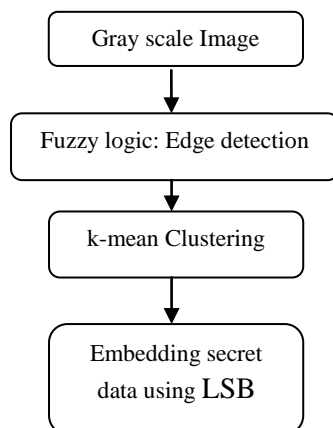


Fig. 1: Flow chart for adaptive method of embedding

The clustering is performed using k-means clustering that is a technique of vector quantization, originated from signal processing, and which is well-known for cluster investigation in information mining. The objective of k-means clustering is to divide η observations into k clusters. Each observation belongs to the cluster with the nearby mean, helping as a sample of the cluster. Following the k-mean clustering, the embedding process has to be performed. The data hiding process have been performed by dividing the edge pixels in four numbers of clusters. The strong edge will contain

maximum information and the smooth pixel will contain less amount of information.

4. SIMULATION RESULTS

In this section, the results obtained using fuzzy logic edge detection method, clustering using k-mean and the embedding process have been discussed.

4.1 Using Fuzzy logic: Edge detection

First of all the gray color image of the cover image is considered which is shown in figure 2.



Fig. 2: Cover image (Grayscale representation)

The edges of this image are to be found by using the fuzzy edge detection method which is based on Fuzzy inference system (MATLAB FIS toolbox). The fuzzy logic edge-detection process relies on the image gradient to locate breaks in uniform regions. The image gradient both along the x -axis as well as y -axis has been considered. The results of I_x and I_y are shown in figure 3 and 4. These figure shows the edges of the image, both in horizontal as well as vertical direction.



Fig. 3: Edges along X-axis



Fig. 4: Edges along Y-axis

A zero-mean Gaussian membership function for each input is specified and the degree of membership function is stated according to gradient value of pixel. Output membership functions are also defined. Thus, the final edge detection of the image is obtained which is shown in figure 5.



Fig. 5: Edge detection using fuzzy logic

After edge detection clustering of the pixels using k-mean clustering technique has been performed. The clustered image is shown in figure 6. Next the data has been embedded in the original grayscale image. This is done in accordance with the values of pixels obtained after clustering process. The edge pixels are embedded with high number of bits and the smooth pixels are embedded with lower number of bits. This is done to achieve a high embedding capacity as well as to maintain an acceptable image quality of the stego image with a high value of PSNR and least value of MSE. The stego image so obtained is shown in figure 7.



Fig. 6: Clustering using k-mean



Fig. 7: Stego image

Hence, using fuzzy edge detection and k-mean clustering a new algorithm for embedding the secret data in to cover image is achieved. The PSNR, MSE and the payload values are shown in table 1.

Table 1: Value of Parameters using fuzzy logic




Image	PSNR	MSE	Payload
Lena (256×256)	44.77	2.18	150099

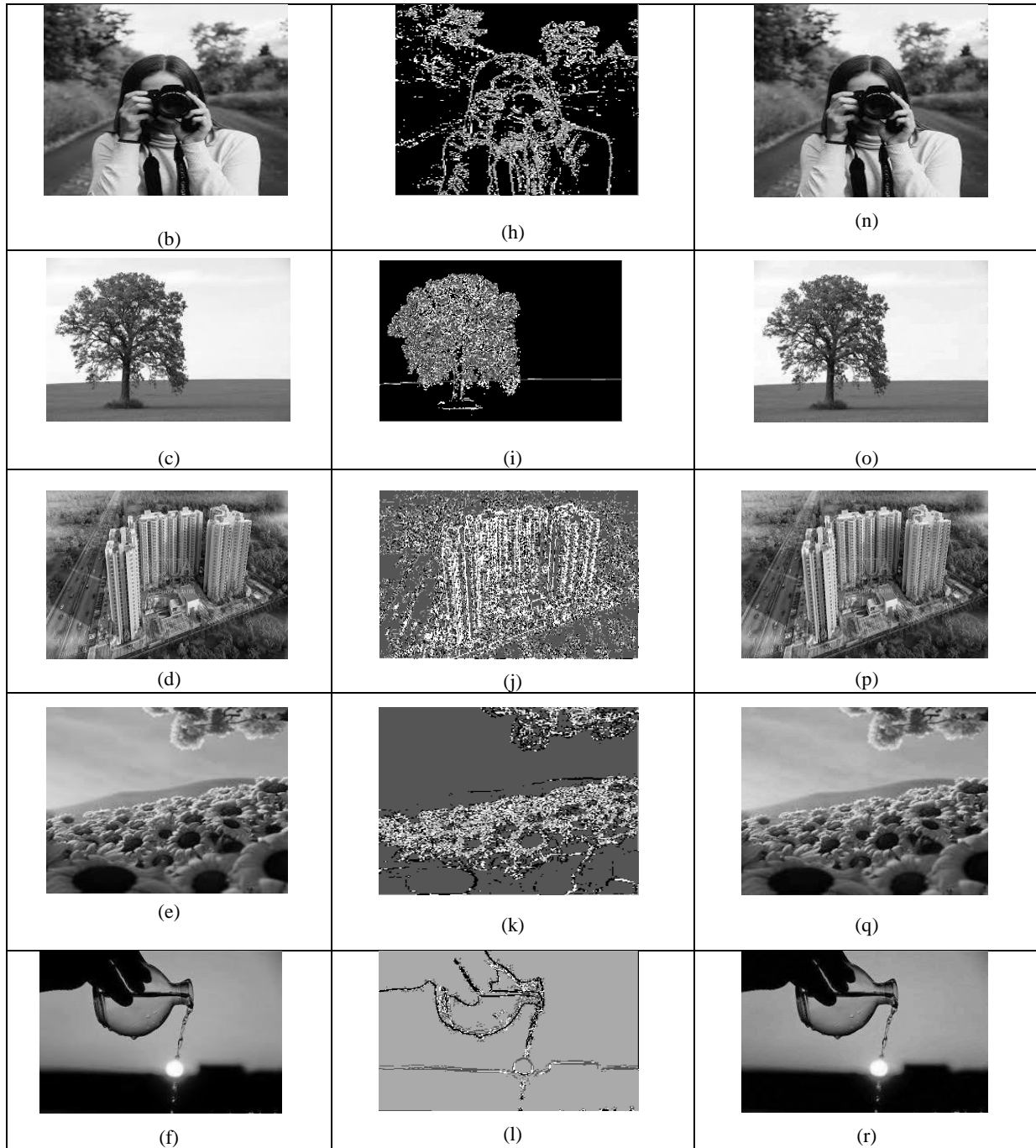
Thus, it has been observed that for image ‘Lena’ shown in figure 2, high value of PSNR i.e. 44.77 dB is achieved along with a large embedding capacity which is 150099 bits. Now to analyze the proposed method a new edge method based on sobel edge technique is also used. The results using fuzzy logic have been compared with sobel technique in the next section.

4.2 Comparison between sobel and fuzzy logic based edge detection

In last section, fuzzy logic method for edge detection has been used. This method is tested on various images of different pixel sizes and their results are analyzed in this section. Also, the results have been compared with same algorithm but using a different edge detection technique which is the sobel edge detection. The results are shown in table 2. Six different images which are house, camera girl, tree, skyscraper, sunflowers and sun are considered. The original grayscale image are shown in column one of the table 2 (a)-(f), the images obtained after performing edge detection and k-mean clustering are shown from (g)-(l) in table 2 and finally the stego images are shown in third column of the table 2 from (m)-(r).

Table 2: (a)-(f) Original Images, (g)-(l) Clustered Images and (m)-(r) Stego Images

 (a)	 (g)	 (m)
--	--	--



The comparison of the results obtained using fuzzy edge detection (FED) and sobel edge detection (SED) is shown in table 3.

Table 3: Comparison of MSE, PSNR and Payload values using FED and SED

Image	Pixel Size	MSE		PSNR (dB)		Payload (bits)	
		FED	SED	FED	SED	FED	SED
House	285×177	4.5	5.10	40.949	39.9	115815	120527
Skyscraper	300×168	5.72	6.04	39.451	39.21	127871	130604
Sun	275×183	1.68	2.10	44.77	43.79	104755	108095
Tree	275×183	4.39	4.83	40.59	40.17	117658	121388
Cameragirl	212×238	2.67	4.24	42.75	40.75	110476	119941
Sunflowers	204×204	3.41	4.47	40.867	39.69	94105	99946

It has been observed from table 3 that the MSE value using fuzzy edge detection is comparatively less and as a result a high PSNR value is obtained as compare to sobel edge detection method. This provides a better image quality of the stego image, as it becomes more difficult for an unauthorized person to detect the presence of any secret data in the image. So, for a better quality image, the FED method is more preferred for data hiding as compare to SED. But it should be noticed that the embedding capacity is more in case of SED method. More number of bits can be embedded using the SED. Although the MSE is less and PSNR values are high in case of FED, but the stego images obtained in case of SED are also imperceptible for human eyes to view any major distortion in them, in addition, capacity is also high in case of SED.

5. CONCLUSION

In this paper, improved LSB substitution algorithm is used for embedding any secret data into grayscale images. This is done in two steps: (i) By detecting edges of the cover image using fuzzy logic and sobel method, and (ii) By clustering them according to edge and non edge pixels with the help of k-mean clustering technique. The results show that the stego image is obtained without making a perceptible distortion. Moreover, the given algorithm is used to analyze different cover images which give very similar results. At last, comparison among the fuzzy and sobel edge detection results is done. PSNR and MSE values are also calculated. To get improved value of PSNR the presented work may be further modified using some new intermediate step in the existing algorithm. Also, the given data embedding algorithm can be done using audio or video files.

6. ACKNOWLEDGEMENT

I would like to show gratitude my mentor, the whole faculty and staff of Electronics and Communication Engineering Department of my college and then friends who devoted their valuable time and help me in all feasible ways towards successful completion of this work. I show appreciation to all those who has contributed directly or indirectly to this work. Last but not least, I would like to thanks my parents for their years of unyielding love and encouragement, they have always wanted the best for me and I admire their fortitude and sacrifice.

7. REFERENCES

- [1] Z. Zhang, C. Zhu, and Y. Zhao 2008. Two-Description Image Coding With Steganography. *IEEE Signal Processing Letters*, 15, 887-890.
- [2] S. Sarreshtedari and M.A.Akhaee 2014. One-third probability embedding: a new ± 1 histogram compensating image least significant bit steganography scheme. *IET Image Process*, 8(2), 78-89.
- [3] X. Liao, Q.Y. Wen, J. Zhang 2011. A steganographic method for digital images with four-pixel differencing and modified LSB substitution, *Journal of visual communication and image representation*, 22 (1), 1-8.
- [4] C.L.Hou, C.C. Lu, S.C. Tsai and W.G. Tzeng 2011. An Optimal Data Hiding Scheme with tree-based parity check. *IEEE Transactions on Image Processing*, 20(3).
- [5] S. Bhati, A. Bhati and S. K. Sharma 2012. A New Approach towards Encryption Schemes:Byte-Rotation Encryption Algorithm. *Proceedings of the World Congress on Engineering and Computer Science 2012*, 2.
- [6] M.S. Subhedar and V.H. Mankar 2014. Current status and key issues in image steganography: A survey. *Computer Science Review*, 13, 95-113.
- [7] R. Pakshwar, V.K. Trivedi and V. Richhariya 2013. Survey On Different Image Encryption and Decryption Techniques. *International Journal of Computer Science and Information Technologies*, 4 (1), 113-116.
- [8] M. Jain and S.M. Lenka 2016. A Review of Digital Image Steganography using LSB and LSB Array, *International Journal of Applied Engineering Research*, 11(3), 1820-1824.
- [9] H.R. Kanan and B. Nazeri 2014. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, *Expert Systems with Applications*, 41, 6123-6130.
- [10] A. Kakkar, M.L. Singh and P.K. Bansal 2012. Mathematical Analysis and Simulation of Multiple Keys and S-Boxes in a Multi-node network for Secure Transmission, *International Journal of Computer Mathematics*, 89(16), 2123-2142.
- [11] V. Agrawal, S. Agrawal and R. Deshmukh 2014. Analysis and Review of Encryption and Decryption for Secure Communication, *International Journal of Scientific Engineering and Research*, 2(2), 1-3.
- [12] S.U. Maheswari and D.J. Hemanth 2015. Frequency domain QR code based image steganography using Fresnelet transform, *International Journal of Electronics and Communication*, 69, 539-544.
- [13] H. Sajedi 2016. Steganalysis based on steganography pattern discovery, *Journal of Information Security and Applications*, 30, 3-14.
- [14] H. Dadgostar, F. Afsari 2016. Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB. *Journal of Information Security and Applications*, 1-11.
- [15] A. Malik, G. Sikka and H.K. Verma 2017. A high capacity text steganography scheme based on LZW compression and color coding, *Engineering Science and Technology, an International Journal*, 20, 72-7.
- [16] Maninder singh and Dhanwant singh (2015). Energy efficient key management scheme for wireless sensor networks. *International Journal of Research in Information Technology*, 3 (8), 166-173.