A Secure True Edge based 4 Least Significant Bits Steganography

Sahib Khan[#], Nasir Ahmad[#], Muhmmad Ismail[#], Nasru Minallah[#], Tawab Khan[*]
[#]Department of Computer Systems Engineering, University of Engineering and Technology Peshawar, Peshawar, Pakistan
[*]Department of Mathematics, Abdul Wali Khan University Mardan, Mardan, Pakistan
engrsahib_khn@yahoo.com, n.ahmad@uetpeshawar.edu.pk

***Abstract*—In this paper true edge based data hiding technique is proposed to take advantage of less sensitivity of human visual system to changes in complex regions of the image. This method utilizes edge detection and Steganography techniques. The Canny edge detection technique is used to identify true edge pixels and 4LSB Steganography technique is used to hide a secret message in the 4 least significant bits of edge pixels in the cover image. By hiding data in edges improve the quality of stego-image significantly. The results obtained show that the proposed technique hides large amount secret information in the cover image with better visual image quality than other techniques. The experimental results demonstrate the average hiding capacity of 4%, and the *PSNR* and *MSE* are 45*dB* and 1.60 respectively.**

Keywords—Steganography; Edge detection; 4LSB Steganography; Steganalysis.

I. Introduction

Data hiding, also called Steganography, is a technique of concealing secret information within other information, thereby hiding the message secretly. In the era of modern communication and development of very fast processing systems, Steganography methods have become very important in several applications. For example, copyright, data integrity and authentication are few well-known applications of Steganography. Many digital images, audio and video now comprise a distinctive yet invisible watermark that help in preventing unauthorized copying of these materials [1, 2]. The digital media, e.g. image, audio and video can be used as a cover, but the media with higher redundancy is considered to be the most suitable cover for data hiding. As digital images have high redundancy that's why the images are mostly adopted for data hiding and lots of research has been carried out in the field of image Steganography.

Several data hiding methods have been reported both in the spatial domain and transform domain. Honsinger et al.'s and Fridrich et al.'s proposed Steganography methods in spatial domain by hiding secret information directly in image pixels [3, 4]. VLSB Steganography was introduced by Sahib et al. and they also proposed some algorithms (i.e. MDT and DDDBA), for implementation of VLSB Steganography [5, 6]. In transform domain DCT coefficients are subjected to data hiding instead of pixels. Macq et al. implemented his method by data hiding using transform domain [7]. De Vleeschouwer et al. and Goljan et al. also developed invertible data hiding techniques, but the data hiding efficiency was very low for the acceptable image quality and the quality of a stego-image dropped severely when the capacity was increased [8, 9]. Sahib et al. proposed a variable data hiding method in DCT domain [10]. Xuan et al.'s method, achieved a quite large hiding efficiency by hiding data in cover media using wavelet transform [11]; however, the image quality was affected significantly.

The main aim of Steganography is to hide more data in the cover image in such manner that the change made in the cover is unperceivable to human visual systems (HVS). As a HVS is more sensitive to variations in the smooth area of cover image than the complex area. Due to this characteristic of the HVS different amount of message data is hidden in smooth and complex regions of cover image. The complex region is subjected to more data hiding than smooth areas of the cover image. As a result the quality of the stego-image increases and the security of hidden information also increases. A lot of techniques, including LSB methods, PVD methods, and side-match methods have been proposed to hide data in complex areas of images [12-18]. However, some of these techniques provided a small hiding efficiency [12, 18], and doesn't comply completely with the rule that the edges can tolerate more changes than smooth region [16, 17]. To increase data hiding capacity Jung et al. [19] presented a new technique that hides data in smooth areas along with edges resulting in more distortion.

In the proposed technique of data hiding, canny edge detection is applied on a cover image to detect true edge pixels and the four least significant bits of each edge pixel are substituted with secret data using 4LSB Steganography.

II. Proposed Method

The previous methods hide data in the complex region of cover image, but they also hide data in those pixels that doesn't belong to edges. These methods hide data in a noisy or very weak and disconnected edge pixels which are not considered as the edges by most of the nowadays edge detection technique, e.g. Canny etc. In this paper a spatial domain data hiding method is proposed to hide secret information in true edges by substitution of 4 least significant bits of the cover image. The hiding of a secret message in true edges only, decreases the hiding capacity a bit, but the hiding of data in the true edge

978-1-5090-0436-2/15/$31.00 ©2015 IEEE

pixels avoids the changes in histogram near zero and histogram fluctuations and results in high quality stego-image. This makes the detection of information difficult for LSB and histogram difference based steganalyzers. In the proposed technique of data hiding, canny edge detection is applied on a cover image to detect true edge pixels and the four least significant bits of each edge pixel are substituted with secret data using 4LSB Steganography.

In this section a reversible 4LSB data hiding technique using the canny edge detection technique is presented. The main aim is to separate the edge and the non-edge pixels and then hiding secret data in the edge pixels only, to enhance the quality of stego-image. The proposed method involve of the following major steps:

a) Preprocessing: To remove noise from the cover image by using a Gaussian low pass filter.

b) Calculating gradients: The magnitudes and directions of the gradient are calculated at every single point in the image. The region where the gradient has large magnitude is marked as edges while a low gradient implies non edges. The direction of gradient determines the orientation of the edges.

c) Non maximum suppression: This step is important to convert "blurred" edges to sharp edges and keeping all local maxima and deleting everything else.

d) Double Thresholding: To determine the potential edges, double thresholding is applied to the result of non-maxima suppression.

e) Edge tracking by hysteresis: This is the final step to find the final edges that suppress all the edges that are not connected to a strong edge.

f) Data Hiding: Finally edge pixels are used for data hiding by replacing the 4 least significant.

The cover image "$C(i,j)$" is subjected to Canny edge detection and an array of edges "E(i, j)" is obtained. The detected edges of the cover image are now utilized for data hiding. The pixels from cover image $C(i,j)$ are considered one by one and the pixel corresponding to edge area are subjected to data hiding and all the pixels of smooth region are left unaffected. The 4 least significant bits of each edge pixel are substituted with 4 bits of secret message.

$$\mathrm{E(i,j)} = \mathrm{Canny(C(i,j))} \qquad (1)$$

$$\mathrm{Steg(i,j)} = \mathrm{C(i,j)} * \mathrm{m},\ \forall \text{ i and j}, \mathrm{E(i,j)} = 1 \qquad (2)$$

$$\mathrm{Steg(i,j)} = \mathrm{C(i,j)},\ \forall \text{ i and j}, \mathrm{E(i,j)} = 0 \qquad (3)$$

Where

$m$is the secret message

$Steg(i,j)$is a stego-image pixel

The complete process is given here in the block diagram as shown in Fig 1.

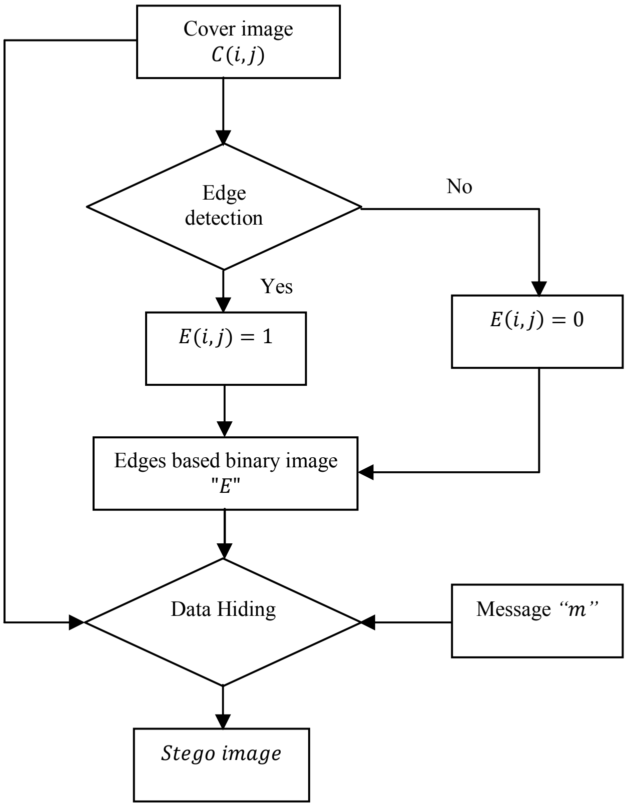


Fig. 1. Block diagram of 4LSB Edge based data hiding

III. Experimental Results

The proposed technique is implemented to hide the same secret message in different cover images, e.g. Tree, Pepper, Lena, Mandrill and Tiffany. The main factor to be considered is the human visual system sensitivity to the changes and hiding capacity. The data hiding capacity determines the amount hidden information and the *MSE* and *PSNR* are used to determine the quality of stego-image and the imperceptibility of hidden data [20]. The *MSE* and *PSNR* are obtained by Equation (13) and (14), respectively.

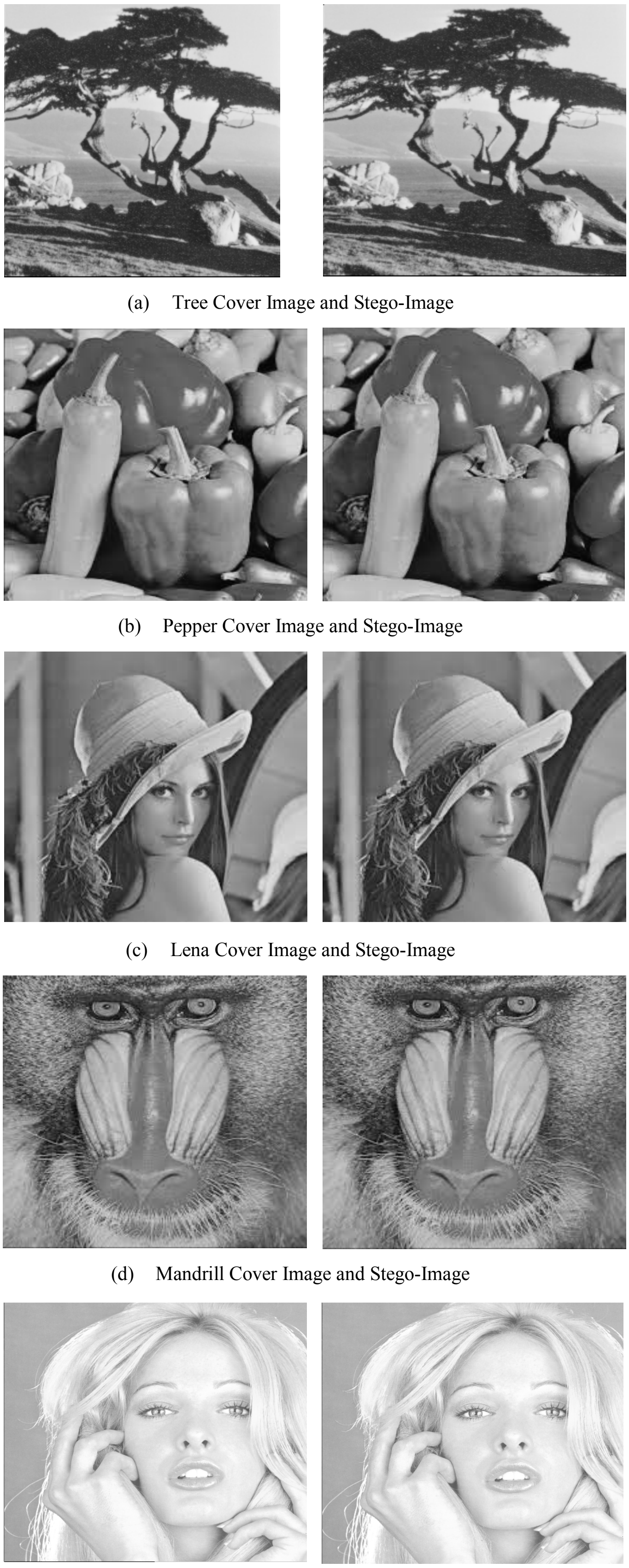
$$\mathrm{MSE} = \frac{\sum_{i=1}^{r}\sum_{j=1}^{c}(\mathrm{Cover(i,j)} - \mathrm{Stego(i,j)})^2}{r*c} \qquad (4)$$

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}} \qquad (5)$$

The data hiding capacity, *PSNR* and *MSE* measured for each cover and corresponding steo-image and listed here below in Table 1.The cover images and corresponding stego-image are shown in Fig 2.

TABLE I. Hiding Capacity, PSNR and MSE

Cover Image	PSNR (dB)	MSE	Hiding Capacity (%)
Tree	45.6453	1.7724	4.3167
Pepper	45.5821	1.7983	3.9812
Lena	46.2279	1.5499	4.1442
Mandrill	42.6069	3.5677	8.3625
Tiffany	46.0790	1.6039	3.8929



(a) Tree Cover Image and Stego-Image

(b) Pepper Cover Image and Stego-Image

(c) Lena Cover Image and Stego-Image

(d) Mandrill Cover Image and Stego-Image

(e) Tiffany Cover Image and Stego-Image

Fig. 2. Cover Images and Steo-Images (a) Tree, (b) Pepper (c) Lena (d) Mandrill (e) Tiffany

IV. Comparison with Previous Method

In this section the proposed method of data hiding is compared with some other data hiding techniques. Table 3 shows the data hiding capacity and PSNR of the proposed method compared with other data hiding technique. The data hiding capacity is presented in bits per pixel (bpp) while PSNR is presented in dB. The results given in Table 3 show that the proposed method, presented in this paper, has a reasonable high PSNR than other methods except Ni et al. The data hiding capacity of the proposed method is much higher than Ni et al. Similarly, the hiding capacity is also higher than the other methods mentioned in Table 3 except Goljan et al. but the PSNR is higher than Goljan et al. method. Also, the presented technique does not need any additional information for data recovery.

TABLE II. Comparison of proposed method with other methods

Method	**Lena**		**Mandrill**	
	Capacity (bpp)	**PSNR (dB)**	**Capacity (bpp)**	**PSNR (dB)**
Honsinger et al.	<0.0156	-	<0.0156	-
Macq and Deweyand	<0.03125	-	<0.03125	-
Fridrich et al.	0.0156	-	0.0156	-
Goljan et al.	0.36	39.00	0.0443	39.00
Vleeschouwer et al.	0.0156	30.00	0.0156	29.00
Ni et al	0.083	48.20	0.0827	48.20
4LSB-EDH	0.33	46.23	0.669	46.08

V. Conclusion

This paper presents a data hiding method that hides a secret message in true edges of a cover image. As HVS is not sensitive to the changes in complex region of the cover image and more sensitive to the smooth areas, the proposed method makes use of this limitation and hide data in edge pixels only without affecting the rest of the pixels. The canny edge detection technique has been used in for finding actual edges and suppressing the noise and weak edges by smoothing and double thresholding and hysteresis edge tracking process. 4 bits of the message are hidden are in the least significant bits of edge pixels. The stego-images generated by this process have a good quality and high *PSNR* and low *MSE*. An average *PSNR* of 46 *dB* and an average data hiding capacity of 4% has been obtained. The hiding capacity and *PSNR* of the proposed work is higher than or comparable to other methods. In short, the true edge based data hiding technique is a strong and secure data hiding method, resulting in a high quality stego-image, significantly high PSNR and reasonable data hiding capacity.

References

[1] N. F. Johnson, and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer 31.2 (1998): 26-34.

[2] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," Proceedings of the IEEE 86.6 (1998): 1064-1087.

[3] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," Photonics West 2001-Electronic Imaging. International Society for Optics and Photonics, 2001.

[4] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," U.S. Patent No. 6,278,791. 21 Aug. 2001.

[5] S. Khan, and M. H. Yousaf, "Implementation of VLSB Stegnography Using Modular Distance Technique," Innovations and Advances in Computer, Information, Systems Sciences, and Engineering. Springer New York, 2013. 511-525.

[6] M. A. Irfan, N. Ahmad, and S. Khan, "Analysis of Varying Least Significant Bits DCT and Spatial Domain Stegnography," Sindh Univ. Res. Jour. (Sci. Ser.) Vol.46 (3): 301-306 (2014)

[7] B. Macq, and F. Dewey, "Trusted headers for medical images," DFG VIII-D II Watermarking Workshop. Vol. 10. Germany: Erlangen, 1999.

[8] C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," Multimedia Signal Processing, 2001 IEEE Fourth Workshop on. IEEE, 2001.

[9] M. Goljan, J. J. Fridrich, and R. Du, "Distortion-free data embedding for images," Information Hiding. Springer Berlin Heidelberg, 2001.

[10] S. Khan, M. N. Khan, S. Iqbal, S. Y. Shah, and N. Ahmad, "Implementation of Variable Tone Variable Bits Gray-Scale Image Stegnography Using Discrete Cosine Transform," Journal of Signal and Information Processing 4.04 (2013): 343.

[11] G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, and W. Su, "Distortionless data hiding based on integer wavelet transform," Electronics Letters 38.25 (2002): 1646-1648.

[12] N. Guan, D. Tao, Z.Luo, and B. Yuan, "Online nonnegative matrix factorization with robust stochastic approximation," Neural Networks and Learning Systems, IEEE Transactions on 23.7 (2012): 1087-1099.

[13] N. Guan, D. Tao, Z.Luo, and B. Yuan, "NeNMF: an optimal gradient method for nonnegative matrix factorization," Signal Processing, IEEE Transactions on 60.6 (2012): 2882-2898.

[14] W. Hong, and T. S. Chen, "A novel data embedding method using adaptive pixel pair matching," Information Forensics and Security, IEEE Transactions on 7.1 (2012): 176-184.

[15] W. Hong, T. S. Chen, and C. W. Shiu, "Reversible data hiding for high quality images using modification of prediction errors," Journal of Systems and Software 82.11 (2009): 1833-1842.

[16] S. Khan, N. Ahmad, and M. Wahid, "Varying index varying bits substitution algorithm for the implementation of VLSB steganography," Journal of the Chinese Institute of Engineers (2015), 1-9.

[17] C. S. Hsu, and S. F. Tu, "Probability-based tampering detection scheme for digital images," Optics Communications 283.9 (2010): 1737-1743.

[18] J. C. Joo, H. Y. Lee, and H. K. Lee, "Improved steganographic method preserving pixel-value differencing histogram with modulus function," EURASIP Journal on Advances in Signal Processing 2010(2010): 26.

[19] Jung, Ki-Hyun, and Kee-Young Yoo. "Data hiding using edge detector for scalable images." *Multimedia tools and applications* 71.3 (2014): 1455-1468.

[20] Z. Wang, and A. C. Bovik, "A universal image quality index," Signal Processing Letters, IEEE 9.3 (2002): 81-84.