J. Engg. and Appl. Sci. Vol.36 No,1 January-June 2017 ISSN 1023-862X, eISSN 2518-4571

4LSB BASED DATA HIDING IN COMPLEX REGION OF DIGITAL IMAGES AND ITS EFFECTS ON EDGES AND HISTOGRAM

Sahib Khan[1], Muhammad Naeem[2], Tawab Khan[3], Nasir Ahmad[4]

ABSTRACT

Data hiding in the complex regions of cover image make the use of edges for hiding and communicating secret information. The complex region in a digital image is the least sensitive to human visual system (HVS) in term of changes than smooth region. The data hiding in the complex regions affect the edges and the histogram of the image. These two may cause the existence of hidden information to be detected. In this paper, the effect on image edges and histogram is investigated when subjected to true edge based 4 least significant bits (4LSB) steganography. The true edge based 4LSB steganography technique has been found very efficient, creating no significant effect on edges and undetectable histogram differences. Which prove this technique immune to histogram difference steganalysis. The quality of the edges is preserved and a PNSR of greater than 74dB has been observed for different cover images for the true edge based 4LSB steganography. The quality of stego images, edges can been observed qualitatively and it be seen clearly that no significant changes are introduced due to hiding information in edges using the true edge based steganography.

Keywords: Steganography, Edge, Canny edge detection, Histogram difference, Steganalysis

INTRODUCTION

Steganography, also called data hiding, is an old technique of securing highly valuable and secret information. Secret message and cover media (e.g. image, audio, and video) are two important elements of any steganography technique [1]. In image steganography, secret message is hidden in cover image and to get stego image. The stego image is of significant high visual quality that it does not attract the attention of HVS. Steganography has found tremendous application in the modern digital era e.g. copyright, data integrity and authentication [2].

Here it is worth mentioning that any digital media can be used as a cover in steganography, but the media with higher redundancy is preferred. That is the main reason that digital image steganography attracted most of the researchers [3, 4]. Various steganography techniques has been proposed and implemented the details is available in [4-11]. All these techniques used either the LSBs of cover image pixels in spatial domain or the LSBs of coefficient of transformation in frequency domain. Along with LSBs exploitation for data hiding in [2], Khan et al, made use of HVS limitations. And this paper is an extension of Khan et al, work.As HVS is more sensitive to variation made in the even area of the digital images than the complex area. Because of this characteristic of HVS a lot of techniques like LSB methods, PVD methods, and side-match methods have been used to hide data in complex areas of the cover images [12-17]. However, some of these techniques provided a small hiding efficiency [12]. Jung et al. [18, 19] presented a new technique with large data hiding capacity that hides data in both smooth and complex areas of the cover images.

The methods that hide data in complex areas also hide data in non-edge pixels. These methods hide data in noisy or weak and disconnected edge pixels that are not considered as the edges by most of the edge detection technique, e.g. Canny etc. In this paper, mainly focus on data hiding in true edges and its effect on edges and histogram. It has been observed that the hiding of a secret message in true edges only, decreases the hiding capacity a bit, but avoids the changes in histogram near zero and histogram fluctuations and results in high quality stego-image [20]. This makes the detection of information difficult for LSB and histogram difference based steganalyzers.

4LSB DATA HIDING IN EDGES

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, the non-edge pixels, and then hiding secret data in the edge pixels only, to enhance the quality of stego-image.

Let a cover image $Cov(i,j)$ is the cover image and $Gf(i,j;\sigma)$is the Gaussian smoothing filter with standard deviation of "σ". A smoothed image $Sm(i,j)$ is obtained by applying the Gaussian filter on the cover image.

$$Sm(i,j) = Gf(i,j;\sigma) * Cov(i,j) \quad (1)$$

Then gradient $Gdx(i,j)$ and $Gdy(i,j)$, in the direction of the x-axis and y-axis respectively, are determined by using the masks shown in Equations (2) and (3)

[1] *Department of Electronics and Telecommunication, Politecnico Di Torino, Turin, Italy*
[2] *Department of Computer Science, University of Peshawar, Pakistan*
[3] *Department of Mathematic, Abdul Wali Khan University Mardan, Pakistan*
[4] *Department of Electronic and Electrical Engineering, Loughborough University, UK*

$$Mgx = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \quad (2)$$

$$Mgy = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \quad (3)$$

Edge strength "$Mg(i,j)$", i.e. gradient magnitude and the direction of the edges is by using the Equation (4) and (5) respectively.

$$Mg(i,j) = \sqrt{(Gdx(i,j))^2 + (Gdy(i,j))^2} \quad (4)$$

$$\theta = tan^{-1}\left(\frac{|Gdy(i,j)|}{|Gdx(i,j)|}\right) \quad (5)$$

The image is scanned in the image gradient direction, and the strength of the edge is compared with the strength of its neighbors. The 8-connected neighbors are used in the comparison process. The edge strength of the current pixel is preserved if its edge strength is the largest otherwise it is suppressed by removing it. The array of edges after the non-maxima suppression $N(i,j)$ is given by Equation (6).

$$N(i,j) = nms(Mg(i,j)) \quad (6)$$

After this two threshold levels, i.e. high threshold "Th", and low threshold "Tl"are defined. The edges in $N(i,j)$are classified as strong, weak and suppressed edges by using the double thresholoding process as given by Equation (7).

$$\left\{ \forall\, i \text{ and } j \left| \begin{matrix} N(i,j) < Tl, & N(i,j) \text{ is a suppressed edge} \\ Tl < N(i,j) < T, & N(i,j) \text{ is a weak edge "W"} \\ N(i,j) \geq T, & N(i,j) \text{ is a strong edge "S"} \end{matrix} \right. \right\}$$
(7)

To decide about the nature of weak edges the hysteresis edge tracking is applied. The strong edges are considered the final edges $Edge(i,j)$and the weak edges are considered as the final edges $Edge(i,j)$ if and only if they are connected with the strong edges otherwise they are discarded. The final edges "$Edge(i,j)$", is an array of 1s and zeros. The edge pixels are marked as 1 and non-edge pixels are marked as 0.

$$Edge(i,j) = \begin{cases} 1, & if\ N(i,j) \in S \ \ or\ N(i,j) \in W \cap N(i,j) ⋓ S \\ 0, & Otherwise \end{cases} \quad (8)$$

Where "⋓" show the neighborhood.

Now the detected edges of the cover images are used for data hiding. The pixels from cover image $Cov(i,j)$ are considered one by one and the pixel corresponding to the edge area are subjected to data hiding and all the pixels of the smooth region are left unaffected. The 4 LSBs of each edge pixel are substituted with 4 bits of secret message.

$$\forall\, i \text{ and } j, Edge(i,j) = 1 \quad (9)$$

$$Steg(i,j) = Cov(i,j) * m \quad (10)$$

$$\forall\, i \text{ and } j, Edge(i,j) = 0 \quad (11)$$

$$Steg(i,j) = Cov(i,j) \quad (12)$$

Where
m is the secret message
$Steg(i,j)$is a stego-image pixel

The complete process is given here in the flow chart diagram in **Figure 1**.

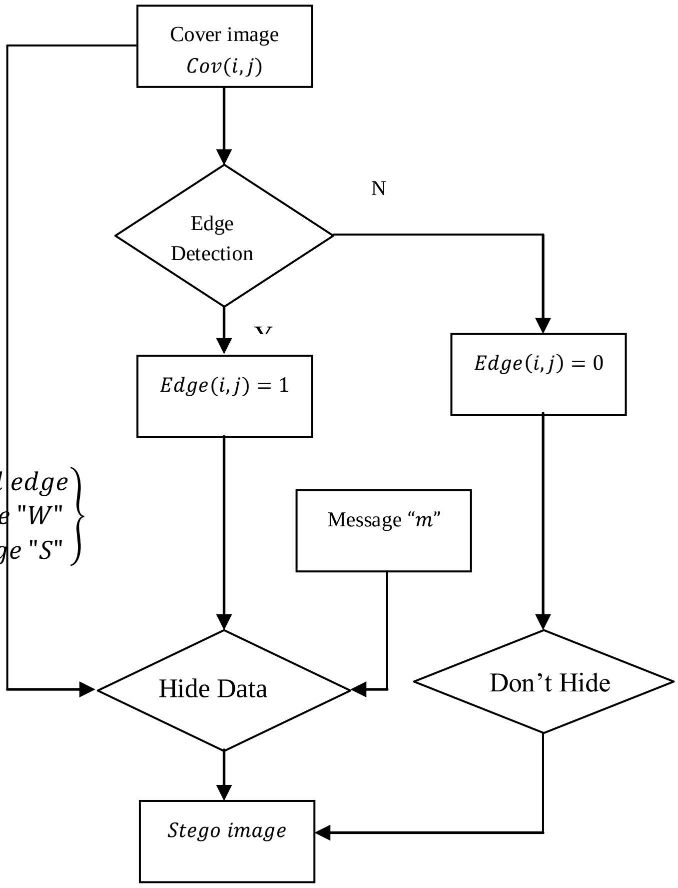
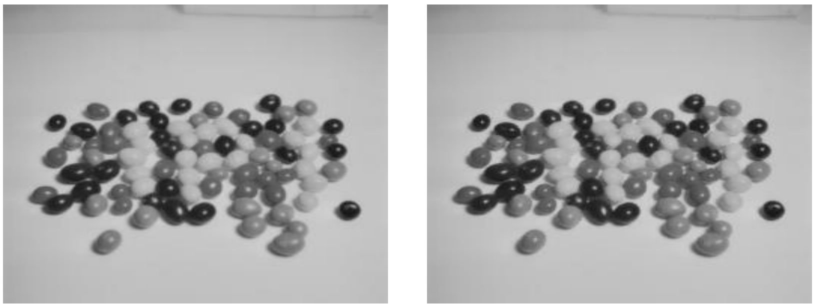


Figure 1. Flow Chart diagram of 4LSB Edge based data hiding

Experimental Results

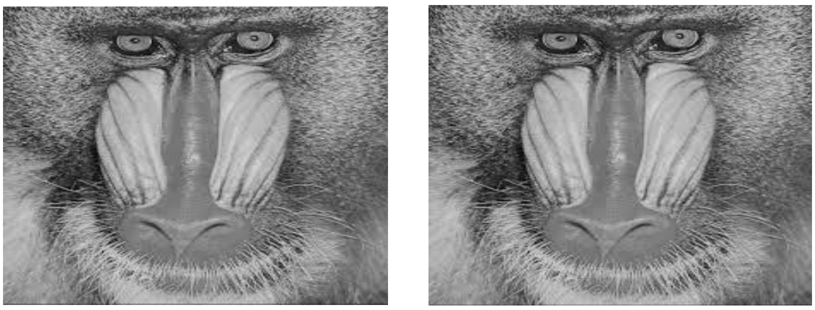
Steganography is a data hiding mechanism that hides secret information in an imperceptible manner. If the changes in the cover image are not perceivable to HVS, it is difficult for a steganalyzers to predict about hidden data. To examine the result of data hiding in true edges, on edges and histogram, a secret message is hidden in the 4 LSBs of edges pixels. The USC-SIPI Image Database has been used for experimentation and analysis [21]. All the images in the database are in Tiff format. Before edge detection and hiding information, all the images are converted to grayscale. Some of these cover images used for experimentation are shown in **Figure 2**. The results show that the data hiding in true edges does not affect the quality of cover image after data hiding.

(a) Woman, Cover and Stego Image



(b) Jelly beans, Cover and Stego Image

(c) Lena, Cover and Stego Image



(d) Mandrill, Cover and Stego Image

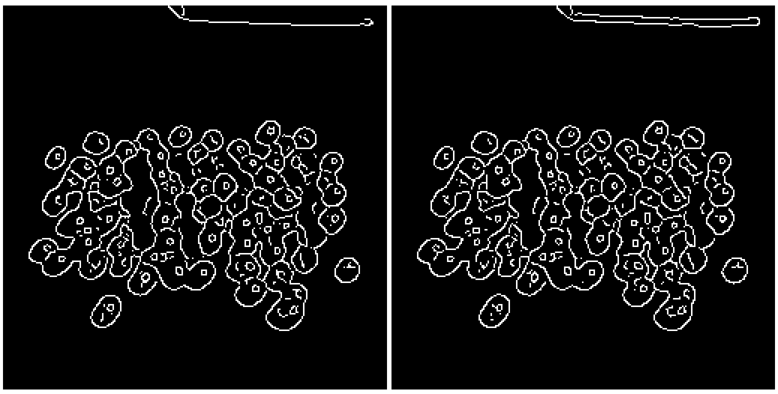
(e) House, Cover and Stego Image

Figure 2. Cover and Stego Images (a) Jelly beans, (b) Pepper, (c) Lena, (d) Mandrill, (e) House

However, the quality of stego-image is not the only factor that is used by steganalyzers. For data hiding in edges the effect on the edges is also an important factor. The edges of the cover images used in experimentation process and the respective stego-images should also closely match with each other and the changes should be small enough and imperceptible to HVS. To observe the effect of data hiding on the edges, the canny edge detection technique is also applied to the stego-image and corresponding cover image. Edge images are shown here in **Figure 3**.

The experimental results show that the edges of the original and modified stego images are identical to the HVS and there are no visually significant changes occurring on the edges after data hiding. The images showing edges of original unaffected images and respective stego images are shown in **Figure 3**. To check the quality of the edges before and after data hiding, the peak signal to noise ratio (*PSNR*) and mean square error (*MSE)* are calculated. The experimental results show an average *PSNR* and *MSE* of 72*dB* and 0.0036 respectively. The *PSNR* and *MSE* for each cover image edges are listed in the **Table 1**. The edges and the statistical results show that the data hiding in the edges of the proposed method doesn't affect the edges significantly, both visually and statistically. Hence the analysis of the edges doesn't help the steganalyzers detect and predict the presence of secret information in stego-image.

(a) Woman, Cover Image Edges and Stego-Image Edges



(b) Jelly beans, Images of Cover and Stego Edges

(c) Lena, Images of Cover and Stego Edges

(d) Mandrill, Images of Cover and Stego Edges

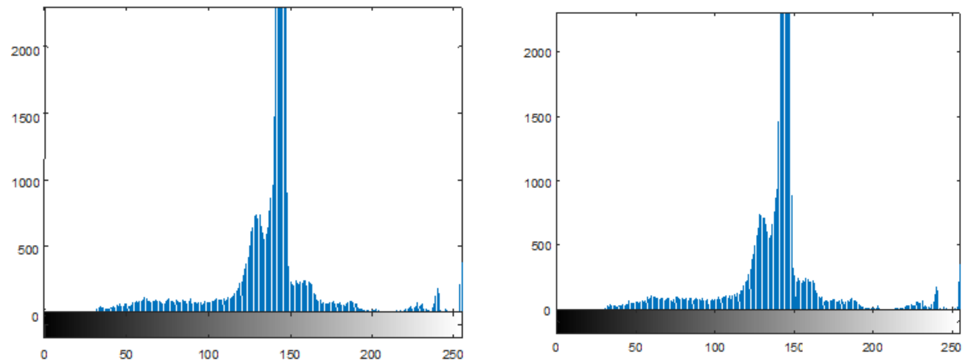
(e) House, Images of Cover and Stego Edges

Figure 3. Cover and Stego image Edges (a) Woman, (b) Jelly beans, (c) Lena, (d) Mandrill, (e) House

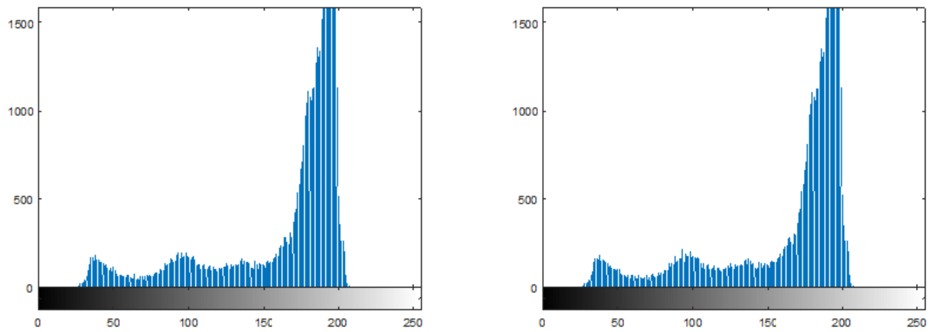
Table 1. Effect on the edges

Cover Image	***PSNR (dB)***	***MSE***
Woman	***64.1711***	***0.0249***
Jelly beans	***72.8160***	***0.0034***
Lena	***72.6217***	***0.0036***
Mandrill	***70.1502***	***0.0063***
House	***69.8057***	***0.0068***

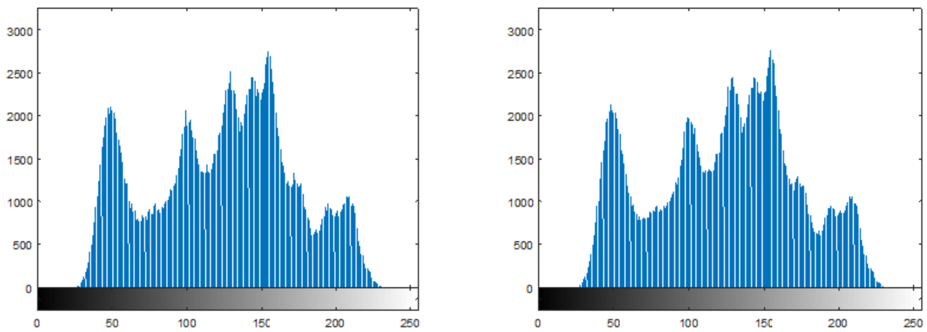
Besides, the edge analysis, there is a very important factor, i.e. histogram difference that may be helpful for steganalyzers to break a Steganography technique. The previous PVD-based methods produce abnormal differences in histograms. The changes in the histogram near zero and the irregular fluctuations in the difference histogram are probable to be detected. The proposed method 4LSB-EDH avoids the change in histogram near zero and hence difficult for the prediction of hidden data for histogram steganalyzers. The histogram of original cover images and the corresponding stego-images are shown here in **Figure 4**.



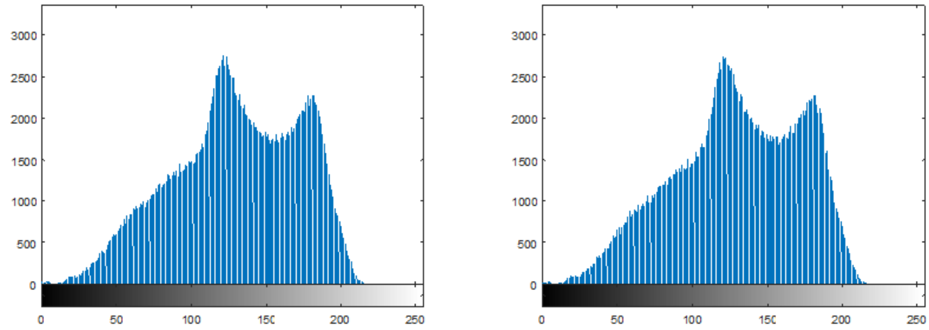
(a) Histogram of Woman, Cover and Stego image



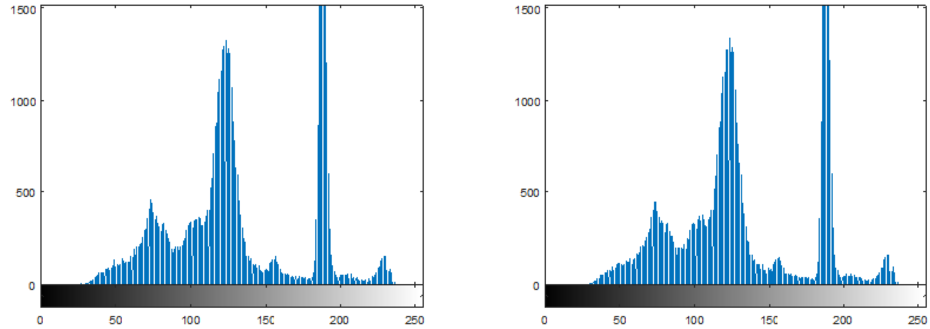
(b) Histogram of Jelly beans, Cover and Stego image



(c) Histogram of Lena, Cover and Stego image



(d) Histogram of Mandrill, Cover and Stego image



(e) Histogram of House, Cover and Stego image

Figure 4. Histograms of cover image and stego-image (a) Tree, (b) Jelly beans, (c) Lena, (d) Mandrill, (e) House

CONCLUSION

The HVS is not much sensitive to modifications in the complex regions of the cover image. Data hiding in true make use of this limitation by hiding data in complex area of the cover image and leave the smooth area unaffected. The data hiding in true edges results in high quality stego images and create no visually significant distortion in the cover images. Along with this, the data hiding in true edges technique preserves the quality of edges and histogram. This techniques is very robust to changes in histogram near zero and histogram fluctuations. This makes the proposed method immune to the histogram-based steganalyzers. In short, the true edge based data hiding technique is a strong and secure data hiding method.

REFERENCES

1. Johnson, N. F., and Jajodia, S., (1998), "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26-34.

2. Khan, S., Ahmad, N., Ismail, M., Minallah, N., and Khan, T., (2015), "A secure true edge based 4 least significant bits steganography," *International Conference on Emerging Technologies* (*ICET*), Peshawar, Pakistan, pp.1-4.

3. Ma, B., and Shi, Y. Q., (2016), "A reversible data hiding scheme based on code division multiplexing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp.1914-1927.

4. Honsinger, C. W., Jones, P. W., Rabbani, M., and Stoffel, J. C. (2001), "Lossless recovery of an original image containing embedded data," Washington, DC: U.S. Patent and Trademark Office, 6 (278&791), issued August 21, 2001.

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

6. Irfan, M. A., Ahmad, N., and Khan, S., (2014), "Analysis of Varying Least Significant Bits DCT and Spatial Domain Stegnography," *Sindh Univ. Res. Jour.* (*Sci. Ser.*), vol. 46, no. 3, pp. 301-306.

7. Macq, B., and Dewey, F., (1999), "Trusted headers for medical images," *DFG VIII-D II Watermarking Workshop*, Germany: Erlangen, vol. 10.

8. Vleeschouwer, C. D., Delaigle, J. F., and Macq, B., (2001), "Circular interpretation of histogram for

reversible watermarking," *IEEE 4th Workshop on Multimedia Signal Processing*, pp. 345-350.

9. Goljan, M., Fridrich, J., and Du, R., (2001), "Distortion-free data embedding for images," *Information Hiding*, Springer Berlin Heidelberg, pp. 27-41.

10. Khan, S., Khan, M. N., Iqbal, S., Shah, S. Y., and Ahmad, N., (2013), "Implementation of Variable Tone Variable Bits Gray-Scale Image Stegnography Using Discrete Cosine Transform," *Journal of Signal and Information Processing*, vol. 4, no. 4, pp. 343-350.

11. Xuan, G., Zhu, J., Chen, J., Shi, Y. Q., Ni, Z., and Su, W., (2002) "Distortionless data hiding based on integer wavelet transform," *Electronics Letters*, vol. 38, no. 25, pp. 1646-1648.

12. Liu, C., Hoi, S. C., Zhao, P., Sun, J., and Lim, E. P., (2016) "Online Adaptive Passive-Aggressive Methods for Non-Negative Matrix Factorization and Its Applications" *25th ACM International on Conference on Information and Knowledge Management*, pp. 1161-1170.

13. Guan, N., Tao, D., Luo, Z., and Yuan, B., (2012), "NeNMF: an optimal gradient method for nonnegative matrix factorization," *IEEE Transactions on Signal Processing*, vol. 60, no. 6, pp. 2882-2898.

14. Hong, W., and Chen, T. S., (2012), "A novel data embedding method using adaptive pixel pair matching," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 176-184.

15. Hong, W., Chen, T. S., and Shiu, C. W., (2009), "Reversible data hiding for high quality images using modification of prediction errors," *Journal of Systems and Software*, vol. 82, no. 11, pp. 1833-1842.

16. Hong, W., Chen, T. S., and Shiu, C. W., (208), "A minimal Euclidean distance searching technique for Sudoku steganography," *IEEE International Symposium on Information Science and Engineering* (*ISISE'08*), vol. 1, pp. 515-518.

17. Khan, S., Ismail, M., Khan, T., and Ahmad, N. (2016), "Enhanced stego block chaining (ESBC) for low bandwidth channel", *Security and Communication Networks*, vol. 9, no. 18, pp. 6239-6247.

18. Jung, K. Y., and Yoo, K. Y., (2014), "Data hiding using edge detector for scalable images," *Multimedia tools and applications*, vol. 71, no. 3, pp. 1455-1468.

19. Wang, Z., Bovik, A. C., Sheikh, H. R., and Simoncelli, E. P., (2004), "Image quality assessment: from error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, no. 4, pp.600-612.

20. Khan, S., Ahmad, N., and Wahid, M., (2016) "Varying index varying bits substitution algorithm for the implementation of VLSB steganography", *Journal of the Chinese Institute of Engineers*, vol. 39, no. 1, pp. 101-109.

21. SIPI, USC, (2016) "The USC-SIPI Image Database" http://sipi.usc.edu/services/database/data-base.html.