Image Steganography Based on a Key & Modified LSB for Improved Security

Sreekutty S Kumar*
*PG Scholar,
Department of ECE,
College of Engineering, Karunagappally

Sylish S V**
**Assistant Professor,
Department of ECE,
College of Engineering, Karunagappally

Abstract— **In this modern era, the internet has become the most widely used communication channel. The contents of transmission must be of any forms i.e. message texts, voices, images etc. To secure these contents various techniques are used. Steganography is one such technique where the data is hidden from an intruder. This paper makes use of the concept that more information can be hidden in the edge regions when compared to that of smooth regions. The cover image used for embedding the payload or information bits is first altered using a key, which adds to the security of the system. An improved cover image, a novel edge preserving mechanism along with a final control improves the efficiency of the system. The experimental results show the performance of the proposed scheme.**

Keywords—Steganography;edge preserving mechanism; canny edge detection ; modified LSB substitution.

I. INTRODUCTION

With the expansion of network and bandwidth, digital media can be transmitted conveniently over the internet. Data security,copy right protection etc. are some problems that need to be faced while communicating in such public systems.Encryption of these datas can be used to provide safety but the transformation of data into a cipher text alters the message and therefore it gets distorted.In such distorted messages,an intruder finds it easy to suspect the presence of highly confidential data. To overcome these problems,we make use of Steganography.The word steganography is derived from the Greek words “stegos” and “grafia” which means “cover”and “writing” respectively.Thus it can be defined as “covered writing”.In contrast to Cryptography,where an outsider is allowed to detect,intercept and change the messages,the main aim of Steganography is to hide messages in a medium in such a way that no one can even detect the presence of a hidden message.Image steganography can be broadly classified into spatial domain,frequency domain(transformation domain),spread spectrum and model based steganography.In spatial domain techniques,the data bits are embedded directly into the pixel values of the images. For transformation domain, the images are first transformed using any one of the transforms such as Discrete Cosine Transform(DCT),Discrete Wavelet Transform(DWT), Hadamard Transform, Dual Tree DWT,Double Density Dual Tree DWT and then the messages are embedded into these transform coefficients.

In case of spread spectrum steganography the data is embedded in noise, which is inherent from the image acquistion phase.Model based steganography is purely based on the statistical model of the cover image.Also,there are mainly two categories to achieve embedding of data bits,they are Least Significant Bits (LSB) substitution method and Pixel Value Differencing(PVD) [1] .There are two types of LSB insertion methods,namely fixed-size and variable size. For the variable-size embedding scheme,the number of LSBs used varies in accordance with the contrast and luminance characteristics.The fundamental concepts include cover image, payload, stegoimage, imperceptibility, robustness, capacity and security. Cover image refers to the carrier image used in steganography for hiding a text data whereas the payload refers to embedded data.The cover image along with the payload forms the stego image.Capacity refers to the amount of data that can be hidden in a cover image.It is represented in bits per pixel(bpp).Robustness denotes the amount of alteration that a stego image can withstand before an intruder or adversary can destroy the hidden data.Security means the eavesdropper’s inability to detect the hidden data. The proposed scheme falls under the spatial domain technique where the secret message is embedded in the Least Significant Bits of variable size.Steganography finds various useful applications in different fields of life for e.g.,copyright control of different materials,increasing the robusntess of various search engines, and smart IDs where each individuals’ details are embedded in their photographs.Other applications are video-audio synchronisation,companies’ safe circulation of secret data,TV broadcasting etc.

II. RELATED WORKS

The most popular image formats include the Graphics Interchange Format(GIF), Joint Photographic Experts Group(JPEG) and to a lesser extend the Portable Network Graphics(PNG). Most of the techniques used in the existing works make use of these image formats with some exceptions that use the Bitmap format(BMP) for its simple data structure. LSB substitution method usually does not lead to increase in the file size, but depending on the size of the information that is to be hidden, the file can become noticeably distorted. Many steganographic tools based on LSB substitution data hiding are available e.g. StegHide, S tool, Stegnos etc. [2]. In literature, a variety of LSB based steganography approaches are discussed. Some of them include Adaptive LSB substitution based on brightness, edges and texture masking of the host image to estimate the number *k* of LSBs for data hiding [3], loss less generalized LSB data embedding [4], optimized LSB substitution using cat swarm strategy and genetic algorithm [5,6], data hiding based on histogram modification [7,8] etc. Soleimanpour et al. [9] proposed a Scientific Technique for Steganography Method Based on Advanced Genetic Algorithm Optimization in the Spatial Domain field and a new LSB method came into the picture. Here different LSB match structures are evaluated. And then score matrix is generated. Total cover image is broken into different frequency divisions. A transform domain help us to hide the message in the most effective pixels. Advantage of this method is higher PSNR value of stego image is achieved here and it improves the visual quality of stego image. This method gives better output from other similar type of methods like Mielikainen and some different methods. The drawback of this method is it takes a long time to calculate score matrix. If this drawback can be somehow eliminated then it is an effective method. In most cases the bit length of the original data that is replaced with the embedded data remains the same. However, different pixels in an image tolerate different amounts of changes without noticeable distortion [10]. Therefore, whenever there is equal change in LSBs of all pixels then it results in a poor quality stego image. In order to tackle this problem, some LSB based methods employed Human Visual system(HVS) masking characteristics to embed the secret data into the variable sizes of LSBs of each pixel values. Liao et al. [13] proposed an adaptive LSB steganographic method using PVD and LSB replacement. In their scheme, the difference value of four consecutive pixels is used to estimate the hiding capacity into the four pixels. Pixels located in the edge areas are embedded by a k-bit LSB substitution method with a greater value of k than that of the pixels located in smooth areas. The scheme embeds more secret data into edge areas than smooth areas in the cover image. Dadgostar & Afsari [1]in their work on image steganography, proposed an interval-valued intuitionistic fuzzy edge detection algorithm & modified LSB substitution method. The proposed system make use of those algorithms in an improved cover image which increases the security.

III. PROPOSED WORK

The embedding system here makes use of an adaptive LSB substitution method. It takes advantage of the Human Visual System (HVS) and is based on the fact that edge regions in an image can tolerate more number of bits than that in smooth regions. First a cover image is chosen for embedding the payload. The cover image is first altered in a specific pattern using a key. A key can be a numerical, string or any data which is further converted to a binary data. The key is duplicated to half the number of rows and columns of the cover image. Thus, there is the presence of a binary number corresponding to those halves i.e., each rows and columns of the cover image. The presence of a binary 1 besides the rows and columns result in an interchange of symmetric rows and symmetric columns respectively. Let the original image be represented as shown in Fig. 1(a). Assume that the key is '11', then all the rows and columns are interchanged as mentioned above which is shown in Fig.1 (b). Thus, the pixel values of the cover image are altered to obtain an improved cover image.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

Fig.1(a)

25	24	23	22	21
20	19	18	17	16
15	14	13	12	11
10	9	8	7	6
5	4	3	2	1

Fig. 1(b)

Fig. 1

1(a)The original cover image 1(b)Improved/Altered cover image

Pixels are embedded using the ***l***-bit LSB substitution method. This implies that the ***l*** LSBs of each pixel in the cover image is used to embed the message bits (secret data). The number of bits that must be embedded (***l***) depends on whether the pixel value is an edge or not. $\boldsymbol{l_e}$ number of bits are embedded in the edge region whereas $\boldsymbol{l_s}$ number of bits are embedded in the non-edge region. Always the value of $\boldsymbol{l_e}$ is greater than $\boldsymbol{l_s}$.

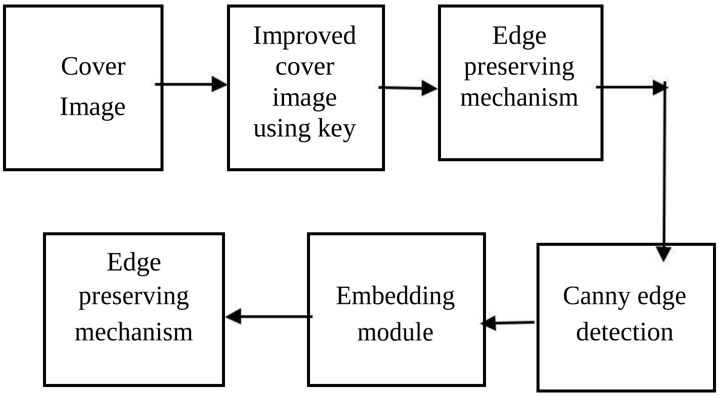

Cover Image
Improved cover image using key
Edge preserving mechanism
Canny edge detection
Embedding module
Edge preserving mechanism

Fig.2 Schematic representation of the proposed method

A canny edge detection algorithm is used to distinguish between an edge and a non-edge. Embedding a message in the LSBs of a pixel of cover image is given by

$$x' = x * m \qquad (1)$$

where x is a pixel value in the improved cover image, m is the message bits and '*' denotes the LSB substitution operator that embeds ***l*** bits. x′ denotes the obtained stego pixel value after the embedding process. LSB substitution method known as the modified LSB substitution is used here [10,11]. It increases or decreases the most significant bit (MSB) by 1 and thus the square error between the original pixel value and the stego pixel is reduced and hence it increases the quality of the stego images. It adds or subtracts 2^l values to each pixel values.

Thereby a pixel value with x is transformed to x ± 2^l. Both these transformations do not alter the *l* LSB bits of the pixel values[l]. In order to extract the message bits correctly, the edge pixels before and after the embedding process must be the same. The main disadvantage of any steganographic system is that the edges of the images are altered during the embedding process. The proposed system rectifies this flaw with the help of an edge preserving mechanism where the MSBs are preserved at the beginning of the embedding process. Normally, 3 bits are embedded to edge pixels and 2 bits to smooth pixels.

Let x denotes the intensity value of the cover image. Let x′ be the *l*-LSB substituted value of x. After applying the modified LSB substitution method, the pixel x′ may get converted to x″. If the difference between the pixel value of the cover image(x) and x″ is greater than $\mathbf{2^{l-1}}$, then the modified LSB substitution is applied and x″ is calculated as x″= x′+ 2^l or x″= x′- 2^l. The selection of x″ depends on which one will decrease the difference. A final control is used in the edge preserving mechanism. If the MSBs of x″ is same as that of x**'**, then the pixel value with intensity x″ is selected. On the other hand, if they are different then the pixel value with x′ is selected as a pixel corresponding to the stego image. All these processes are done in the sender side. Thus, after the embedding process, the stego image is sent to the receiver side. The authentication of the receiver is ensured with the help of the same key used in the sender side, which adds to the security of the system.

For instance, let the input pixel be 159 which has an equivalent binary, $(10011111)_2$. The edge preserving mechanism preserves the edge by removing the last 4 bits and storing the MSB bits. It is achieved by setting the last 4 LSB bits to zero. So here we get 144, $(1001000)_2$. The pixel value 159 is categorized as an edge or non-edge based on canny edge detection method. If it is an edge then 3 (000) bits of messages are added while in smoother areas we embed only 2 (00)bits. Both the cases where the pixel value 159 is considered an edge as well as a non-edge is shown in Fig. (3). The modified LSB substitution method and also the final control is clearly described in the flowchart given below. The presence of a final control ensures that the embedding process does not alter or modify any of the most significant bits of pixels in the stego image.

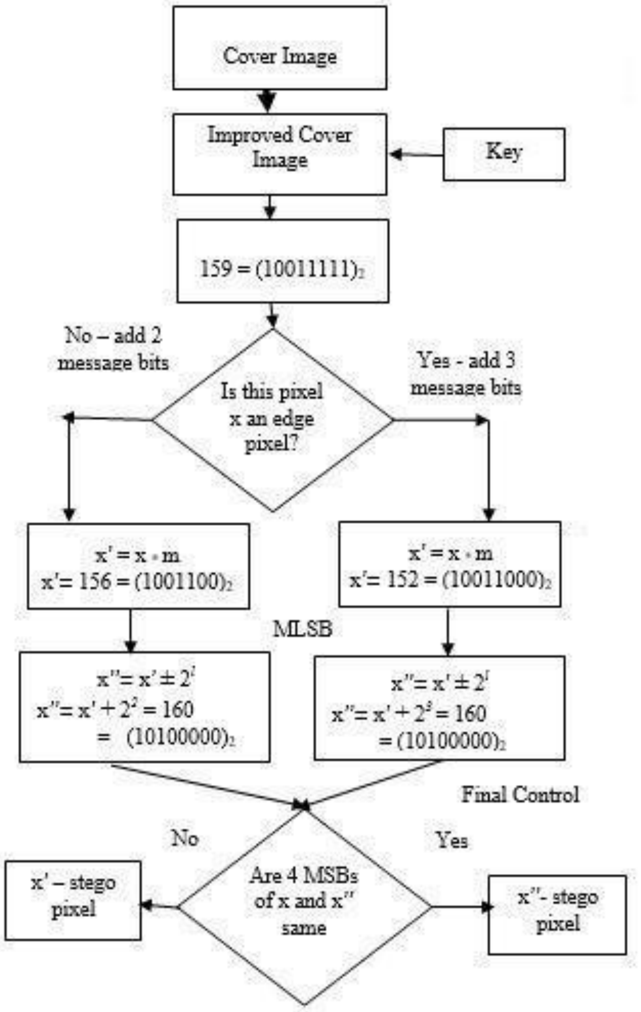
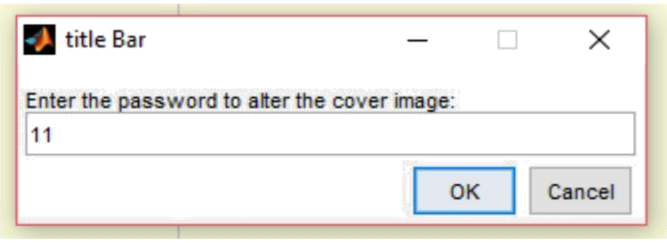


Fig.3 Flow chart showing the entire process of embedding

IV. EXPERIMENTAL RESULTS

This section shows the comparison of various results obtained in the proposed system with some well-known methods proposed in Liao et al. [13] which used 4-pixel differencing and modified LSB substitution (4PVD) and another steganographic method which is known as the Med proposed by Wang [14]. MATLAB 2014a (8.3.0.532) is used as the simulation space. The result obtained is a quantitative comparative study. The experiments are done on the famous Lena image. The original image is reduced to 256×256 so as to reduce the computational complexity. In-order to compare various techniques we make use of an image quality metric known as the Peak Signal-to-Noise Ratio (PSNR). For an M×N gray image, the PSNR value is calculated as:

$$\mathbf{PSNR = 10 \log_{10} (255 / MSE)} \qquad (2)$$



Enter the password to alter the cover image:

11

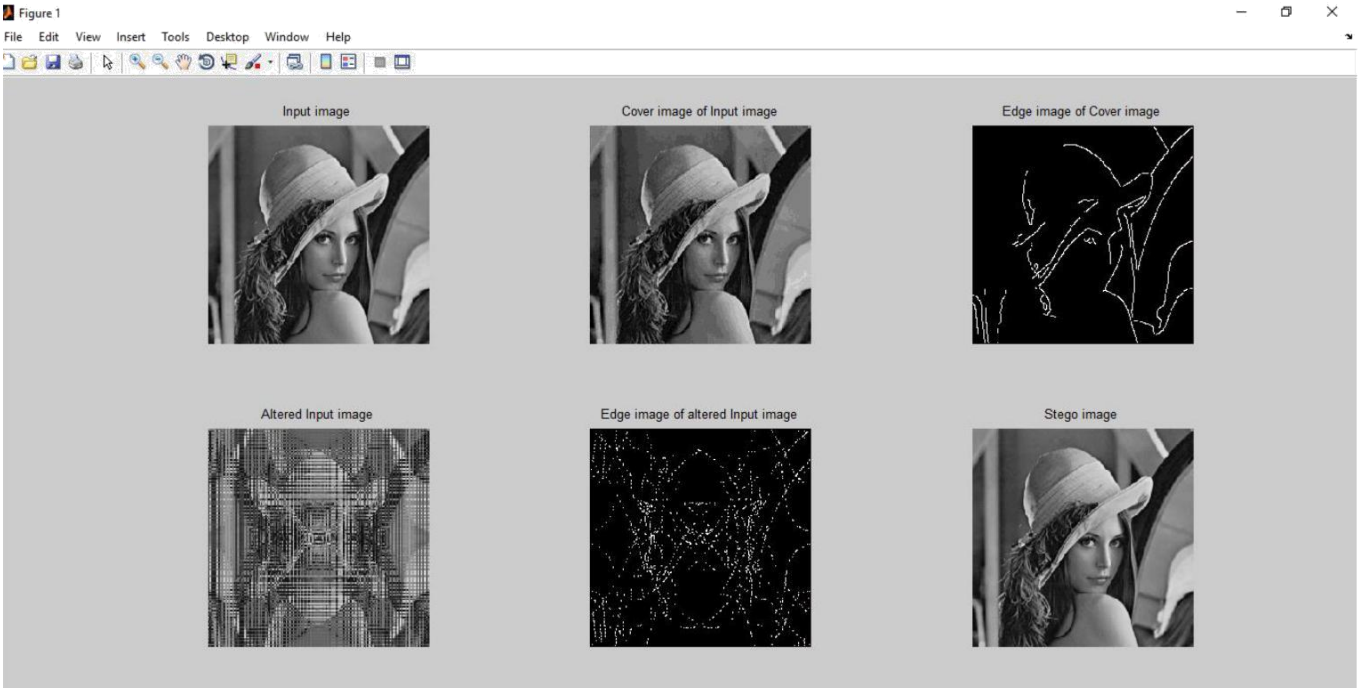
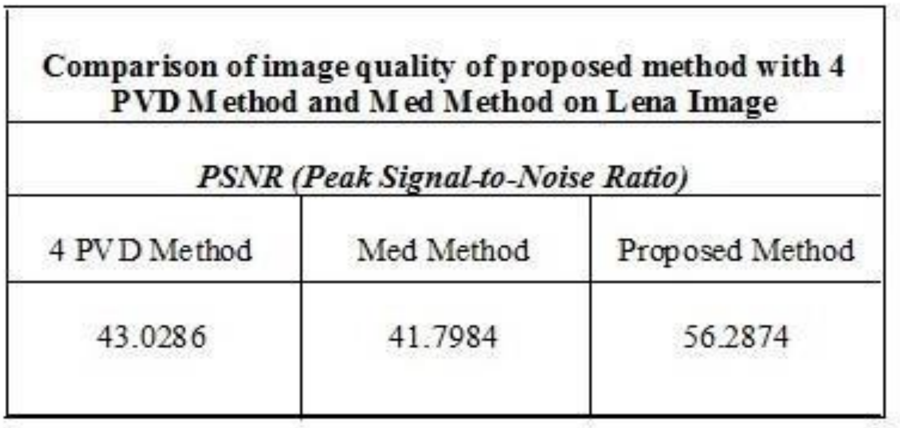


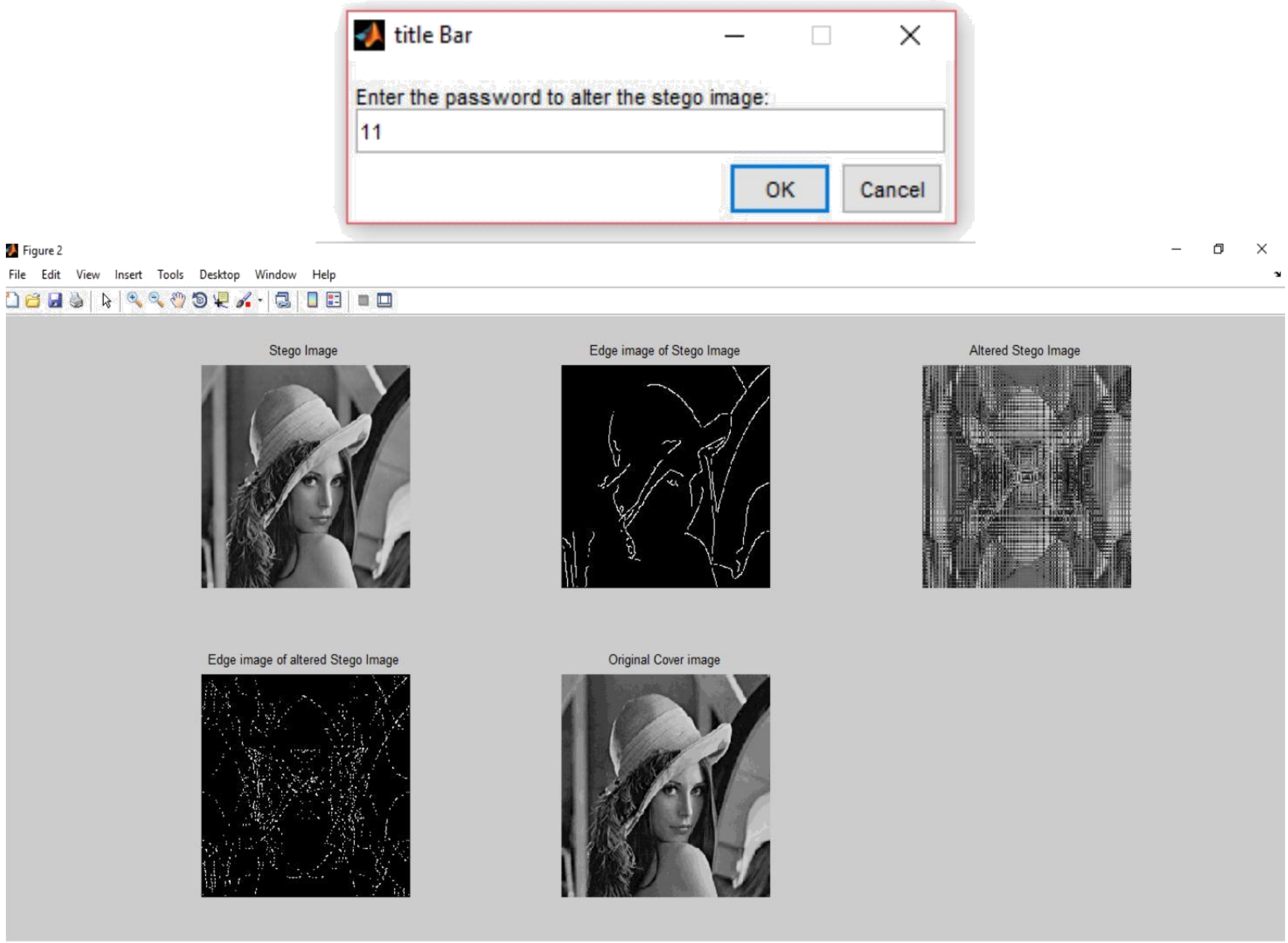
Figure 1
File Edit View Insert Tools Desktop Window Help
Input image
Cover image of Input image
Edge image of Cover image
Altered Input image
Edge image of altered Input image
Stego image

Fig. 4 Output at the sender side

TABLE 1



Comparison of image quality of proposed method with 4 PVD Method and Med Method on Lena Image		
PSNR (Peak Signal-to-Noise Ratio)		
4 PVD Method	Med Method	Proposed Method
43.0286	41.7984	56.2874



title Bar
OK
Cancel
Figure 2
File Edit View Insert Tools Desktop Window Help
Stego Image
Edge image of Stego Image
Altered Stego Image
Edge image of altered Stego Image
Original Cover image

Enter the password to alter the stego image:

11

Fig. 5 Output at the receiver side

Fig. 4 and Fig. 5 denotes the output obtained in the sender side as well as the receiver side respectively. A key is used in both the sender side as well as the receiver side which adds to the security of the system. From Table 1, it is clear that the proposed method provides higher PSNR value of 56.2874(dB) which shows the improved image quality obtained from the system.

V. CONCLUSION

The paper presents a novel steganographic method with higher image quality and better security. The system makes use of canny edge detection which is used to distinguish between edges and smooth regions. Adaptive LSB substitution method adds more number of bits to the edge regions when compared to the non-edge regions. Modified LSB substitution method for embedding the message bits helps to preserve the edges even after the embedding process. Experimental results show that the system provides higher PSNR value when compared to other methods.

REFERENCES

[1] H. Dadgostar & F. Afsari , 'Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB', Journal of information security and applications 30 (2 0 1 6) 94–104.

[2] W. Bender, D. Gruhl, N. Morimoto, A. Lu, 'Techniques for data hiding', IBM Syst. J. 35 (1996) 313–336.

[3] H. Yang, X. Sun, G. Sun, 'A high-capacity image data hiding scheme using adaptive LSB substitution', Radio Eng. 18 (2009) 509–516.

[4] M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber, 'Lossless generalized-LSB data embedding', IEEE Trans. Image Processing 14 (2005) 253–266

[5] Z.-H. Wang, C.-C. Chang, M.-C. Li, 'Optimizing least significant- bit substitution using cat swarm optimization Strategy', Inform. Sci. 192 (2012) 98–108.

[6] S. Wang, B. Yang, X. Niu, 'A secure steganography method based on genetic algorithm', J. Inf. Hiding Multimedia Signal Process. 1 (2010) 28–35.

[7] Z. Zhao, H. Luo, Z.-M. Lu, J.-S. Pan,' Reversible data hiding based on multilevel histogram modification and sequential recovery', Int. J. Electron. Commun. 65 (2011) 814–826.

[8] C.-C. Lin, W.-L. Tai, C.-C. Chang, 'Multilevel reversible data hiding based on histogram modification of difference images', Pattern Recognit. 41 (2008) 3582–3591.

[9]. M. Soleimanpour, S. Talebi and H. Azadi: 'A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain', Iranian Journal of Electrical & Electronic Engineering, Vol. 9, No. 2,pp. 198 203, June 2013.

[10] Yang CH,Weng CY,Wang SJ, Sun HM, ‘Adaptive data hiding in edge areas of images with spatial LSB domain systems’. IEEE Trans Inf Forensic Secur 2008;3(3):488–97.

[11] Lee YK, Chen LH, ‘High capacity image steganographic model’. IEE P-Vis Image Sign 2000;147(3):288–94.

[12] Yang CH,Weng CY,Wang SJ, Sun HM ‘Adaptive data hiding in edge areas of images with spatial LSB domain systems’, IEEE Trans Inf Forensic Secur 2008;3(3):488–97.

[l3] Liao X,Wen QY, Zhang J , ‘A steganographic method for digital images with four-pixel differencing and modified LSB substitution’, J Vis Commun Image R 2011;22(1):1–8.

[14] Wang Y, ‘The LSB-based high payload information Steganography’ In: International conference on mechatronics, electronic, industrial and control engineering (MEIC-15). Atlantis Press; 2015. p. 776–9.