Secret Data Hiding Based on Zigzag Pixel Indicator

P.Mahimah[1]
M.E communication systems
Parisutham Institute of Technology and Science,
Affiliated to Anna University, Chennai, India.
pmahimah@gmail.com

R.Kurinji[2]
Assistant Professor, Dept of ECE,
Parisutham Institute of Technology and Science,
Affiliated to Anna University, Chennai, India.
kurinjirajkumar@yahoo.com

Abstract*— Steganography permits a user to cover the massive amount of secret information inside a image and audio files. It has become a remarkable analysis space to reinforce the safety of network communications, copyright protection etc. In the proposed system the information will be embedded into the LSB of cover image using pixel Indicators in an exceedingly Zigzag manner. The aim is to produce a stronger security by achieving more robust stego-image quality than the prevailing systems. Two different indicators are used, based on those indicators employed in a Zigzag manner the hidden information is embedded into the LSB of the cover image. Finally the stego-image is obtained. For further improving the quality of stego-image OPAP (Optimal Pixel Adjustment Process) method is used. This type of embedding technique creating it tough for any wrongdoer to extract the hidden information from the stego-image.The proposed technique provides higher PSNR value than the prevailing systems.

***Keywords*— LSB, OPAP, Pixel Indicator.**

I. Introduction

The art of concealing data in ways in which stop the detection of hidden messages referred to as Steganography. Some of the techniques utilized in Steganography are domain tools or uncomplicated system such as least significant bit (LSB) insertion. The least-significant-bit (LSB) technique directly replaces the LSBs of the cover-image with the message bits. LSB strategies usually come through high capability [1]. Data embedding is a technique of concealing secret messages into a cover-media such that an uncaused observer won't aware of the existence of the hidden messages. Cover-images with the secret messages embedded in them are referred to as stego-images. In a data hiding strategies, the image superiority refers to the quality of the stego-images [2]. We have a tendency to analysis this pixel indicator technique for RGB [4] pictures Steganography. This technique uses the least significant bits of anyone of the channels Red, green or Blue as indicator of information existence within the other 2 channels. The indicator bits are locate arbitrarily (based on the image nature) among the channel .To improve security; the indicator channel isn't fastened. The Pixel indicators are chosen in a sequence manner. In the cover image the initial pixel Red is the indicator, whereas green is channel one and Blue is that the channel 2. Within the second pixel, green is that the indicator, whereas Red is channel one and Blue is channel 2. In third pixel Blue is that the indicator, whereas Red is channel one and green is channel 2.

Steganography in pictures will be usually exhausted in 2 domains: they're, spacial and transform domain. The proposed method involved in the spacial domain. First the cover image is split into four blocks and every block is additionally divided into 3 planes(R, G, B).At every divided block pixel indicators are used. There are 2 kinds of pixel indicators used (i) Default, (ii) User defined. The secret information will be embedded into the LSB of covering image based on the pixel indicators employed in every divided block. The embedding method is finished in Zigzag manner and also the ensuing image is termed stego-image. For further improving the quality of stego-image OPAP (Optimal Pixel Adjustment Process) method is used. The goal of the proposed system is to achieve higher PSNR than the present systems [3].

II. Proposed Method

In the proposed method, Secret information is embedded into the LSB of the cover image based on the pixel indicators utilized in a Zigzag manner. The aim of the proposed system is to give a high security by achieving higher PSNR value.

A. Methodolog y

In the proposed system, LSB substitution, pixel Indicators, OPAP are used for information concealing. The cover image is employed to cover the secret information. The cover image may be a RGB image, it's twenty four bit depth color image using RGB color model. Twenty four bit in RGB color model refers to eight bit for every RGB color channel, i.e. eight bits for red, bits for green and eight bits for blue. This suggests that we will store 3 bits of data per element at the LSB of RGB image. It's having high embedding capability. The cover image thought of here has the dimensions of (256*256). 1st the cover image is split into four sub images. The dimensions of every sub images are (128*128). When divided into four images the sub images are again divided into 3 planes (R, G, B).Then pixel indicators are applied in every sub image in an exceedingly zigzag manner. The secret information is embedded based on the applied pixel indicator by using LSB substitution method.

*1) LSB Substitution Technique:*LSB technique uses the LSB of consecutive pixels for embedding the message which attracts suspicion to transmission of a hidden message. LSB technique is that the most generally used method because it is easy. LSB technique comes below substitution techniques of Steganography. For concealing most information more than one LSB will be changed. The LSB substitution technique can be used for numerous file formats. In this method, the message is stored within the LSB of the pixels. So neutering them doesn't considerably have an effect on the standard of the cover image. The procedure for such technique is to convert the specified hidden message into binary kind and encrypt every digit into LSB of image [5].

2) Pixel Indicator Technique: The technique uses LSB of anyone of the channels Red, green or Blue as an indicator for engrafting secret data in other two channels. [3]. If the LSB of chosen indicator channel contains 0 means there is no indication it will check the next pixel. If the LSB contains 1,it is an indication for data embedding .There are two types of pixel indicators used in the proposed system. They are,(i)Default,(ii)User defined.

In the Default pixel indicator, Red is fixed as a default indicator. It's denoted as channel one. The 2 least significant bits of the red channel are going to be used as a indication for hidden data in green channel and blue channel. Green is denoted as channel 2 and blue is denoted as channel 3. In User defined pixel indicator technique, among the 3 channels (R, G, B) we can choose anyone as an indicator. The secret information is embedded into the other two channels based on the indicator channel. If Red is that the indicator, green is channel one and Blue is that the channel 2. If green is that the indicator, Red is channel one and Blue is channel 2. If Blue is that the indicator, Red is channel one and green is channel 2.

Figure 1 shows the system architecture for the proposed method. First the cover medium is subdivided into 4 equal sub blocks. Again it is divided into three planes (R, B, G). Then the Pixel indicators Default and User defined is applied in a zigzag manner. For sub image 1 and 4 default pixel indicator is applied. For sub image 2 and 3 user defined pixel indicator is used. By using the least significant bit substitution the secret information is engrafted into the cover medium based on the applied pixel indicators indication.

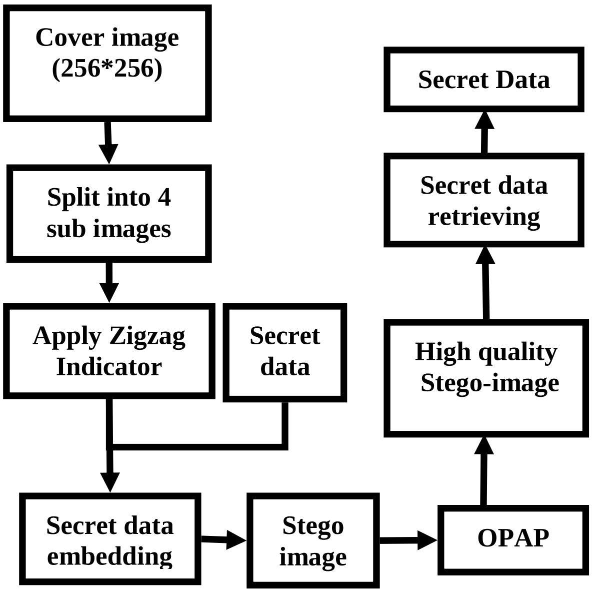


Fig.1.System Architecture for proposed method

Finally the stego-image was obtained. Also greater than 50 dB PSNR value was achieved. For further improving the security OPAP(Optimal Pixel Adjustment Process) method is used. As a result a high quality stego-image is obtained. After that the engrafted secret data is recovered.This type of embedding technique creating it tough for any wrongdoer to extract the hidden information from the stego-image.

III. TESTING PROCEDURE

The parameters used here to measure the proposed method is,

i. PSNR (Peak Signal to Noise Ratio).
ii. MSE (Mean sq. error).

A. PSNR (Peak Signal to Noise Ratio)

Peak signal-to-noise (PSNR) is employed to measure the standard of the stego-images. The PSNR is expressed in decibel (dB). Larger PSNR indicates higher quality of the image or in different terms lower distortion. i.e., there's solely a little dissimilarity between the cover medium and stego-image.The larger the PSNR the smaller the chance of visual attack by human eye. Additionally on the opposite hand, a smaller PSNR means that there's big distortion between the cover-image and the resultant stego-image [7].

$$\text{PSNR} = 10\log_{10} (I^2 / \text{MSE})\text{dB} \qquad (1)$$

Where, I_{max} = Maximum intensity of every pixel.
MSE = Mean sq. error.

B. MSE(Mean square error)

The MSE (Mean sq. Error) is a cumulative square error between the embedded and the original cover image [4]. A lower MSE means that lesser error, and as seen from the inverse relation between the MSE and PSNR, this results to a high PSNR.

$$\text{MSE}= (1/MN)*(\text{original image-stego image})^2 \qquad (2)$$

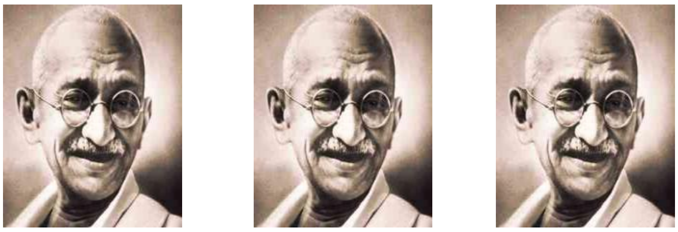
Where, X i, j = original image,
Yi, j = stego-image,
M, N = dimensions of the pictures.

IV. SIMULATION AND EXPERIMENTAL RESULTS

The simulation is completed by using Mat lab (7.9 or higher) version. The secret information is embedded within the cover image of dimension (256*256).The cover pictures taken here is Lena.jpg,, Mahatma Gandhi.bmp.

K=1 K=2 K=3

Fig.2. Simulation results of Lena image



K=1 K=2 K=3

Fig.2. Simulation results of Mahatma Gandhi image

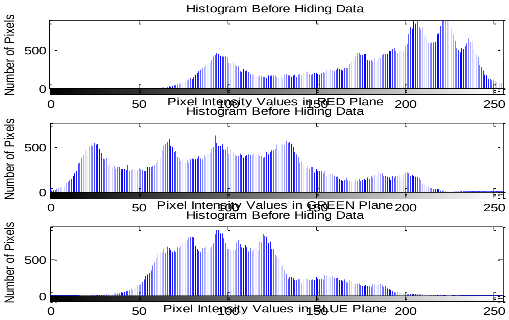


Figure 4(a)

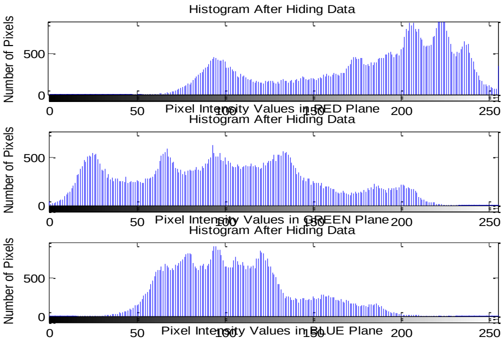


Figure 4(b)

Figure 4(a) & (b). Histogram of Lena Image before and after embedding

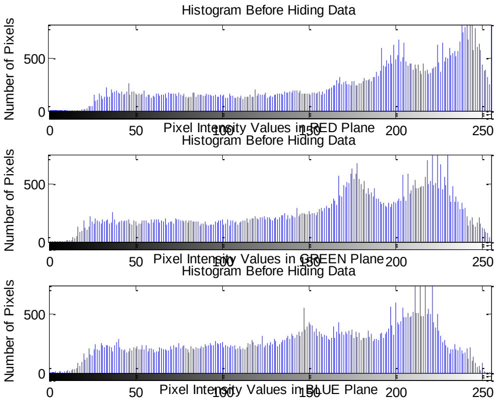


Figure 5(a)

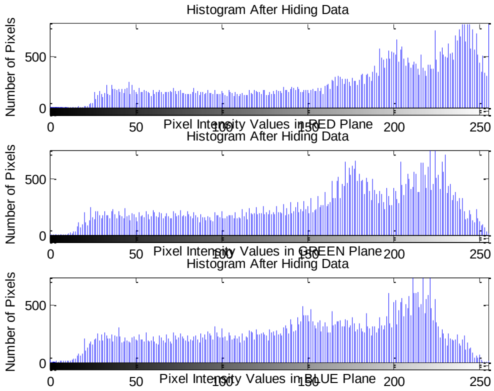


Figure 5(b)

Figure 5(a) & (b). Histogram of Mahatma gandhi image before and after embedding

TABLE I. MSE VALUES OF PROPOSED SYSTEM

Cover image	**No of bits**	**Channel RED**	**Channel GREEN**	**Channel BLUE**
		MSE	***MSE***	***MSE***
Lena	K=1	0.0272	0.0410	0.0402
	K=2	0.1387	0.2126	0.2073
	K=3	0.6359	0.9447	0.9346
Mahatma Gandhi	K=1	0.0281	0.0404	0.0384
	K=2	0.1496	0.2131	0.2054
	K=3	0.6726	0.9514	0.9317

TABLE II. PSNR VALUES OF PROPOSED SYSTEM.

Cover image	**No of bits**	**Channel RED**	**Channel GREEN**	**Channel BLUE**
		PSNR	***PSNR***	***PSNR***
Lena	K=1	63.7817	62.0040	62.0840
	K=2	56.7090	54.8552	54.9645
	K=3	50.0971	48.3780	48.4247
Mahatma Gandhi	K=1	63.6435	62.0659	62.2850
	K=2	56.3820	54.8441	55.0058
	K=3	49.8535	48.3472	48.4379

Table I and 2 shows the Experimental results PSNR (Peak to Signal Noise Ratio), and MSE values obtained in the proposed approach for different embedding capacity (k=1, k=2, k=3) for the cover medium Lena image, Mahatma Gandhi.

V. Conclusion

In the proposed technique, 3 information concealment strategies are proposed. They're pixel Indicator and LSB substitution technique, OPAP. The contributions of the proposed technique are summarized as follows: foremost the cover image is split into four sub images. Then pixel Indicator technique is applied in an exceedingly Zigzag manner .Secondly supported the applied pixel Indicators the secret information is embedded into the LSB of the cover image using LSB substitution method. For further improving the quality of stego-image OPAP is used. Finally the proposed technique gives a high quality stego-image with > 50 dB PSNR.

References

[1] Wien Hong ,“Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique”,0020-0255,2012 Elsevier Inc..

[2] Supriya Rai and Ruchi Dubey, “A Novel Keyless Algorithm for Steganography,” 978-1-4673-0455- 9/12,2012 IEEE.

[3] Amitava Nag, Saswati Ghosh,”An Image Steganography Technique using X-Box Mapping,” IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012 ,ISBN: 978-81-909042-2-3.

[4] S. M. Masud Karim, Md. Saifur Rahman,”A New Approach for LSB Based Image Steganography Using Secret Key,” Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 2011 IEEE.

[5] J. AnitaChristaline1, D.Vaishali, ”Image steganographic techniques with improved embedding capacity and robustness,” 978-1-4577-0590-8/11, ICRTIT 2011 IEEE.

[6] Gandharba Swain and Saroj Kumar Lenka,“A Novel approach to RGB channel Based Image Steganography Technique,” International Arab Journal of e-Technology, vol. 2, No. 4, June 2012.

[7] R.Amirtharajan, Sandeep Kumar Behera, “Colour Guided Colour Image Steganography,” Universal Journal of Computer Science and Engineering Technology, ISSN:2219-2158, 2010 UniCSE.

[8] M. Khodaei, K.Faez,, “New adaptive steganographic method using least significant-bit substitution and pixel-value differencing,” published in IET Image Processing, The Institution of Engineering and Technology 2012.

[9] El-Sayed M. El-Alfy, Azzat A. Al-Sadi,“Improved Pixel Value Differencing Steganography Using Logistic Chaotic Maps,” International Conference on Innovations in Information Technology (IIT) , 978-1-4673-1101-4/12,2012 IEEE.

[10] Chi-Kwong Chan, L.M. Cheng, “Hiding data in images by simple LSB substitution,” 0031-3203, 2003 Pattern Recognition Society. Published by Elsevier Ltd2003.

[11] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, “Digital image steganography: Survey and analysis of current methods,” 0165-1684, 2009 Elsevier B.V.

[12] Gandharba Swain and Saroj Kumar Lenka,“A Better RGB Channel Based Image Steganography Technique,” CCIS 270, pp. 470–478, Springer-Verlag Berlin Heidelberg 2012.

[13] Ramadhan Mstafa, Christian Bach,” Information Hiding in Images Using Steganography Techniques,” 2013 ASEE Northeast Section Conference Norwich University Reviewed Paper.

[14] Fei Wang , Liusheng Huang,” A novel text steganography by context-based equivalent substitution, ” 2013 IEEE International Conference on signal Processing,Communication and computing(ICSPCC) , 5-8 Aug. 2013, INSPEC Accession Number:13899216, 10.1109/ICSPCC.2013.6663950.

[15] Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub,” RGB Intensity Based Variable-Bits Image Steganography,” 2008 IEEE Asia-Pacific Services Computing Conference, 978-0-7695-3473-2/08.