A Novel Approach for Parallel Encoder by Pixel Bit Manipulation

P.Gitanjali [#1] , R.Manikandan[*2]
[#1]Department School of Computing, SASTRA University, Thanjavur,TamilNadu, India.
[*2]Senior Asst Prof, School of Computing, SASTRA University, Thanjavur,TamilNadu India.
gitanjali.moorthy@gmail.com
manikandan75@core.sastra.edu

***Abstract* - Steganography is art of hiding the secure information. The propaganda may be embedded in all form of multimedia files.To hide the secret data, the binary image, intensity image or RGB images(true color image) are used as a cover images in the steganography. In existing proposals a normal architecture has been developed by using hardware for 8-bit pixel manipulation. In this proposed method, 24-bit will be manipulated simultaneously by the decoder and a maximum of 8 bits has been flipped to hide 12 bits in secret message in each pixel. Besides this methodology not only embed message in Least Significant Bits, but also hide the secret message in 5,4, 2 and 1 or any one of the likely arrangements. Comparison is made between the MSE and PSNR for existing and proposed system. In the proposed method the algorithm is implemented in the FPGA hardware in an efficient way , considering the hardware resources and power.**

Keywords-Color Image steganography; Information Encryption; Encoder circuit; Decoder circuit.

I. INTRODUCTION

Cryptography, in general, means shielded lettering which includes a massive array of covert communications methodology that hides the message presence. An important sub discipline of information hiding is Steganography, wherein the message is concealed within an image. The applications of cryptography are very common that anyone can identify the secret key. Steganography is used to increase obscurity. The three most popular and researched uses for Steganography in an open systems environment are printers, digital watermarking, intelligence bureau etc.

The information bit is embedded in a cover image, which can be in jpeg or png format, by the stegosystem encoder. The resulting stegoimage is then transmitted via channel. The estimate of stegoimage is then decoded, to produce the estimate of the message, by the decoder which uses the same key that is used by the transmitter. The cover used in this method is an image. Most probably image are used as a cover medium for steganography, because of their inherent nature to provide high safekeeping, toughness also ability too.

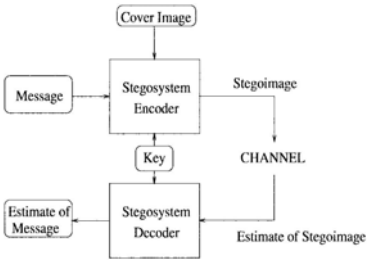

Fig 1. Overview of Steganographic system[1]

Domains used for hiding message in the cover medium is broadly splitted into spatial based[1] and frequency based steganography[1].In spatial-based steganography, the data is rooted into the image pixel's LSB using stego algorithms while frequency-based steganography, allows to convert pixels to frequency domain by means of renovation mechanism preceding this secret data is get hidden in the constants, but afore transformation it is essential be transformed back into spatial based to certify insignificance of secret data.

Steganography is used to, but not restricted to, the below specified field: private communication and secret message saving, fortification of data amendment, admittance control system for digital data circulation, Mass communication Database systems. Steganography provides us with: Potential capability to hide the existence of confidential data, Hardness of detecting the hidden (i.e., embedded) data, Strengthening of the secrecy of the encrypted data.

In Section II the previous research has been explained. An newly designed decoder is explained in Section III. Comparing the value of PSNR and MSE between previous work and newly proposed work is done in Section IV whereas in last section, the analysis of an newly designed decoder is concluded.

II. RELATED WORKS

In existing method,it marginally shrinks inaudibility but upturns the embedding capacity. The chance that a pixel was permitted to flipped is given below:

•By flipping one bit in the pixel of the original image, is leads to embed four message bits in the place of last four bits in the pixel of the original image(cover).

•By the flipping the two bits of the original image, four bits of the message get embedded. In this type, four of its bits were inserted with a maximum flipping of two bits.

Decoder has been designed to obtain stego pixels. The decoder circuit is used to flip the pixel of the cover effigy, to yield new stego-image. In decoder circuit, the leading five LSB of each pixel are set as inputs. The circuit does only XOR function, in order to produce the outputs O1, O2, O3, and O4. Hidden information can split into many groups where each group contains four bits. If O1, O2, O3,O4 were the identical as secret data, there will not be any kind of modification will take place. Or else, flip the pixels of the cover medium, in such a manner that the result of the circuit to be equal to the secret data.

III. PROPOSED WORK

In this proposed method, 24-bit will be manipulated simultaneously by the decoder and a maximum of 2 bits in one pixel has been flipped to hide 4 bits of message. Here, the data is embedded in 5,4,3 and 1 or any one of the fifteen combinations. The decoder used in this method is shown below.

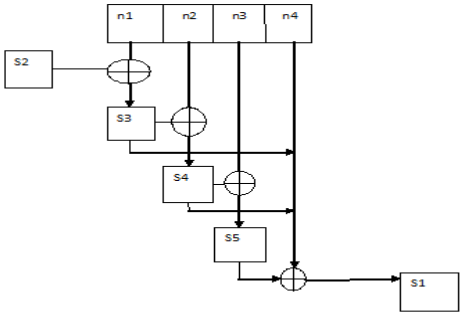

Fig.2 Decoder circuit

Here, the first four least significant bits are given as input to the decoder. XOR operation is performed. S1, S2, S3, S4, S5 are the results of XOR operation. The decoder has been designed to handle 24 bits with a maximum of one or two bit alteration. The message bit considered here is of 4 bits. The data is embedded in , 5,4,3 and 1 or any one of the fifteen combinations.

A. Embedding algorithm:

1. Read the secret data.
2. Convert secret data to binary format.
3. Secret data 4 bits is given to the decoder circuits.
4. Stego pixels of 5 bits are obtained.
5. Embed the stego pixel in the equivalent position of the decoder inputs in the cover image.
6. If message length is not equal to zero

   Goto step3
7. Save and transfer this stego image.

B. Extraction algorithm:

1. Read the stego image.
2. Convert its pixel into binary format.
3. Last five bits of each pixel is supplied as a input to the extraction design(circuit).
4. Repeat preceding stage until complete secret image is obtained.
5. Store the result data.

IV. RESULTS AND DISCUSSIONS

To appraise the efficiency for the above design decoder circuit we used two parameters MSE and PSNR. For example we took four 128x128 images such as lena, baboon, Gandhi, temple as cover images. The secret image used here is sastra logo which is 64x64 image. As a result we get four stego images, such that we compute the PSNR and MSE value for the four stegoimages using the following equations:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

Where M and N are rows and columns of the matrix of the image's pixels and R denotes the maximum disturbance occurs in the resultant image.

Comparsion is made between the MSE and PSNR for existing and proposed system.

Fig 3. Original images

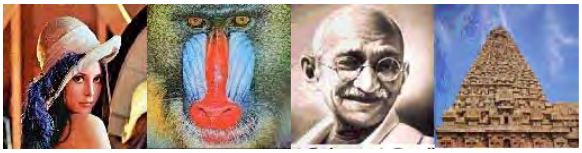

Fig4. Stego images

TABLE I
Comparision between existing method and proposed method

Cover images	**Existing Method**		**Proposed Method**					
	MSE	**PSNR**	**R(RED)**		**G(GREEN)**		**B(BLUE)**	
			MSE	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**
Lena	38.4405	32.2829	32.3553	37.8051	33.6644	27.9664	32.8385	33.8243
Gandhi	34.7573	32.7203	6.4136	40.0598	7.1364	39.5960	6.1652	40.2313
Temple	37.5218	32.3880	8.0360	39.0804	8.3692	38.9039	7.7184	39.2555
Baboon	35.6992	32.6042	31.5020	46.0134	31.9014	41.9698	31.5189	45.8345

V.CONCLUSION

Thus we have implemented decoder circuit for 24 bit color image to obtain stego image here by using 24 bit we can embed eight bits per pixel additionally compare to previous work . This proposed method can

be further enhanced by using audio or video in the place image as a cover and message object.

REFERENCES

[1] Siva Janakiraman, Anitha Mary.A, Jagannathan Chakravarthy," Pixel Bit Manipulation for Encoded Hiding", International Conference on Computer Communication and Informatics (*ICCCI* -2012),
[2] Amirtharajan, R., & Balaguru, R. J. B. (2009). "Tri-layer stego for enhanced security - A keyless random approach". Paper presented at the 2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications, IMSAA 2009.
[3] Ali Daneshkhah , Hassan Aghaeinia, Seyed Hamed Seyedi,'' A More Secure Steganography Method in Spatial Domain", SecondInternational Conference on Intelligent Systems, Modelling and Simulation.2011
[4] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding—a survey, Proc. IEEE 87 (7) (1999) 1062–1078.
[5] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding" IBM Syst. J. 35 (3&4) (1996) 313–336.