Volume 4, No. 2, Jan-Feb 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Some Steganographic Techniques using Bit Plane Slicing with their Embedding capacity

H. Faheem Ahmed
Department of Computer Science
Islamiah College, Vaniyambadi Tamil Nadu, India
hfaheemahmed@rediffmail.com

U. Rizwan*
Department of Mathematics
Islamiah College, Vaniyambadi Tamil Nadu, India
rizwanmaths@yahoo.com

Abstract: In this paper, a new steganographic technique using the bit plane slicing is proposed. The actual image and the data embedded stego-images using the techniques are given. The Mean Square Error (MSE) and Peak to Signal Noise Ratio (PSNR) values have been determined. Histograms for the computed values of MSE and PSNR indices and embedding capacity are drawn.

Keywords: Steganography, MSE, PSNR, LSB, Bit Planes.

I. INTRODUCTION

Gray scale images can be transformed into a sequence of binary images by breaking them up into their bit-planes. If we consider the grey value of each pixel of an 8-bit image as an 8-bit binary word, then the 0th bit plane consists of the last bit of each grey value. Since this bit has the least effect in terms of the magnitude of the value, it is called the least significant bit, and the plane consisting of those bits the least significant bit plane. Similarly the 7th bit plane consists of the first bit in each value. This bit has the greatest effect in terms of the magnitude of the value, so it is called the most significant bit and the plane consisting of those bits the most significant bit plane.

Faheem Ahmed and Rizwan [2] have introduced a new concept in data embedding. The authors have embedded text message and digital image in audio files. They have also presented a technique for embedding text message and/or digital image in another image. A lot of examples have been presented. Fridrich etal. [3] have studied quantitative stegnanalysis of digital images. They have estimated the length of the secret message. Rizwan and Faheem Ahmed [5] have made a comprehensive study on various types of steganographic schemes. Faheem Ahmed and Rizwan [6] have introduced and studied seven different steganographic techniques applying randomization concept. They have also computed the MSE and PSNR indices for these techniques. Structural similarity indices have also been determined.

Let A be the 5x7 image.

$$A = \begin{matrix} 167 & 133 & 111 & 210 & 34 & 56 & 78 & 211 \\ 87 & 144 & 140 & 135 & 44 & 88 & 34 & 123 \\ 159 & 154 & 148 & 87 & 45 & 88 & 12 & 242 \\ 34 & 89 & 77 & 123 & 87 & 36 & 90 & 91 \\ 78 & 123 & 98 & 156 & 189 & 187 & 20 & 201 \end{matrix}$$

The image A in its binary equivalent is

10100111	10000101	01101111	11010010	00100010	00111000	01001110	11010011
01010111	10010000	10001100	10000111	00101100	01011000	00100010	01111011
10011111	10011010	10010100	01010111	00101101	01011000	00001100	11110010
00100010	01011001	01001101	01111011	01010111	00100100	01011010	01011011
01001110	01111011	01100010	10011100	10111101	10111011	00010100	11001001

Let the message to be embedded is Hello Welcome to Steganography

If 1st bit (LSB) position of each element in each row is used we can embed 5 characters Hello. Then matrix A becomes

166	133	110	210	35	56	78	210
86	145	141	134	44	89	34	123
158	155	149	86	45	89	12	242
34	89	77	122	87	37	90	90
78	123	99	156	189	187	21	201

If 1st bit (LSB) and 2nd bit positions of each element in each row are used we can embed 10 characters Hello Welc. Then matrix A becomes

164	133	110	208	33	56	76	208
84	147	141	134	44	91	34	123
156	155	151	84	45	91	12	242
32	91	79	120	87	39	88	88
76	123	99	156	189	185	23	203

If 1st bit (LSB), 2nd bit and 3rd bit positions of each element in each row are used we can embed 15 characters Hello Welcome t. Then matrix A becomes

160	133	110	208	37	60	76	212
80	151	141	130	44	95	34	127
152	159	151	80	41	95	8	246
32	91	79	120	83	35	88	88
72	127	103	156	185	189	19	203

If 1st bit (LSB), 2nd bit and 3rd bit ,4th bit positions of each element in each row are used we can embed 20 characters Hello Welcome to Ste. Then matrix A becomes

160	141	110	208	45	60	76	220
80	151	141	130	36	87	34	119
144	159	151	88	33	87	8	254
32	91	79	120	83	43	80	80
64	127	111	148	177	189	19	203

If 1st bit (LSB), 2nd bit and 3rd bit ,4th bit,5th bit positions of each element in each row are used we can embed 25 characters Hello Welcome to Steganog. Then matrix A becomes

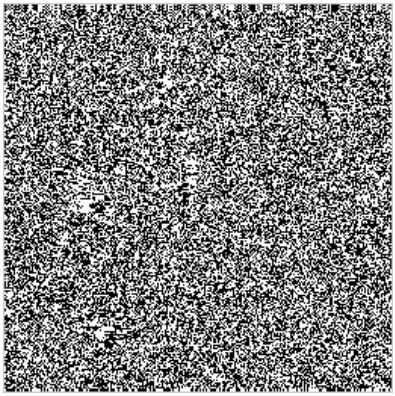
160	157	126	192	45	60	92	220
64	151	157	130	36	71	34	119
128	159	151	72	49	87	24	238
32	91	91	104	83	59	80	80
64	127	127	132	161	189	19	219

and so on.

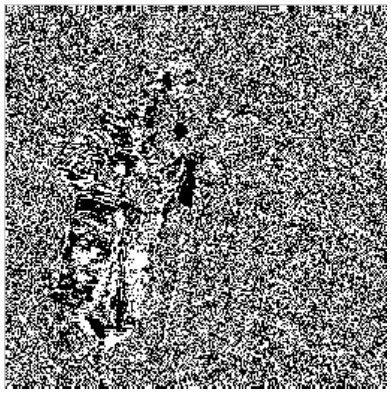
We use the cameraman.tif 256 x 256 gray scale image shown in fig 1.

Figure 1. Actual Image

The actual image in figure 1, is sliced into 8 distinct figures in their bit planes 0 to 7 and are shown in figures 2 (a) to (h).

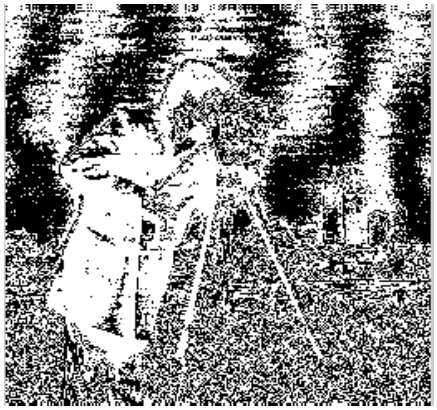


(a)

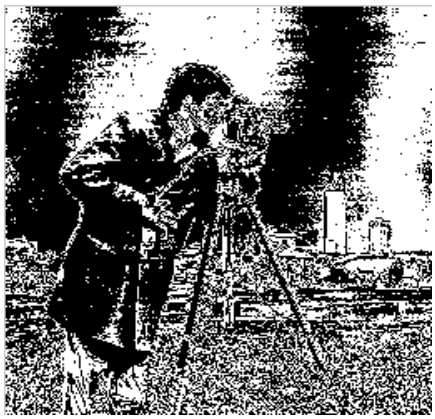


(b)

(c)



(d)



(e)

(f)

(g)

(h)

Figure 2. The bit planes of an 8-bit greyscale image. (a) Bit 0 (LSB), (b) Bit-1, (c) Bit-2 ,(d) Bit-3, (e) Bit-4, (f) Bit-5, (g) Bit-6, (h) Bit(7)(MSB)

Now we take a 256 x 256 gray scale cameraman.tif image and shall embed using each bit planes. The resulting figure with number of characters embedded in each bit plane is given in figures 3 (a) to (h).

(a)

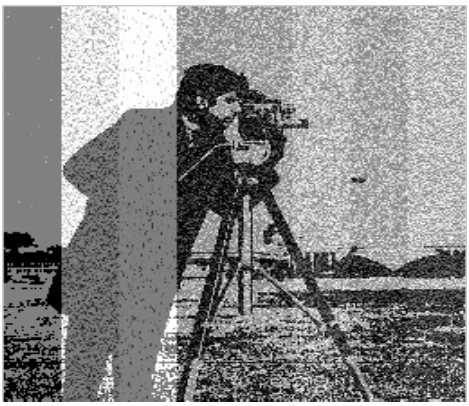
(b)

(c)

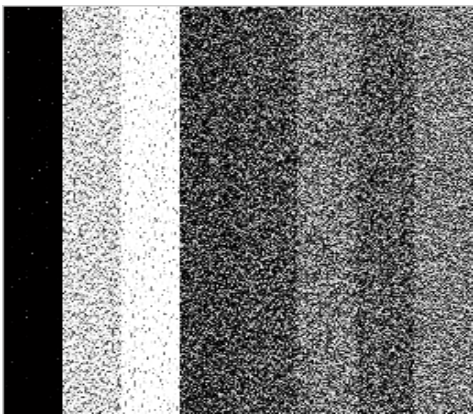
(d)

(e)

(f)



(g)



(h)

Figure 3. The bit planes of an 8-bit greyscale image after embedding text. (a) Bit 0 (LSB), (b) Bit-1, (c) Bit-2 ,(d) Bit-3, (e) Bit-4, (f) Bit-5, (g) Bit-6, (h) Bit(7) (MSB)

The Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) are performance parameters to measure the quality of image.[6]

a. ***MSE:*** It is defined as square of error between cover stego-image. The error indicates the distortion in an image.MSE can be calculated by using two dimensional mathematical equation described as follows:

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - \bar{X}_{ij}\right)^2$$

where Xij = the value of pixel in cover image and $\bar{X}_{ij}$ =the value of pixel in stego-image and N is the size of image.

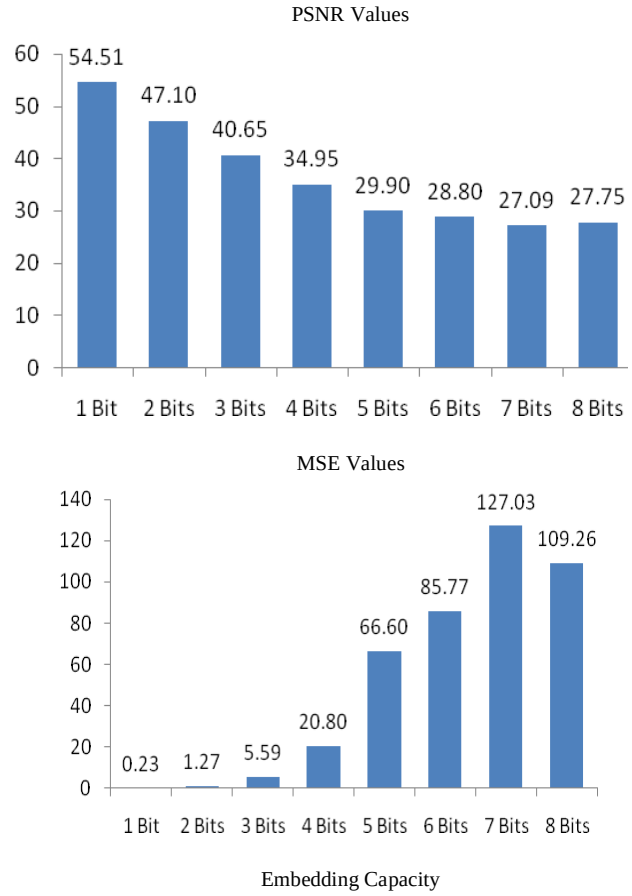
b. ***PSNR:*** It is a measure of quality of image. PSNR can be calculated by using the mathematical formula given below:

$$PSNR = 10 \text{ x } \log \frac{255^2}{MSE} \text{db}$$

Table 1. The computed values of PSNR , MSE and Embedded capacity

S.No	Number of Bits Used	PSNR	MSE	Embedded Capacity
1.	1st Bit (LSB)	54.50900	0.23024	8192
2.	1st , 2nd Bits	47.10310	1.26698	16384
3.	1st ,2nd , 3rd Bits	40.65414	5.59328	24576
4.	1st ,2nd ,3rd, 4th Bits	34.94929	20.80423	32768
5.	1st ,2nd ,3rd, 4th , 5th Bits	29.89638	66.59515	40960
6.	1st ,2nd ,3rd, 4th ,5th , 6th Bits	28.79762	85.76668	49152
7.	1st ,2nd ,3rd, 4th ,5th ,6th, 7thBits	27.09164	127.03297	57344
8.	1st ,2nd ,3rd, 4th ,5th , 6th, 7th ,8th (MSB)Bits	27.74600	109.26486	65536

The histograms for the computed values of PSNR and MSE indices and embedding capacity for each of the bit planes are presented in figure 4.



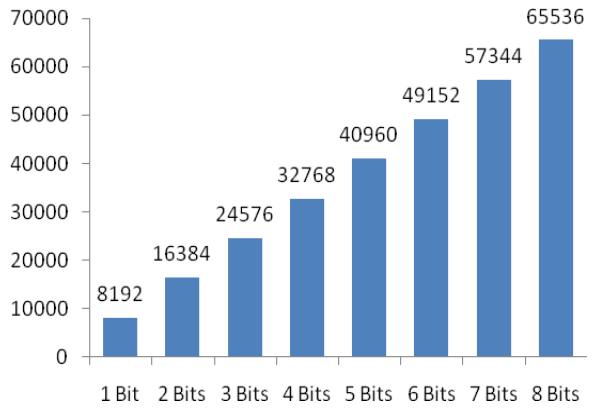


Figure 4. Histograms for PSNR, MSE indices and embedding capacity

II. CONCLUSION

In this article, a new steganographic technique using the bit plane slicing is introduced and studied. Considering the cameraman.tif image in 256 x 256 gray scale, the data embedded stego-images using the proposed technique of slicing the 8 different bit planes are shown explicitly. The MSE and PSNR indices with their respective maximum embedding capacity are presented. Statistical analysis has been carried out.

III. REFERENCES

[1] Cachin. C., An information-theoretic model for steganography, Information and Computation, Vol. **192** (1), Ed. Academic, USA, pp. 41 – 56, 2004.

[2] Faheem Ahmed, H and Rizwan. U, An Alternative Technique in Data Embedding, Advanced Materials in Physics, pp 233 – 242, 2012

[3] Fridrich, J, M. Goljan, D. Hogea and D. Soukal, Quantitative steganalysis of digital images: estimating the secret message length, Multimedia Systems Journal - Special issue on Multimedia Security, Vol. **9 (**3), pp. 288 – 302, 2003.

[4] Rafael Gonzalez and Richard E. Woods, Digital Image Processing, Addison-Wesley, second edition, 2002.

[5] Rizwan. U and Faheem Ahmed. H, Comprehensive study on various types of steganographic schemes and possible steganalysis methods for various cover carrier like image, text, audio and video, International Journal of Scientific and Engineering Research, Volume **3 (**11), November 2012, pp 151 – 154.

[6] Rizwan. U and Faheem Ahmed. H, A New Approach in Steganography using different Algorithms and Applying Randomization Concept, International Journal of Advanced Research in Computer and Communication Engineering, Vol.**1** (9), November 2012, pp 233 – 242.

Short Bio Data for the Author

H. Faheem Ahmed earned his M.Tech. degree in Information Technology from Punjabi University and M.Phil. degree course in Computer Science from Manonmaniam Sundaranar University. He is pursuing Ph.D. in Computer Science. He has guided 50 M.Phil. research scholars in Computer Science. He is currently the Head of the Department of Computer Science and Applications, Islamiah College, Vaniyambadi and is serving the institution for the past 28 years. His research interest includes Steganography and Image processing. He has published 8 research articles and authored one book.

U. Rizwan earned his Ph.D. degree in Mathematics from the University of Madras. He is currently the Head of the Department of Mathematics, Islamiah College, Vaniyambadi and is serving the Institution for the past 26 years. He has published 43 research articles in journals of international repute. He has authored 7 books and is also the editor of two international journals. He has guided 30 M.Phil. in Mathematics scholars and one M.Tech. (IT) candidate. Presently, he is guiding Ph.D. research scholars in Mathematics and Computer Science. His research interest includes Image Processing, Hacking algorithms, Stochastic Processes, Fuzzy Logic, etc. He is the member of the board of studies in PG Mathematics of Thiruvalluvar University, Vellore. He is also an Academic Auditor.