Random Traversing Based Reversible Data Hiding Technique Using PE and LSB

Rhythm Katira[#1], Prof. V. Thanikaiselvan [*2]
[#] ECE Department, VIT University
Vellore, Tamil-Nadu, India
[1] rhythm.katira2009@vit.ac.in
[*] ECE Department, Assistant Professor (senior)
VIT University, Vellore, Tamil-Nadu, India
[2] thanikaiselvan@vit.ac.in

Abstract

The rise in the use of internet, secure transmission of the data has become an utmost priority. Steganography makes the data invisible by hiding it in the multimedia such as image, audio or video file and thereby covering for its existence. In this project we use prediction error (PE) technique steganography and Least Significant Bit (LSB) substitution method to hide data in the image. As we do PE expansion method it can lead to expansion of pixels like it can lead to pixel value above 255. In order to solve this problem, we restricted the pixel values between 15 and 240.The PSNR was high at low threshold values. The hiding capacity increased with increase in threshold with a reasonable decrease in PSNR. There was 2dB difference then other methods because of high data hiding capacity. Also we have used knight's tour for increasing the security of data hidden. In comparison to other methodology, this methodology proves to be better and more effective.

Keywords: Steganography, LSB, Knight's tour, Random traversing, PE expansion.

I. INTRODUCTION

Now-a-days the internet has become the greatest used channel for the transmission of the multi-media data like audio, image, video, text etc. But this transmission is under serious threat of the hackers and eavesdropper. The method Cryptography [1] [2] is used to send the data secretly. But the encrypted message is attracted and comes to notice of all and thus the eavesdropper come to know that some data is hidden in this multi-media file. So in order to solve this problem we use another technique called Steganography. In this method the cover image is used to embed the data and the image generated is stego-image which is similar to cover image and the change is unnoticed unless someone is looking for it carefully. Presently, there are two types of data hiding method namely irreversible [3], [4] data hiding method and reversible [5], [6], [7], [8], [9] data hiding method. Irreversible data hiding method is the data hiding method in which the user can't retrieve the cover image from stego-image after embedding the data in the image. But it still has an advantage of having high hiding capacity and good image quality. The reversible data hiding technique overcomes this problem as it recovers the original cover image back from the stego-image without any distortion. Hence reversible data hiding can be used for the transmission of the military and medical images. A reversible data hiding method using difference expansion (DE) [9], [10], [11] was proposed in 2003. In this method, we find the difference between adjacent pixels and then double it, generating an even number.

In embedding, if the data was 0, the difference was unchanged, while if the data is 1, the difference was odd. By subtracting the two adjacent pixel values we can find the secret data from their LSB. An expansion scheme based on prediction error (PE) to embed secret data [12] was proposed in 2007. This method used predicted function to predict the pixel value and then find the difference between them. Prediction error was increased to two times for data embedding. In this paper, we propose a reversible data hiding method based on PE expansion method and LSB substitution method in order to avoid any kind of distortion due to embedding; we use an absolute threshold [13], [14] value to determine whether the pixel can be used to embed the secret data. If the pixel value is higher than threshold, the pixel remains unchanged to achieve high image quality.

The rest of the paper is organized as follows. In Section 2, we have the theory related to this paper like PE expansion, LSB substitution method and knight's tour with performance measures. Proposed methodology is explained in Section 3. Section 4 gives result and discussion. Paper's conclusion is in Section 5.

II. RELATED WORKS

2.1 PE expansion method (Method 1):

Proposed by Thodi[12] in 2007.

2.1.1 Embedding process:

Step 1: Divide the cover image into overlapping 2×2 blocks. The block is represented as:

K	l
M	N

Fig. 1, 2×2 Block Example

where k is the current embedding pixel.

Step 2: The prediction value ˆp can be calculated as:

$$\hat{p} = \begin{cases} \min(b,c), if \;\; a \ge \max(b,c) \\ \max(b,c), if \;\; a \le \min(b,c) \\ \quad b+c-a, otherwise \end{cases} \quad (1)$$

Step 3: Compute the prediction error e between the current embedding pixel p and the prediction value ˆk, i.e., e=k− ˆk.

Step 4: Calculate the stego pixel p’ by

$$k' = \hat{k} + (2\times e) + w \quad (2)$$

where w is secret data and w Є {0, 1}.

2.1.2 Extraction process:

Step 1: The stego image is divided into several overlapping 2×2 blocks. The four pixels in one block can be represented as:

k’	l
m	n

Fig. 2, 2×2 Block Example for extraction

where k’ is the current embedding pixel.

Step 2: The prediction value ˆk’ can be calculated as:

$$\hat{p}' = \begin{cases} \min(b,c), if \;\; a \ge \max(b,c) \\ \max(b,c), if \;\; a \le \min(b,c) \\ \quad b+c-a, otherwise \end{cases} \quad (3)$$

Step 3: Compute the prediction error e’ between the current embedding pixel p’ and the prediction value ˆk’, i.e., e’=k’− ˆk’, where ^k’ is predicted value and k’ is the current stego pixel.

Step 4: The embedded data w can be extracted from the LSB of the prediction error e’, and the original pixel can be recovered as:

k= ^k’+ (e’/2);

2.2 LSB substitution method (Method 2):

The least-significant-bit (LSB) is the most widely used spatial domain data hiding technique. It generally embeds the same amount of data as the LSB pixels.

2.2.1 Embedding process:

$$r_i' = r_i - r_i \bmod 2^n + s_i, \quad (4)$$

where s_i represents decimal value of n-bit message bits to be embedded.

2.2.2Extraction process:

In the extraction process, given the stego-image, the embedded messages can be readily extracted without referring to the original cover-image. Using the same sequence as in the embedding process, the set of pixels storing the secret message bits are selected from the stego-image. The n LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits. Mathematically, the embedded message bits can be recovered by

$$s_i'=r_i' \bmod 2^n, \quad (5)$$

where s_i’ is the extracted message bits (in decimal).

2.3 KNIGHT'S TOUR:

Knight's tour [15] is a random traversing method that increases the security of data by randomly embedding the data into pixel. It does this based on the way a knight moves on a chessboard. It takes 2 step vertically and 1 step horizontally or 1 step vertically and 2 steps horizontally. Thus it moves in 'L' shape. In the knight's tour, if it comes to know the starting point of embedding still it will be difficult to guess the correct path of the data embedding and thus increasing the security of the data embedded. Here a 8×8 matrix is taken which is assumed to be cylindrical in shape and thus at the last column the movement can be taken to the first column and the path can be completed.The following are four possible knight's tour:

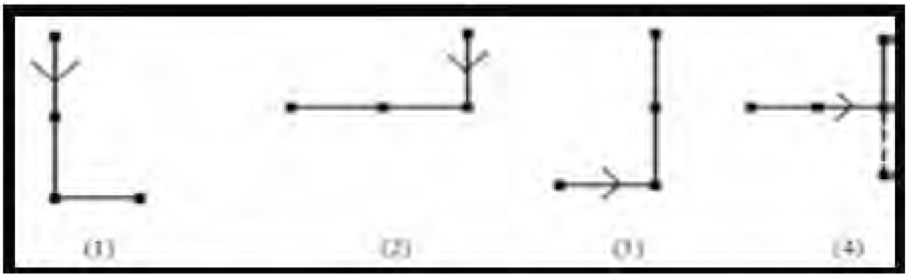

Fig. 3: Four ways of traversing

Table 1: 8 × 8 matrix after Knights tour as:

61	46	49	34	53	38	57	42
64	35	52	39	56	43	60	47
13	62	1	50	5	54	9	58
16	51	4	55	8	59	12	63
29	14	17	2	21	6	25	10
32	3	20	7	24	11	28	15
45	30	33	18	37	22	41	26
48	19	36	23	40	27	44	31

2.4 Performance measures:

In this project we calculate the PSNR between the cover image and stego image (PSNR1) and also between cover image and cover image after extraction (PSNR2). The PSNR is calculated as:

$$\mathrm{PSNR}=10 \times \log_{10} 255^2/\mathrm{MSE}\ (\mathrm{dB}) \qquad (6)$$

$$\mathrm{MSE}=(1/W\times H)\ \Sigma^{W}_{i=1}\ \ \Sigma^{H}_{j=1}\,(I(i,j)-I'(i,j))^2 \qquad (7)$$

where MSE is the mean square error and W×H is the matrix size say 512×512 or 256×256.Also we calculated PSNR for various images like Boats, Lena, Barbara, Gold-hill, and peppers. A graph is also plotted between PSNR and various threshold values depicting the change of PSNR with threshold for above five images.

III. PROPOSED METHODOLOGY

3.1 Embedding Algorithm

Step 1: Divide the cover image into blocks of 2×2 size. Now the last row and last column are not embeddable and thus they are in non-embeddable regions. The other pixels are embeddable.

Step 2: The 2×2 block is as shown in fig. 1.

Step 3: The absolute difference of the neighbouring pixels is calculated as:

$$d=|c-a| + |b-a| \qquad (7)$$

Step 4: The predicted value is found using (1).

Step 5: Now to increase the security we go for random traversing. The knight's tour is used for this purpose. It is very effective methodology as it works as the knight moves on chess board. It moves 2n steps in horizontal and 1 in vertical or 2 in vertical and 1 in horizontal. This gives us 'L' shaped movement and it becomes difficult to find the correct order. This can be seen from fig.1 and table 1.

Step 6: After random traversing we go for LSB substitution were the secret data is embedded in the image. The embedding is done using (4). Thus the stego-image is generated.

3.2 Extraction Algorithm:

When the receiver obtains the stego image and the threshold T, the embedded data m can be extracted and the original pixel can be recovered by the procedure of extraction and recovery

Step 1: The cover image is divided into two regions in the same way as the embedding procedure.

Step 2: The absolute difference d' of the neighbouring pixels is calculated from (7)

Step 3: Now we do the LSB de-substitution using (5).

Step 4: Now the original image pixel values are found by subtracting the secret data from stego-pixels. Thus we get the original cover image which can be re-used for further data transmission.

IV. RESULTS AND DISCUSSIONS

In this paper, we generated a stego-image using PE expansion method and using LSB substitution with increased security of the hidden data because of the use of knight's tour random traversing methodology. We selected some five gray scale images as test images namely Lena, Boats, Barbara, Gold-hill, and Peppers. The PSNR (equation (6)) was used to check the quality of the stego image. Along with that to check whether the reversibility is attained or not, PSNR values were calculated between the original cover image and the cover image after extraction. Fig. 4 shows the comparison of cover image, stego image and the cover image after extraction for the Barbara image. The table 2 shows the variation of PSNR with threshold for the first method i.e. PE expansion method for Barbara image. The table 3 shows the result of method 2 i.e. LSB substitution method. The similar results were obtained for the remaining four gray scale images.



(a) (b) (c)

Fig. 4 Barbara (a) cover image, (b) stego-image, (c) cover image after extraction

Table 2, Method 1: PE expansion method PSNR v/s Threshold

PSNR	THRESHOLD	Images				
		Lena	Barbara	Boats	Gold-hill	Peppers
PSNR1	0	51.13	51.14	51.15	51.14	51.13
PSNR2		51.13	51.14	51.15	51.14	51.13
PSNR1	4	38.67	41.94	43.50	40.89	43.8
PSNR2		35.87	38.43	40.18	38.19	40.45
PSNR1	8	33.59	36.72	38.97	35.37	40.53
PSNR2		30.25	32.66	35.24	31.84	37.07
PSNR1	12	31.19	34.80	36.53	32.65	38.75
PSNR2		27.55	29.91	32.84	28.9	35.29
PSNR1	16	29.72	32.36	35.03	31.04	37.43
PSNR2		25.96	28.32	31.43	27.42	34.03

Table 3, Method 2: LSB substitution method; PSNR v/s Threshold

PSNR	THRESHOLD	Images				
		Lena	Barbara	Boats	Gold-hill	Peppers
PSNR1	0	51.14	51.13	49.17	50.95	49.94
PSNR2		51.14	51.14	49.54	51.44	50.16
PSNR1	4	44.85	47.4	47.27	46.54	48.11
PSNR2		44.85	47.36	47.53	46.69	48.31
PSNR1	8	40.41	43.3	44.73	41.99	46.34
PSNR2		40.42	43.25	44.86	42.01	46.5
PSNR1	12	38.06	40.89	42.86	39.47	45.04
PSNR2		38.06	40.85	42.94	39.48	45.16
PSNR1	16	36.67	39.24	41.58	37.93	43.98
PSNR2		36.67	39.21	41.64	37.93	44.08

V. CONCLUSION

In this paper, we propose a reversible data hiding scheme based on two methods, one being PE expansion and the other being LSB technique (with increased security of data because of random traversing methodology Knight’s tour). To increase the hiding capacity we can increase the number of bits embedded but it will reduce the quality of the image. The proposed scheme has higher hiding capacity and better image quality than that of the recently proposed schemes. We conclude that the LSB substitution method has better PSNR values compared to PE expansion method. Also with increase in threshold the PSNR value degrades. But the advantage of the PE expansion method over LSB substitution method is that on increasing the number of bits the PSNR values are not much affected whereas in LSB substitution method, with increase in number of bits PSNR decreases. Thus we prefer PE expansion method over LSB substitution method.

REFERENCES

[1] Chu YH, Chang S. Dynamical cryptography based on synchronized chaotic systems. IEE Electronics Letters 1999;35(12):974–5.

[2] Highland HJ. Data encryption: a non-mathematical approach. Computers and Security1997;16(5):369–86.

[3] Zhang X, Wang S. Efficient steganographic embedding by exploiting modification direction. IEEE Communication Letters 2006;10(11):781–3.

[4] Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Pattern Recognition 2004;37(3):469–74.

[5] Li YC, Yeh CM, Chang CC. Data hiding based on the similarity between neighbouring pixels with reversibility. Digital Signal Processing 2009;20(4):1116–28.

[6] Hong W, Chen TS, Shiu CW. Reversible data hiding for high quality images using modification of prediction errors. Journal of Systems and Software 2009;82(11):1833–42.

[7] Ni Z, Shi YQ, Ansari N, Su W. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology 2006;16(3):354–62.

[8] Yu-Chiang Li , Chia-Ming Yeh , Chin-Chen Chang. Data hiding based on the similarity between neighbouring pixels with reversibility. Digital Signal Processing, 2010; 20:1116-28.

[9] Hsien-Chu, Yen-Ping chu, Hung-Reuj Chen. A high capacity reversible data hiding scheme with edge prediction and difference expansion. Journal of Systems and Software 2009; 82(12)1966-73.

[10] Tian J. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology 003; 13(8):8906.

[11] Alattar AM. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing 2004;13(8):1147–56.

[12] Thodi DM, Rodriguez JJ. Expansion embedding techniques for reversible watermarking. IEEE Transactions on Image Processing 2007;16(3):721–30.

[13] Jin HL, Fujiyoshi M, Kiya H. Lossless data hiding in the spatial domain for High quality images. IEICE Transactions on Fundamentals of Electronics,Communications and Computer Sciences 2007;E90-A(4):771–7.

[14] Chuan-Quin, Chin-Chen Chang, An adaptive prediction-error expansion oriented reversible information hiding scheme. Pattern Recognition, 2012.

[15] Thanikaiselvan V, Arulmozhivarman P, Rengarajan Amirtharajan, John Bosco Balaguru Rayappan. Horse Riding & Hiding in Image for Data Guarding. Procedia Engineering 2012;30(1):36 – 44.