Int. J. Chem. Sci.: 14(S3), 2016, 747-752
ISSN 0972-768X
www.sadgurupublications.com

PVD BASED RANDOM DATA HIDING WITH HIGH PAYLOAD AND PSNR

V. THANIKAISELVAN[a*], S. SUBASHANTHINI[b] and S. RENUGADEVI[a]

[a]School of Electronics Engineering, VIT University, VELLORE – 632014 (T.N.) INDIA
[b]School of Information Technology, VIT University, VELLORE – 632014 (T.N.) INDIA

ABSTRACT

Data hiding is the research about embedding secret information into a digital media. The proposed method is based on embedding unequal amounts of secret information using pixel complexity. In the proposed method, secret information is embedded in 2 × 2 embedding cells which were composed with randomized embedding units to reduce the falling-off-boundary problem and to eliminate sequential embedding. This paper designs a new quantization range table based on the perfect square number to decide the payload by the difference value between the consecutive pixels. Furthermore, the payload size maybe adjusted by reference tables and threshold value. New viewpoint can be put forward by alterations in the existing Pixel Value Differencing methods to obtain better image quantity and higher capacity.

Key words: Information security, Steganography, Pixel value differencing, Data hiding.

INTRODUCTION

In any communication, security is the most important task. With the advancement of technology and the wide use of World Wide Web for communication increase the challenges of security. In this context, to provide the security two techniques has been used widely, Cryptography and Steganography[1]. Cryptography is used to scramble the information, deals with changing the meaning and appearance of message. To improve these limitations and to reduce the issues of cryptographic methods[2], an alternative mechanism, the steganography has its use widely. The Steganography technique[3] embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion in some cases; sending encrypted information may draw attention, while invisible information will not. Data hiding in an image can be done in spatial domain and transform[4,5] domain of the image. Simple Least Significant Bit Substitution is a common method used in both domains[4]. In Spatial domain, PVD[6-8] is a good performing method.

*Author for correspondence; E-mail: thanikaiselvan@vit.ac.in

A new and efficient steganographic method[9] for embedding secret messages into a gray-valued cover image is proposed. A cover image is partitioned into non-overlapping blocks of two consecutive pixels for the process of embedding a secret message. A difference value is calculated from the values of the two pixels in each block. An idea of a new image steganographic technique[10] capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye. In addition, our new method avoids the falling-off-boundary problem by using pixel-value differencing and the modulus function. A new adaptive least-significant- bit (LSB) steganographic[11,12] method using pixel-value differencing (PVD) that provided a larger embedding capacity and imperceptible stego images.

Proposed method

Embedding algorithm

Step 1: Two Reference Tables, RTl and RTu, are generated from ‘l’ and ‘u’ values, respectively.

The values in reference table R are randomly generated. Assume that pair pixel are to be embedded with k bits of secret information, and the corresponding reference table RT has to be filled with integers within the range [0 v-1], where v=(2^k). First, create a block of size n × m or n × n with integers [0 (2^k)-1] randomly filled, where n × m or n × n = 2^k. Next, the block is expanded by repeated concatenation until it becomes a 256 × 256 reference table. Assuming k = 4 bits of secret information to be embedded (hence, v=16). The 4 × 4 block is illustrated in Fig. 1(a) where the number elements are random and concatenated into a 256 × 256 reference table as in Fig. 1(b). The random orientation of the table increases the difficulty for the unauthorized person to guess and retrieve.

a

6	12	9	5
4	7	2	15
8	3	10	13
14	0	1	11

b

	0	1	2	3	4	5	6	7	..	254	255
0	6	12	9	5	6	12	9	5		9	5
1	4	7	2	15	4	7	2	15		2	15
2	8	3	10	13	8	3	10	13		10	13
3	14	0	1	11	14	0	1	11		1	11
4	6	12	9	5	6	12	9	5		9	5
5	4	7	2	15	4	7	2	15		2	15
6	8	3	10	13	8	3	10	13		10	13
7	14	0	1	11	14	0	1	11		1	11
:											
254	8	3	10	13	8	3	10	13		10	13
255	14	0	1	11	14	0	1	11		1	11

Fig. 1: (a) 4 × 4 block, and (b) 256 × 256 reference table

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

Fig. 2: Random seed

Step 2: The Cover image is partitioned into blocks of 2 x 2 and random seed is taken for each block to assign (Pivot Embedding Unit) PEU and NPEU (Non-Pivot Embedding Unit).

Step 3: Then these 2 × 2 cells are grouped in order to make 8 rows and 8 columns of each cell. So that 8 × 8 blocks of 2 × 2 cells are obtained.

Step 4: Those cells will be numbered randomly from 1 to 64 using pseudo random numbers. The pseudo random number generation can be done using the following equation.

$$X_n = [((a^*X_{n-1}) + c) \text{ modulus } (64) + 1]$$

Where, a is a multiplier and its value may be between 0 to 64, Xo is treated as an initial seed to be taken whose value range is $0 \leq Xo < 64$ and c is a constant adder value whose value may lie in the same range as the initial seed value. (a = 13), c = 5, x0 = 1.

According to the number generated by the pseudo random generator, numbers are allotted to these cells and hence will be accessed randomly. An example of which is given Fig. 2.

Step 5: The absolute value of the difference (di) between both PEUs is taken. This leads to emergence of β(Ci) (as shown in the equation below) value which determines number of bits to be embedded in PEUs. This is done by converting the above binary bits into decimal value (S).

$$B\ (Ci) = \begin{cases} l;\ d \leq To \\ u;\ d > To \end{cases}$$

Step 6: Depending on the 'To' Value, Reference table RTl or RTu will be referred.

Step 7: Taking the two PEUs as the coordinates of the Reference table, the decimal value (S) is searched in the vicinity of the element obtained by the coordinates.

Step 8: After finding the S value in RT, Check if the absolute value of the difference between the coordinates of the same satisfies the same β(Ci) Condition as the original PEUs.

Step 9: If the condition is not satisfied, search for the element is continued till the particular condition is satisfied.

Step 10: As the condition is satisfied, PEU values are replaced by the new coordinate value. NPEU follows the same Reference Table as the PEU of the same block. Embedding in NPEU is done in same fashion as that of PEU except for checking the β(Ci) condition for the new coordinate values.

Extraction algorithm

Exact reverse procedure of Embedding Algorithm will be followed for extracting the information.

RESULTS AND DISCUSSION

To evaluate the performance of our proposed method several experiments has been performed. Eight images are taken with size 512 × 512 as cover images which are shown. Our proposed method considers 2 × 2 non overlapping pixel blocks instead of two consecutive pixels, so the edge features may be considered sufficiently and the pixels in edge areas can endure much more changes without having perceptible distortion. A large text is taken as secret data, which is converted in digital format that is in ones and zeroes and they are embedded into cover image. To evaluate the quality of the stego image, peak signal to noise ratio (PSNR) is used, for each 512 x 512 image. The cover images taken and the stego images obtained by our proposed method with various values of l and u are tabulated in Table 1. Simulations were done for different values of l, u and threshold values. The results of proposed method are shown in the Table 1 with embedding capacity and PSNR values for different l and u values and threshold values of To=3, for different cover images.

Table 1: Result of the proposed method

To = 3	L=1 U=2			L=1 U=3			L=2 U=3		
	MSE	**PSNR**	**Payload**	**MSE**	**PSNR**	**Payload**	**MSE**	**PSNR**	**Payload**
Baboon	1.4986	46.4081	374205	3.9457	42.2035	486265	2.9431	43.4767	636349
Lena	1.7285	45.7882	339397	3.1987	43.1151	416649	1.9617	45.2384	601541

Cont…

To = 3	L=1 U=2			L=1 U=3			L=2 U=3		
	MSE	**PSNR**	**Payload**	**MSE**	**PSNR**	**Payload**	**MSE**	**PSNR**	**Payload**
Boat	1.604	46.1127	357837	3.5702	42.6379	453529	2.4612	44.2534	619981
Splash	1.8536	45.4846	320157	2.8265	43.6523	378169	1.4665	46.5019	582301
Pepper	1.667	45.9455	348385	3.3232	42.9492	434625	2.1507	44.839	610529
House	1.7853	45.6476	331013	3.1722	43.1512	399881	1.8848	45.412	593157
Aerial	1.5931	46.1425	359689	3.6248	42.5719	457233	2.528	44.137	621833
Plane	1.8553	45.4808	320149	2.9335	43.491	378153	1.5739	46.1951	582293

CONCLUSION

The proposed algorithm includes partition of cover image into cells of 2×2 embedding cells for embedding by random embedding arrangements with the help of random seed. Two reference tables were generated to increase the random embedding characteristic. The random mechanism increases security of the embedded data from human visual detection. The main contribution of the proposed method is that it offers high payload, i.e., a lot of information can be embedded in the cover image. The embedding arrangements of Pivot Embedding Units and Non Pivot Embedding Units of the embedding block were generated and the order of embedding in embedding 2×2 cells were randomly selected, so the order of embedding cannot be easily known by any unauthorized person. The value of the stego image is found to be very close to the values of the cover image and hence imperceptibility is maintained.

REFERENCES

1. A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, Digital Image Steganography: Survey and Analysis of Current Methods, Signal Processing, **90(3)**, 727-752 (2010).
2. A. Aarthie and R. Amirtharajan, Image Encryption: An Information Security Perceptive, J. Artificial Intelligence, **7(3)**, 123-135 (2014).
3. R. Amirtharajan and J. B. B. Rayappan, Steganography-Time to Time: A Review, Res. J. Information Technol., **5(2)**, 53-66 (2013).
4. V. Thanikaiselvan and P. Arulmozhivarman, RAND-STEG: An Integer Wavelet Transform Domain Digital Image Random Steganography using Knight's Tour, Security and Communication Networks, **8(13)**, 2374-2382 (2015).

5. V. Thanikaiselvan, P. Arulmozhivarman, R. Amirtharajan and J. B. Balaguru Rayappan, Wave (Let) Decide Choosy Pixel Embedding for Stego, Paper Presented at the 2011 International Conference on Computer, Commun. Electrical Technol., ICCCET, 157-162 (2011).

6. C. K. Chan and L. M. Cheng, Hiding Data in Images by Simple LSB Substitution, Pattern Recognition, **37**, 469-474 (2004).

7. V. Thanikaiselvan and P. Arulmozhivarman, Horse Communication Against Harsh Attack: A Stego Ride, Res. J. Information Technol., **5(3)**, 263-276 (2013).

8. V. Thanikaiselvan, P. Arulmozhivarman, R. Amirtharajan and J. B. B. Rayappan, Horse Riding & Hiding in Image for Data Guarding, Paper Presented at the Procedia Engineering, **30**, 36-44 (2012).

9. V. Thanikaiselvan, S. Subashanthini and R. Amirtharajan, PVD Based Steganography on Scrambled RGB Cover Images with Pixel Indicator, J. Artificial Intelligence, **7(2)**, 54-68 (2014).

10. D. C. Wu and W. H. Tsai, A Steganographic Method for Images by Pixel-Value Differencing, Pattern Recognition Letters, **24**, 1613-1626 (2003).

11. C. M. Wang, N. I. Wu, C. S. Tsai and M. S. Hwang, A High Quality Steganographic Method with Pixel Value Difference and Modulus Function, J. Syst. Softw., **81(1)**, 150-158 (2008).

12. C.-K. Chan and L. M. Cheng, Hiding Data in Images by Simple LSB Substitution, Elsevier J., Pattern Recognition, **37**, 469- 474 (2004).

13. C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun, Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems, IEEE Trans. Inf. Forensics Secur., **3(3)**, 488-497 (2008).

Accepted : 11.10.2016