A HIGH CAPACITIVE EMD TECHNIQUE FOR WET IMAGE

Parvinder SINGH[1], Mamta KALRA[2]
[1,2]Department of Computer Science & Engineering, DeenbandhuChhoturam University of Science & Technology
[1]parvinder23@rediffmail.com, [2]mamtakalra21@gmail.com

Keywords: Steganography, Exploiting Modification Direction (EMD), Stego image.

Abstract: *Exploiting Modification Direction (EMD) is a technique to hide secret data into digital images whereas wet paper coding is a technique for hiding data into specific pixels called dry pixels. In our scheme, we combined both the techniques. Before embedding, we classify image pixels into wet and dry pixels using location mapper that is shared between sender and receiver and then we embed secret data on each dry pixel using EMD technique. The experimental results show that our scheme provides high embedding capacity as compared to the earlier techniques.*

1. INTRODUCTION

Since the rise of internet secure data transmission has been a significant problem. The early approach was to secure communications is via data encryption. In data encryption, the content of the message is kept secret whereas sometimes the existence of message is also need to be kept secret. The technique used to implement this is called steganography. Steganography is a technique for hiding secret message into some other medium in such a way that no one can detect the existence of the hidden message. The word steganography is basically derived from two Greek words[1]: Steganos and Graphie, which means covered writing. Therefore steganography is a technique of hiding secret and confidential message in another media such that no one apart from the intended recipient can even detect the presence of the hidden message.

The main goal of the steganography is to hide messages inside other messages in such a way that it does not allow any eavesdroppers and attacker to even detect that there is a second secret message present inside that message [2-12].

One way for improving security of the Steganographic system is to reduce the amount of changes introduced in the cover object due to embedding secret data i.e. increasing the embedding efficiency of the Steganographic system. Various techniques were designed for this purpose. EMD(Exploiting Modification direction) is one those Steganographic techniques that leads to higher embedding efficiency as compared to other techniques such as run length encoding[13] and matrix encoding[14].

In 2006, Zhang et al in [15] proposed a technique that exploits the modification directions, called EMD technique. EMD is a method of steganography embedding in digital images in which each secret digit in (2n+1)-ary notational system is carried by n cover pixels and only one cover pixel is either increased by one or decreased by one or remain same. In general, for each group of n cover pixels there are 2n possible ways of alteration. These 2n ways of modification and one case in which no pixel is changed form (2n + 1) different values of a secret digit. The direction of modification of cover pixel is fully exploited that's why it achieves high embedding efficiency as compared to other techniques.

In WPC [24], all the image pixels are firstly classified into wet and dry pixels and the information is embedded only to the dry pixels. The idea of WPC came from the idea of a paper passing through the rain which results into some wet and some dry portions, and only dry portion of the paper can now be used for writing. Hence

only dry pixels of the image, which are called embeddable, can only be used for hiding secret and the wet pixels are called unembeddable. For defining wet and dry pixels, a location mapper is used and secret information is embedded only to the LSB of the dry pixels. Receiver extracts the hidden data from the same pixel locations by using the same location mapper that is pre-shared between sender and receiver.

Various modification of EMD have been proposed in [16-23]. In 2008, Byun et al [17] proposed an improved EMD technique that provides more embedding capacity for hiding secret data in cover image while maintaining the high PSNR value as compared to Zhang and Wang's[15] methods . In this paper, we combine the concept of high capacitive EMD and WPC together to define a new steganographic technique. In our proposed scheme a secret location mapper is used to define the wet and dry pixels of the image. The capacity of our proposed scheme is better than that of the scheme proposed by Chang et al [18]. And also for the same message length the PSNR value is better than Chang et al [18] scheme.

2. THE PROPOSED SCHEME

In the proposed scheme, WPC and EMD techniques are combined together. The extraction formula that is used for EMD is given as follows:

$$r = p_i + x\big(\mathrm{mod}(2n+1)\big) \qquad (1)$$

The embedding and extracting procedure for the proposed scheme is given as follows:

A. The Embedding procedure

Step 1. The cover image is divided into 2 categories of wet (unembeddable) and dry (embeddable) pixels using secret location mapper as shown in fig. 1.

Step 2. The secret data represented in a binary bitstream $b_1b_{2.....}b_N$ is converted into sequence of digits $d_1d_{2....}d_{N/3}$ in 8-ary notation.

Step 3. For i=1 to N/3 {Select a pixel from the image. If the pixel is classified as unembeddable then we ignore that pixel and move to the next pixel otherwise we apply extraction formula on that by using (1). If the resultant value r is same as secret digit d_i, then no change will be required. If both values are not same, then pixels value is changed with smallest distortion to make the resultant r to become equal to the secret digit d_i.}

19	10	19	10
21	17	21	17
21	11	20	13
18	18	21	20

(a) Cover image

19	10	19	10
21	17	21	17
21	11	20	13
18	18	21	20

(b) selection channel of (a)

Fig. 1 An example of wet and dry pixel classification

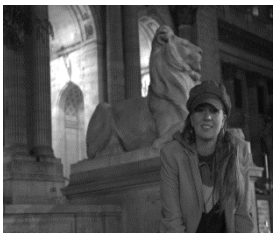
B. The Extracting procedure

Step 1. At receiver side, the stego image is divided into 2 groups of wet and dry pixels using the same location mapper that is pre shared between sender and receiver.

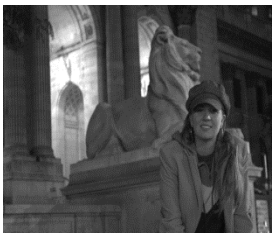
Step 2. For i=1 to N/3 {A pixel is selected from the stego image. If the pixel is wet then we ignore that pixel and select the next pixel. If the pixel is dry, then the secret digit d_i is obtained by applying the same extraction formula defined in (1).}

Step 3. The secret digits $d_1d_{2....}d_{N/3}$ are converted back from 8-ary notation to bitstream $b_1b_{2.....}b_N$ in order to obtain the secret data.

3. EXPERIMENTAL RESULTS



(a) Mandi (128×128)



(b) Mandi (256×256)

(c) Mandi (512×512)

Fig. 2 Three test images

(a) stego image
(32 kb)
Size=128×128
PSNR=49.7987

(b)stego image
(131 kb)
size=256×256
PSNR=49.8019

(c) stego image
(526 kb)
Size=512×512
PSNR=51.4470

Fig. 3 Stego images with different hiding capacities

For our experiment, we have taken three sized images as shown in fig. 2(a), 2(b) and 2(c) respectively. Different hiding capacities of these images are shown in fig. 3(a), 3(b) and 3(c) respectively. As the hiding capacity increases, visual quality of image decreases whereas the difference between cover images and stego images are not more that the changes in the stego-images are imperceptible to most users.

Table 1 shows the experimental results of hiding capacities of our proposed technique and the scheme proposed in [18]. From these results it is clear that our technique provides high embedding capacity as compare to the technique proposed in [18] while maintaining reasonable PSNR value.

Table 1. Comparison of hiding capacity (kb) of our scheme and Chang et al scheme [18]

Techniques	Images		
	Mandi (128×128)	Mandi (256×256)	Mandi (512×512)
	(kb)	(kb)	(kb)
proposed scheme	32	131	526
Scheme[18] (s =2)	15	60	241
Scheme[18] (s =3)	22	90	362
Scheme[18] (s =4)	30	120	482

Table 2 shows the experimental results of PSNR value for different capacities of data. From this table it is clear that as the hiding capacity increased, the visual quality of our proposed technique gets increased slightly than that of Chang's scheme [18].

Table 2. Comparison of PSNR valuedB) of our scheme and Chang et al scheme [18]

Hiding capacity	**proposed scheme**	**Scheme[18] (s=3)**
(kb)	(dB)	(dB)
90	57.4434	57.4592
128	55.9257	56.0060
192	54.2446	54.2165
256	52.9734	52.9507
362	51.4470	51.4310

4. CONCLUSION

From Table 1, we observe that the hiding capacity of our proposed technique is greater than that of the technique proposed by Chang et al in [18]. And from Table 2 it is also clear that our proposed technique provides reasonably good visual quality and the stego-images look like the cover images to the naked eye. The technique also provides security because attacker will not be able to extract the secret data without knowledge of the secret location mapper.

ACKNOWLEDGMENT

The work in this paper is funded by Major UGC Project **"**Development of a Model for Secured Communication".

REFERENCES

[1] Rengarajan Amirtharajan, John Bosco Balaguru Rayappan, "*An intelligent chaotic embedding approach to enhance stego-image quality*", Information Sciences 193, pp. 115–124, journal homepage: www.elsevier.com/locate/ins, 2012.

[2] Parvinder Singh, Sudhir Batra, H R Sharma, "*Message Hidden in 6th and 7th Bit*", Proceedings of International Conference on Controls, Automation and Communication System, Dec. 22-24, 2004, Allied Publishers, pp-281-284.

[3] Parvinder Singh, Sudhir Batra, HR Sharma, "*Message Hidden in 1st and 2nd Bit Plane*",

Proceedings of 9th WSEAS International Conference on Computers, Athens, Greece, July 14-16, 2005, pp 1-5.

[4] Prince Kumar Panjabi, Parvinder Singh, "*An Enhanced Data Hiding Approach using Pixel Mapping Method with Optimal Substitution Approach*", International Journal of Computer Applications, vol.74(10), July 2013, pp. 36-43.

[5] Parvinder Singh, Sudhir Batra, HR Sharma, "*Hiding Credentials in Biological Images*", A & B Research, vol 22(1), Jan 2006, ISSN 0970-1970, pp 22-25.

[6] Sonam Chhikara, Parvinder Singh, "S*BHCS: Spike based Histogram Comparison Steganalysis Technique*", International Journal of Computer Applications, vol.75, 2013.

[7] Parvinder Singh, Sudhir Batra, HR Sharma, "*A review of digital signatures and status in India*", WSEAS Transactions on Computers 4 (4), 408-410.

[8] Jasvinder Kaur, Manoj Duhan, Ashok Kumar, "*Digital Logic Embedding Using Single Row*", International Journal on Computer Science & Engineering, vol. 3, no. 12 , 2011.

[9] Sudhir Batra, Parvinder Singh, "*A Class of $ q $-ary 2-IPP Codes*", Journal of Informatics and Mathematical Sciences 5 (2), 65-76

[10] Parvinder Singh, Sudhir Batra, H R Sharma, "*Steganographic Methods Based on Digital Logic*", 6th International Conference on Signal Processing, Dallas, USA, March 22-24, 2007.

[11] Currie, D.L. & Irvine, C.E., "*Surmounting the effects of lossy compression on Steganography*", 19th National Information Systems Security Conference, 1996.

[12] Parvinder Singh, Sudhir Batra, HR Sharma, "*Evaluating the Performance of Message Hidden in 1st and 2nd Bit Plane*", WSEAS Transactions on Information Science and Applications, issue 8, vol 2, August 2005, pp 1220-1227.

[13] X. Zhang and S. Wang, "*Dynamically running coding in digital steganography*", IEEE Signal Processing Lett., vol. 13, no.3, pp. 165-168, Mar. 2006.

[14] Jasvinder Kaur, Manoj Duhan, Ashok Kumar, Raj Kumar Yadav, "*Matrix Matching Method for Secret Communication using Image Steganography*", Annals of Faculty Enginnering, Hunedoara, International Journal of Engineering, Tome X, Fascicule 3, pp. 45-48, 2012

[15] X. Zhang and S. Wang, "*Efficient Steganographic Embedding by Exploiting Modification Direction*", IEEE Communications Letters, vol. 10, no. 11, pp. 781-783, November 2006.

[16] Chin-Feng Lee, Yi-Ren Wang and Chin-Chen Chang, "*A steganography method with high capacity by improving Exploiting Modification Direction*", IIHMSP, Volume 1, pp.497 – 500, 2007.

[17] Jin-Yong Byun, Ki-Hyun Jung and Kee-Young Yoo, "*Improved Data Hiding Method by Exploiting Modification Direction*", International Symposium on Ubiquitous Multimedia Computing, pp. 264–266, 2008.

[18] Chin-Chen Chang, Zhi-Hui Wang, Yi-Hui Chen and Ming-Chu Li, "*A Wet Image Data Hiding Scheme Based on Coordinate Modifications*", Third International Symposium on Intelligent Information Technology Application, 2009.

[19] Duc, K., Chang, C. C., "*A steganographic scheme by fully exploiting modification directions*", Technique Report of Feng-Chia University.

[20] C. N. Shyi, S. H. Kuo and W. C. Kuo, "*Data Hiding Method Based on High Embedding Capacity by Improving Exploiting Modification Direction*", 2008 Conference on Global Logistic Management and Industry Practice Research. 25, pp.455-462, December 2008.

[21] Wen-Chung, Kuo Jiin-Chiou Cheng, Chun-Cheng Wang, "*More Efficient Steganoraphic Embedding and Capacity-Improvement by Generalized Exploiting Modification Direction Method*", Fourth International Conference on Innovative Computing, Information and Control, 2009.

[22] Hamzeh Hajizadeh, Ahmad Ayatollahi and Sattar Mirzakuchaki, "*A New High Capacity and EMD-based Image Steganography Scheme in Spatial Domain*", 2013.

[23] Kai Yung Lin, Wien Hong, Jeanne Chen, Tung Shou Chen, Wen Chin Chiang, "*Data Hiding by Exploiting Modification Direction Technique Using Optimal Pixel Grouping*", 2nd International Conference on Education Technology and Computer (ICETC), 2010.

[24] Fridrich, J., Goljan, M., Lisonek, P. and Soukal, D., "*Writing on wet paper*", IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3923-3935, 2005.