Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 4; April-June, 2015 pp. 347-350

http://www.krishisanskriti.org/acsit.html

A High Capacity Reversible Data Hiding Scheme: A Case Study

Jibi G Thanikkal[1], Jinu G Thanikkal[2] and Mohammad Danish[3]

[1,3]Department of Computer Science & Engineering Al-Falah University, Dhauj, Faridabad
[2]Department of Computer Science & Engineering Royal College of Engineering and Technology Akkikavu, Thrissur, Kerala
E-mail: 1jibimary@gmail.com

Abstract—*The advancement in IT sector escalated the capacity of information transmission and the need for the safety of data being transferred. Steganography is the art of masking the sensitive data in any cover media. Data hiding is an embedding method that conceals messages into digital media to convey the message secretly, and is classified into non-reversible and reversible. Reversible data hiding technique not only embeds data into cover images, but also restores the original images from the stego-images after the embedded data have been extracted. Location map was used in this scheme to store the location information of all selected cover image pixels. The proposed scheme achieved high capacity with the help of location map. RDH has the capability to erase the distortion introduced by embedding step after cover restoration. The complexity of our proposed scheme is low and the execution time is short. RDH is capable of restoring the original image at the data extracting stage; therefore, the embedding methods of this type are useful in the field of military or law enforcement, where the original images are demanded.*

Keyword: *Steganography, XOR, cover image, Secret data, PSNR.*

1. INTRODUCTION

The advancement in the field of Information and Communication sector along with rapid development in internet usage escalated the capacity of information transmission. This also has lead to a new era of research in the field of information security. Many a times, crackers are in news for exploring the secret information. Hence it was important to secure the data from being stolen or illegally altered or to keep secrecy while transferring. The secrecy of data can be achieved through cryptography and steganography [1]. Cryptography provides encryption of data into another format where the sender and receiver only can able to understand the actual meaning of it. Steganography is the art of masking the sensitive data in any cover media. Steganography together with cryptography is found to provide high security in data transfer [1,2].

Data hiding is an embedding method that conceals messages into digital media to convey the message secretly [3]. Data hiding methods can be classified into non-reversible [4,5] and reversible [6-8]. Non-reversible methods generally provide higher payload and better image quality than those of reversible methods, and therefore, have many applications, such as image authentication [9] and tamper detection [10]. Reversible data hiding technique not only embeds data into cover images, but also restores the original images from the stego-images after the embedded data have been extracted [11]. RDH is capable of restoring the original image at the data extracting stage; therefore, the embedding methods of this type are useful at some applications such as military or law enforcement, where the original images are demanded [12]. Reversible data hiding involves selection of cover medium which can completely hold the data, and a function to fix the secret message in cover medium and retrieve the message and original cover medium at the receiver side.

Several researchers [6-8,13,14] proposed lossless data hiding techniques to provide solutions for completely restoring the original host medium. Tian [6] explored the redundancy in the host images and developed a high capacity/ low distortion loss less data hiding technique using the difference expansion. Alattar [11] used the generalized difference expansion of an arbitrary size instead of pairs and presented a reversible hiding scheme. Lin *et al*. [15] took advantage of the block difference histogram of a host medium to develop a reversible data hiding scheme. A simple lossless data hiding method based on the coefficient-bias algorithm by embedding bits in both spatial domain and frequency domain is also been proposed [7].

Recent research proposed novel ideas in the RDH techniques. Zhang *et al*. [8] showed higher efficiency in RDH based on lossless compression of encrypted data. High capacity RDH with limited distortion was proposed based on generalization predictions-error expansion and adaptive embedding strategy [16]. High performance in RDH was also obtained by: SMVQ and locally adaptive coding scheme [17]; index mapping mechanism [14]; block median presentation and modification of prediction errors [18]; LSW [19]; combining compression, data hiding and partial encryption of image in a single processing step [20], etc. The RDH schemes conducted in spatial domain achieved a high payload size. There are also

arguments that schemes embed bits in spatial domain are vulnerable to manipulations [7]. Hidden data is incapable of being extracted if even a slight alteration was imposed to the marked images. To provide a larger hiding capacity with a better robust performance, bit embedding in both spatial and frequency domain are also proposed by various researchers.

In this paper, we propose a novel high performance reversible data hiding scheme that can embed high capacity of secret bits and recover image after data extraction. This new scheme is based on XOR algorithm. It can embed more data than many of the existing reversible data hiding algorithms. With the reversibility nature of XOR operation the original message data was restored. Location map was used in this scheme to store the location information of all selected cover image pixels.

2. THE PROPOSED SCHEME AND ALGORITHM

XOR is a logical operation, pronounced *Exclusive OR.* It yields true if exactly one (but not both) of two conditions is true. For multiple arguments, XOR is defined to be true if an odd number of its arguments are true, and false otherwise. The proposed method can be explained in a simpler manner. Let, P (pixel) and M (message) are two binary numbers, then XOR (P, M) is the exclusive-or operation of the two binary numbers, i.e., if P=1 and M=1, then L (location map) = XOR (P, M) = 0. In this method, we utilize the reversibility nature of XOR operation. Let us apply this peculiarity in the above analysis, i.e. if L= XOR (P, M) = 0, then M=XOR (P, L) =1 and P=XOR (L, M) =1. This property of XOR is utilized in the proposed scheme. If we apply this in experimental set up, inserting one bit message M into least significant bit (LSB) of pixel P, location map L is marked as 1 if the LSB of P and M are different, otherwise L is marked as 0.

The above operation will provide the result of the location map, and based on XOR, result on LSB of P and M, decision for the embedding at LSB of image pixel will be taken. If the location map is 0, it indicate that the LSB bit of P and M are same and the pixel remains without getting edited, else otherwise. Image name, secret message, result image name are the inputs to the embedding algorithm. XOR operations for the data hiding are given in table 1& 2. Table 1 represents the embedding process and Table 2 represents the extraction process employed in the proposed scheme using XOR.

In the present study, all the experiments are performed in actual bit stream. At the sender side, gray scale image is converted to 8 bit pixel array. Location map array is generated to store the location information of editable position of pixel values. In the receiver side, to retrieve message data, LSB of image pixels are extracted. And to retrieve the original image back, the XOR operation is performed between each of the LSB of image pixels with location map bit.

Table 1: XOR operations for the embedding process.

Input		Output	
LSB of pixel	**Message bit**	**Location map**	**LSB of embedded pixel**
0	0	0	0
0	1	1	1
1	1	0	1
1	0	1	0

Table 2: XOR operations for the extraction process

Input Values		Result	
LSB of Pixel	**Location Map**	**Message Bit**	**LSB of Original Pixel**
0	0	0	0
1	1	1	0
1	0	1	1
0	1	0	1

3. EXPERIMENTAL RESULT AND DISCUSSION

In the current experimental setup, four 8-bit gray images are used (Table 3). The pure payload and location map length are used to calculate amount of payload after improvement. Peak Signal to Noise Ratios (PSNR) are calculated to verify the efficiency of the proposed scheme. The PSNR measure the difference between cover image and embedded image. PSNR is calculated as per the following equation (1).

$$PSNR = 10 \log_{10} \frac{2552 \ldots\ldots}{MSE} \qquad \ldots\ldots(1)$$

Fig. 1 represents examples of bit embedding (in spatial domain) using XOR algorithm. This Fig. illustrates the case of 8-bit embedding with a bit stream of 11001011. Fig. 2 represents retrieval of 8 bit secret data from the embedded image at the received end. From the Fig. 2, it can be seen that, the present scheme using XOR algorithm can not only embed the secret data/information, but also retrieve the data/information at receiver end without making any change in the cover image. It is known that, location map may significantly affect the embedding performance of RDH [16]. In the present study, the size of the location map is similar to the size of the message data and hence high performance of RDH is achieved with the proposed scheme.

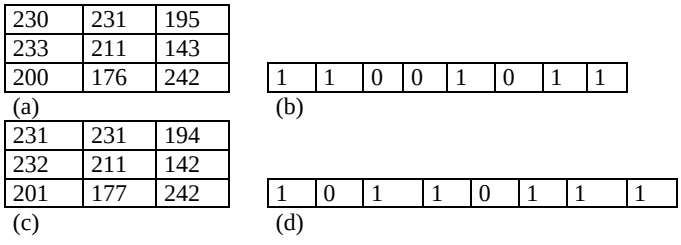


Fig. 1: Example of bit embedding (a-Cover image, b-message data, c-embedded image, d-location map).

231	231	194
232	211	142
201	177	242

(a)

1	0	1	1	0	1	1	1

(b)

230	231	195
233	211	143
200	176	242

(c)

1	1	0	0	1	0	1	1

(d)

Fig. 2: Example of data extraction and reversibility (a- embedded image b-location map, c- Cover image, d- message data).

Table 3 provides the embedded pay load size and the PSNR of embedded image. The present study using XOR algorithm attained a PSNR of 49 dB. Tian [6] could achieve PSNR of 44 dB. Gui *et al*. [16] achieved average PSNR of 40.53 dB. Tian [6] used difference expansion algorithm and the redundancy in the digital content to achieve reversibility. Whereas, Gui *et al*. [16] used generalization predictions-error expansion and adaptive embedding strategy and attained high capacity RDH with limited distortion. The trade-off between PSNR and payload for the proposed method using various images in the spatial domain is drawn in Fig. 3. Fig. 3 indicates that the average PSNR is about 46.5 dB under a payload of 36000. On the other hand, the average of 48.5 PSNR is achieved at payload 18000.

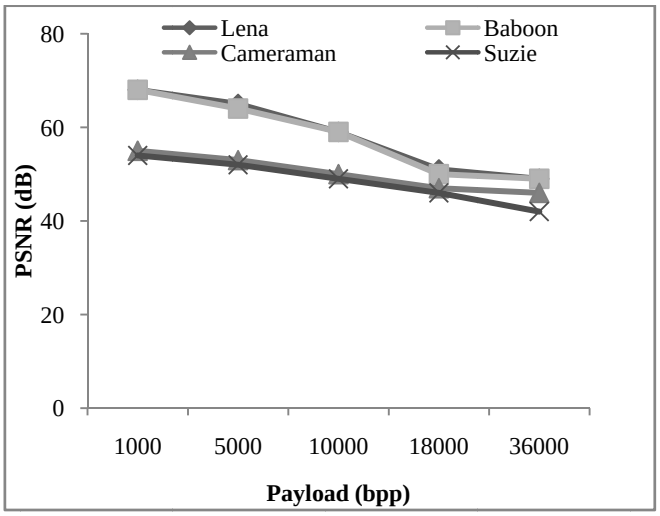


Fig. 3: The PSNR and payload performance generated by the proposed method in the spatial domain

Our algorithm can embed 1/8 bit of the cover image (width x height). Multilayer embedding is also possible by extending the algorithm. The proposed system employ location map similar to the message bits array, and this schemes is also simpler compared to the other reversible data hiding algorithms in spatial domain [6,21].

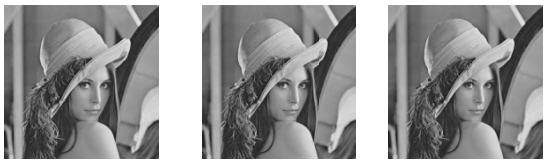
Table 3: Embedded payload size vs PSNR of embedded image.

Image and Size	PSNR at Payloads				
	36000	**18000**	**10000**	**5000**	**1000**
 Lena (512x512)	49	51	59	65	68
 Baboon (512x512)	49	50	59	64	68
 Cameraman (256x256)	46	47	50	53	55
 Suzie (240x351)	42	46	49	52	54

4. COMPUTATIONAL COMPLEXITY

The computational complexity of the proposed system is very low. All the operations are performed in the spatial domain. The required process mainly lies on generating the image pixels and determine the exclusive result between the LSB of image pixel and the message bits. Hence, the execution time of the algorithm is very short. It can be explained as, if the cover image has height M and width N, for the embedding process, it is required to scan the image only once and hence the computational complexity is O (MN). Similarly for the extraction process computational complexity is O (MN).

Fig. 4 illustrates the comparison between cover, embedded and extracted images of Lena. There is no perceptional LSB bit change in the embedded image. The original image is extracted at the receiver side with PSNR value 100.



Cover Image **Embedded Image** **Extracted Image**

Fig. 4: Different facets of Lena image.

5. CONCLUSION

The proposed reversible data hiding scheme using XOR algorithm achieved very high performance. The system shows high capacity compared to other methods in spatial domain. The basic structure of the proposed schemes is explained in the present work. The capacity and security of the message data can be increased by adding compression, encryption, multilayer embedding, etc. The experimental result shows that the proposed system can retrieve more than 49db PSNR for 512x512 images. The PSNR obtained in the current schemes is higher than that of reversible data hiding techniques proposed by many researchers. The proposed system is also applicable to all types of images. Furthermore this embedding and extraction system is simple and execution time is very

short and therefore, the overall performance is better than other steganography techniques. The proposed schemes can very well utilized in medical, scientific, and other fields where the need of original image is required.

REFERENCES

[1] Stallings, W., 2003. Cryptography and Network Security-principles and practices. Pearson Education, Inc.

[2] Singh, A., S.Malik, 2013. Securing Data by Using Cryptography with Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5): 404-409.

[3] Provos, N., P.Honeyman, 2003. Hide and seek: an introduction to steganography. IEEE Security and Privacy, 1(3): 32-44.

[4] Mielikainen, J, 2006. LSB matching revisited. IEEE Signal Process. Lett. 13(5): 285-287.

[5] Zhang, X., S.Wang, 2006. Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters, 10(11): 781-783.

[6] Tian, J, 2003. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, 13(8): 890-896.

[7] Yanga, C. Y., W.C.Hua, C.H.Linb, 2010. Reversible Data Hiding by Coefficient-bias Algorithm. Journal of Information Hiding and Multimedia. Signal Processing, 1(2):91-100.

[8] Zhang, X., Z.Qian, G. Feng, Y. Ren, 2014.Efficient reversible data hiding in encrypted images. Journal of Visual Communication and Image Representation, 25(2): 322-328.

[9] Chen, Y.S., R.Z.Wang, 2011. Reversible authentication and cross-recovery of images using (*t*,*n*)-threshold and modified-RCM watermarking. Optics Communications, 284(12):2711-2719.

[10] Hsu, S.F., Tu, 2010. Probability-based tampering detection scheme for digital images. Optical Communications, 283(9): 1737-1743.

[11] Alattar, A.M, 2004. Reversible watermark using difference expansion of quads, in: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, 3:377-380.

[12] Hong, W, 2012. Adaptive reversible data hiding method based on error energy control and histogram shifting. Optics Communications, 285: 101-108.

[13] Wang, K., Q.Liu, L.Chen, 2012. Hierarchical reversible data hiding based on statistical information: Preventing embedding unbalance. Signal Processing. 92 (12): 2888-2900.

[14] Qin, C., C.C.Chang, Y.C.Chen, 2013. Efficient reversible data hiding for VQ-compressed images based on index mapping mechanism. Signal Processing, 93(9): 2687-2695.

[15] Lin, C.C., N.L.Hsueh, W.H.Shen, 2007. High-performance reversible data hiding. Fundamenta Informatica, 82: 155-169.

[16] Gui, X., X.Li, B.Yang, 2014. A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding. Signal Processing, 98: 370-380.

[17] Wang,L., Z. Pan, X. Ma, S. Hu, 2014. A novel high-performance reversible data hiding scheme using SMVQ and improved locally adaptive coding method. Journal of Visual Communication and Image Representation, 25(2): 454-465.

[18] Leung,H.Y., L.M.Cheng, F.Liu, Q.K.Fu, 2013. Adaptive reversible data hiding based on block median preservation and modification of prediction errors. Journal of Systems and Software, 86(8): 2204-2219.

[19] Wang,Z.H., H.R.Yang, T.F. Cheng, C.C.Chang, 2013.A high-performance reversible data-hiding scheme for LZW codes. Journal of Systems and Software, 86(11): 2771-2778.

[20] Puech, W., J.M.Rodrigues, J.E.D.Morice, 2007. A new fast reversible method for image safe transfer. Journal of Real-Time Image Processing, 2(1): 55-65.

[21] Yang, C.Y., W.C.Hu, 2010. Reversible Data Hiding in the Spatial and Frequency Domains. International Journal of Image Processing, 3(6): 373-382.