LOSSLESS DATA HIDING SCHEME BASED ON LSB MATCHING

Xiaomei Quan and Hongbin Zhang
College of Computer Science, Beijing University of Technology
Chaoyang District, Beijing, China
xmquan@bjut.edu.cn, zhanghb@bjut.edu.cn

ABSTRACT

In this paper, a simple reversible least-significant-bit (LSB) matching algorithm, which can completely recover the host images without any distortion from the stego images by utilizing the parity features of the host images and defining two embedding pairs. It embeds hidden message via LSB matching instead of LSB replacement, which makes it immune to steganalytical attacks utilizing the imbalance introduced by the LSB replacement. Multiple layer embedding is also allowed for the proposed method, and it won't decrease the PSNR of the stego images. The average PSNR of the stego images generated by the proposed method is 51.14dB. Experimental results show the proposed algorithm has better performance than existing reversible LSB modification in terms of distortion, visual quality, capacity as well as resistance against existing steganalytic detectors.

KEYWORDS

Data hiding, stegnography, least significant bit modification

1 INTRODUCATION

Data hiding in digital image is a technique to embed messages into host image imperceptibly. By dwelling in the hidden message, the data hiding schemes always induce some changes into the host image, resulting in the inevitable distortions to the host image. For most existing data hiding methods, the distortions cannot be recovered after the hidden message extraction. Although it is fine for majority of the data hiding applications, it cannot fit in the scenarios in which preserving the exact fidelity of the host image is a legal or technical requirement, which encourages the development of reversible data hiding techniques. Reversible data hiding, also known as lossless, or invertible data hiding, can recover the host images along with the extraction of the hidden messages. Some reversible data hiding schemes have already been proposed. One typical class of reversible data hiding methods select the host image features, usually the least significant bits (LSB) of the host images, and compress them as part of the embedded payload to create space for the hidden message. By employing the LSB replacement, the payload is embedded. After the payload extraction, the original features and the host image can be restored [1,2,3]. Recently, Tian [4] proposed the difference-expansion (DE) method. The DE, as well as the DE-based approaches [5,6] use an integer transform to decorrelate the image to create features, namely, the difference of the adjacent pixel values or the prediction error. By expanding these features the messages are embedded.

In order to control the induced distortion to maintain a good visual quality, many of the above algorithms [1-4] actually overwrite, or replace the LSBs of the host image to embed message bits. During the modification, the increment operation is always done on the even host pixels while the decrement on the odd ones. However, this asymmetric nature of the LSB replacement makes them very vulnerable to many detectors [7,8,9]. To avoid this inherent drawback of the LSB replacement, LSB matching is proposed [10]. It only differs from the LSB replacement in the encoding process, when the message bit doesn't match the LSB of the host image, the LSB matching either add or subtract 1 from the host pixel value randomly. Nevertheless, to the best of

our knowledge, such an attempt to develop a reversible data hiding scheme using LSB matching has not been made yet. In this paper, a reversible data hiding scheme based on LSB matching is proposed. It uses the parity features of the LSBs of the host image to embed messages as well as to recover the host pixels. Through multiple-layer embedding, the proposed method can achieve a large payload while maintaining high visual quality. Moreover, the symmetric nature of the LSB matching makes the proposed method more robust than most existing reversible data hiding methods against the steganalytical detectors. The complexity of the proposed scheme is quite low. The average peak signal-to-noise ratio (PSNR) of the stego images generated by the proposed method is 51.14dB.

The rest of the paper is organized as follows. The proposed algorithm and its characteristics are described in Section 2. Experimental results and comparisons are presented in Section 3. Section 4 concludes this paper.

2 PROPOSED ALGORITHM

2.1 Data-embedding Algorithm

The host signal is gray-scale image in this work. But the algorithm can also be applied to other media, such as audio and video. In LSB matching, only when the embedded bit doesn't matches the LSB of the host image pixel value, changes, adding or subtracting one, occur. In other words, if the message bit is one, only the even pixel value should be changed, and vice versa. Therefore if the parity information of the host pixel is available when the message bit is extracted, whether the host pixel value was changed or not is known to the decoder. This information will help the exact recovery of the host image. Consequently, in the proposed scheme the parity information of the host pixels is losslessly compressed as *P*. the whole payload embedded into the host image is denoted as *B*, which is composed of *P* and message bitstream *M*

$$B = P \cup M = b_1 b_2 ... b_l$$

where $l \le m \times n$, and the size of the host image is $m \times n$.

To further decide the increment or decrement operation in the encoding process, two subsets of the host image pixels and two corresponding embedding pairs are formulated as the following:

Divide the host image pixels into two equal subsets, *A* and *B*, according to a secret key *K* shared with the encoder and decoder. For subset *A*, the embedding pair is defined as $(2k,2k+1)$, while for subset *B*, the embedding pair is defined as $(2k-1,2k)$.

The embedding pair defined here is to indicate how to embed the message bit, i.e., to carry out the increment or decrement operations.

In the embedding process, if the message bit doesn't match the LSB of the pixel value of the host image, then in subset *A*, the odd pixel value $2k+1$ is subtracted by one and the even pixel value $2k$ is added by one, while in subset *B* the odd pixel value $2k-1$ is added by one and the even pixel value $2k$ is subtracted by one. In this way, the imbalance of the LSB replacement is avoided.

Suppose the embedded bit is b, the host pixel value is x, and the stego pixel value is y. The embedding algorithm is proposed as follows:

If $b = LSB(x)$.
  else if $b = 1$ (host pixel value belongs to the even-valued region)
    if $x \in A$ (the embedding pair is $(2k,2k+1)$)
      $y = x + 1$
    else ($x \in B$, the embedding pair is $(2k-1,2k)$)
      $y = x - 1$
    end
  else ($b = 0$, host pixel value belongs to the odd-valued region)
    if $x \in A$ (the embedding pair $(2k,2k+1)$)
      $y = x - 1$
    else ($x \in B$)

$y = x + 1$

end

end

end

2.2 Data-extracting and Host Image Recovery Algorithm

The hidden payload bitstream *B* is retrieved by collecting all the LSBs of the host image pixels in the same order as in the embedding process. First, the compressed parity information *P* and the embedded message *M* are divided. This division can either based on the end of the message symbol of *P*, or the predefined length of *P*. After the division, the hidden message is decoded. Second, with the help of the decompressed parity information and the shared secret *K*, the host image can be perfectly recovered. The host image recovery algorithm is as follows.

If $LSB(y) = 1$

If the parity information for *y* is even

If $y \in A$

$x = y - 1$

else

$x = y + 1$

end

else

$x = y$

end

else

if the parity information for *y* is odd

If $y \in A$

$x = y + 1$

else

$x = y - 1$

end

else

$x = y$

end

end

2.3Discussion

- Capacity: the maximum payload embedded into the host image is $l = m \times n$ bits, which is composed of the pure payload M and the compressed parity information bitstream P. So to employ an efficient lossless compression method for the parity information is crucial to the capacity of the pure payload *M*. Since the parity information of the host image is more like noise, the current binary image lossless compression methods, such as JBIG, LZW and MMR, are not effective. We adopted the improved CALIC lossless image compression method in [3] to compress the parity information.

Figure 1. One-layer embedded "Lena"(PSNR = 51.14dB)

Figure 2. Three-layer embedded "Lena" (PSNR = 51.15dB)

Table 1. Experimental results for some commonly used images

Images (512*512)	PSNR of the Stego Image (dB)		Pure Payload (bytes)	
	One-layer embedding	*Three-layer embedding*	*One-layer embedding*	*Three-layer embedding*
Lena	51.15	51.15	605	1821
Airplane	51.13	51.16	2154	5896
Baboon	51.14	51.15	78	234
Boat	51.13	51.10	612	1725
Barbara	51.16	51.13	540	1480
Goldhill	51.11	51.12	308	826

Figure 3. Five-layer embedded "Lena"(PSNR = 51.14dB)

- PSNR: to measure the visual quality of the stego images produced by the proposed method compared with the host images, PSNR is calculated in this paper. The proposed embedding algorithm uses the LSB matching to hide message, therefore when the LSB of the host image pixel doesn't match the message bit (The probability is 0.5), the absolute value of the difference between the stego image pixel and host image pixel is 1, otherwise the difference is 0. So the average mean square error (MSE) is:

$$MSE = \frac{1}{512 \times 512} \sum_{i=1}^{512} \sum_{j=1}^{512} (H(i,j) - S(i,j))^2 = 0.5 \qquad (1)$$

where H and S are host and stego images respectively.

The average PSNR is:

$$PSNR = 10 \log_{10} (\frac{255 \times 255}{MSE}) = 51.14dB \qquad (2)$$

This high average PSNR guarantees the good perceptibility of the proposed method, which is also supported by the extensive experimental results in Section 3.

- Multiple-layer Embedding: For large capacity, the proposed method allows multiple-layer embedding. The capacity limit of each layer is almost same, and it won't decrease gradually with the layer increased, as the case in DE method [4]. Because of the symmetric characteristic of the LSB matching, multiple-layer embedding won't decrease the redundancy in the LSBs of the pixel values. In this way, both large capacity and high visual quality are achieved.

- Response to the Steganalysis Detector: By applying LSB matching in the data embedding process, the proposed method doesn't induce the imbalance in the stego image pixels, as does in the LSB replacement.

Compared to the existing reversible data hiding methods, which use LSB replacement to embed message, the proposed method is more robust against most current LSB stegnalsysis detectors, which are based on the asymmetry induced by LSB replacement, such as improved RS and Pairs detectors [9]. Steganalysis detector response and comparisons are shown in Section 3.

3 EXPERIMENTAL RESULTS

One thousand gray-scale images (512*512*8) are used in our experiments, which covers different image types. The average PSNR of one-layer embedding for 1000 images are 51.1dB, which agrees with the theoretical analysis of PSNR in Section II. The average PSNR and pure payload of one-layer embedding and three-layer embedding for some commonly used images, including Lena, Airplane, etc., are presented in

Table I. The embedded “Lena” images with one layer, three-layer and five-layer are shown in Figs. 1, 2 and 3. From these experimental results, with multiple-layer embedding the proposed method can achieve large pure payload and maintain high visual quality simultaneously.

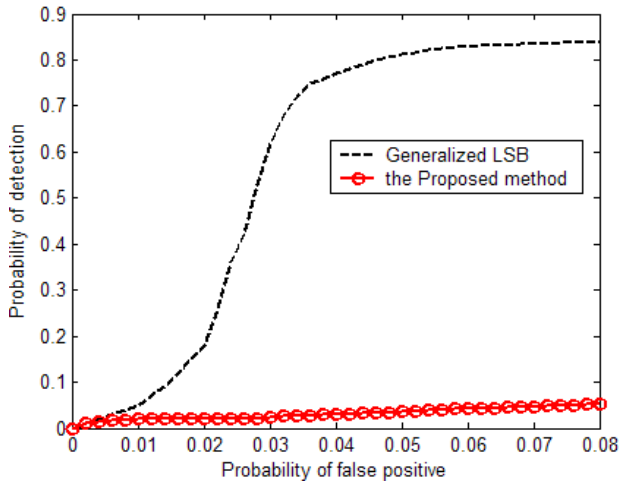

Figure 4. ROC curves for the improved Pairs.

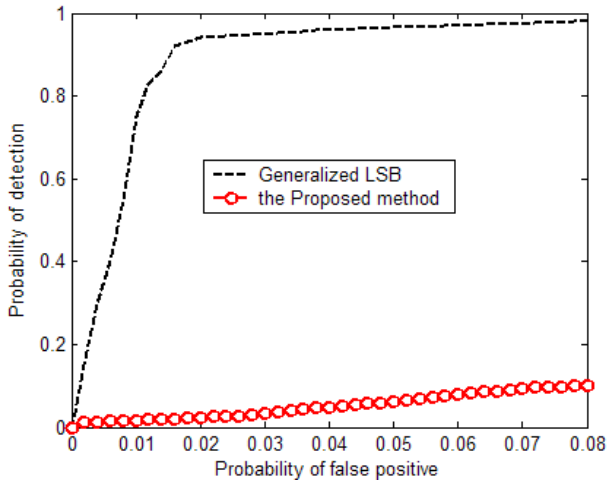

Figure 5. ROC curves for the improved RS

In order to test whether the proposed method introduces bias to the stego images as LSB replacement does, the absolute value of the sum of the average difference between stego and host images in both even and odd regions are computed. Both results are 0, which demonstrates the proposed method is unbiased. Figs.4 and 5 depict receiver operating characteristic (ROC) curves using improved RS and Pairs methods for message detection on the Generalized LSB, which uses LSB replacement to hide message, and the proposed method, respectively. The ROC curves clearly show the inefficiency of the improved RS and Pairs detectors to the proposed method.

4 CONCLUSIONS

A novel reversible data-hiding scheme for covert communication is proposed in this paper. After the message extraction, the host images can be completely recovered. Unlike most LSB-based reversible data hiding algorithms, which employ LSB replacement, the proposed method uses LSB matching, thus avoids introducing any asymmetric distortions to the host image and further makes the proposed reversible method immune against most existing steg-analytical detectors.

The proposed method can be applied to the host image for many times and won’t cause larger distortions. The average PSNR of the stego images is 51.14dB. Consequently, the proposed method can achieve high payload and high visual quality at the same time. Furthermore, this scheme is quite simple and it will fit well in some crucial application scenarios, in which reversible data hiding is required.

5 ACKNOWLEDGEMENTS

This work is supported by Science and Development Plan of Beijing Municipal Commission of Education (JC007011200903) and NSFC (National Natural Science Foundation of China 11007011201002).

REFERENCES

1. J. Fridrich, M. Goljan, R. Du.: Lossless data embedding-new paradigm in digital watermarking, EURASIP J. Appl. Sig. Process., vol. 2002, no. 02, pp. 185-196, (2002).
2. J. Fridrich, M. Goljan, and R. Du.: Invertible authentication, Proc. SPIE, no. 1, pp. 197-208, (2001).

3. M. U. Celik, G. Sharma, A. M. Tekalp.: Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol 14, no. 2, pp. 253-266,(2005).
4. J. Tian.: Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst.: Video Technol., vol. 13, no.8, pp.890-896, (2003).
5. D. M. Thodi, J. J. Rodriguez.: Expansion embedding techniques for reversible watermarking, IEEE Tans. Image Process., vol. 16, no. 3, pp. 721-730, (2007).
6. X. Li, B. Yang, T. Zeng.: Efficient reversible watermarking based on adative prediction-error expansion and pixel selection, IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524-3533, (2011).
7. J. Fridrich, M. Goljan, R. Du.: Reliable detection of LSB steganography in color and grayscale images, in Proc. ACM Workshop. Multimedia and Security, , pp. 27-30. (2001).
8. S. Dumitrescu, X. Wu, Z. Wang.: Detection of LSB steganography via sample pair analysis, in Proc. Information Hiding Wrokshop, Springer LNCS, vol. 2578, pp. 355-372. (2002).
9. A. Ker.: Improved detection of LSB steganography in grayscale imaegs, in Proc. Information Hiding Workshop, vol. 3200. Springer LNCS, pp. 97-115. (2004).
10. T. Sharp.: An implementation of key-based digital signal steganography, in Proc. Information Hiding Workshop, Springer LNCS, vol. 2137, pp. 13-26. (2001).