ISSN 2186-5647

Reversible Data Hiding Exploiting Coefficients Histogram in Wavelet Transform Domain

Department of CSIE, China University of Technology Te-Lung Yin

1. Introduction

Reversible data hiding has drawn lots of interest in the last a few years. With reversibility, original media can be recovered without any distortion from the marked media after the embedded data has been extracted. In this paper, we present a new scheme which utilizes the wavelet transform and better exploited large variance of wavelet coefficient differences to achieve high capacity and imperceptibility. With the particularity of minor changes in the wavelet coefficients after embedding data, low visual distortion can therefore be obtained in the marked image. Furthermore, an extraordinary attribute of our scheme is that the use of embedding level differs greatly from previous schemes. Experimental results showed that the performance our scheme outperforms the state-of-the-art reversible data hiding schemes.

2. Previous studies

Reversible data hiding, which is also referred to as lossless, invertible, or distortion-free, data hiding, is known as a branch of fragile technique. This technique is mainly used for the quality-sensitive applications such as content authentication of multimedia, medical imaging systems, law enforcement, and military imagery, etc. One of the important requirements in these fields is to recover the original media exactly during analysis to take the right decision. The other important requirements are embedding capacity and visual quality of marked media [1].

The reversible data hiding schemes reported in the literature can be classified into two major categories in terms of different domains to hide information. The majority of researches in category-I work on spatial domain [2-8]. In category-II, the schemes work on transform domain, where the message bits were embedded into the corresponding coefficients [9-11].

The scheme we present in this paper is attempted to achieve high performance reversible data hiding, in which the hiding and recovering processes are devised in the frequency domain. The particularities of large variance of coefficient differences and the minor changes in wavelet coefficients are exploited to achieve high capacity and imperceptible embedding.

3. The proposed scheme

In this section, we present a new scheme, combining the Haar discrete wavelet transform (HDWT) algorithm and the histogram shifting technique to achieve reversible data hiding. In our scheme, an original spatial domain image is first transformed into frequency domain consisting of four non-overlapping frequency sub-bands with HDWT algorithm. Sub-bands in middle- and high-frequency are then used to create sub-band differences. Each histogram of these sub-band differences is then shifted according to embedding level selected. Message bits can then be hidden in the empty space of the shifted histogram. Finally, the marked image is constructed with the sub-bands carrying hidden information and the original low-frequency sub-band by performing the inverse HDWT algorithm. This completes the information embedding process. As to the extracting process, proper corresponding inverse operations can be taken to recover the hidden information and the original image.

3.1 Data embedding

The secret message can be hidden in LH, HL,

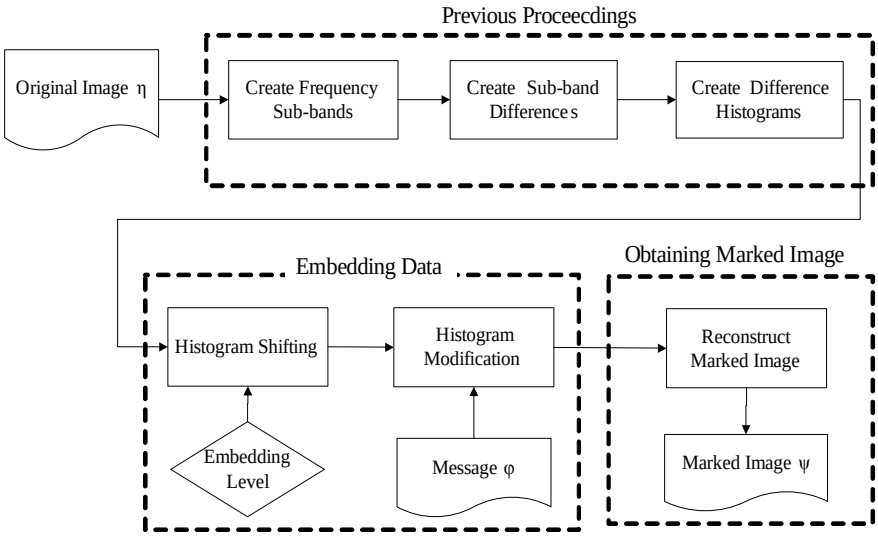

Fig. 1. Flowchart of overall data embedding process.

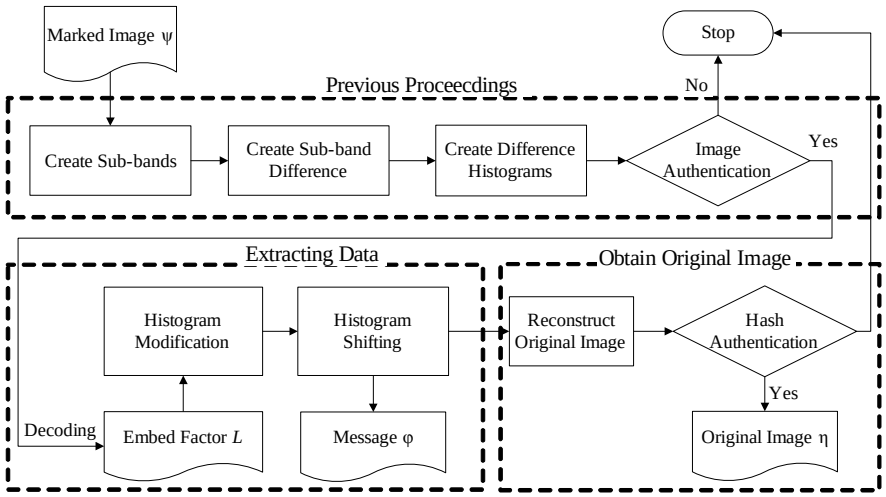

Fig. 2. Flowchart of overall extraction and recovery procedure.

and HH frequency sub-bands so as to achieve high similarity between the marked image and the original image. We assume that the secret messageis a random binary sequence of 0s and 1s, where n denotes the index of a message bit. The histograms of sub-band differences: LH-HH, LH-HL and HL-LH are shifted to embed the secret message. Fig. 1 depicts an overall data embedding process, which is described in details as follows:

3.2 Data extracting and reversing

Fig. 2 is a flowchart of extraction and recovery scheme. Before extracting the hidden message, receiver needs to verify whether the marked image has been modified or not. If the marked image is tampered, the proposed scheme stops the following extraction steps immediately. The authentication can also be implemented by using an extra simple hash function. With the hash value of the original image being embedded, the marked image is authentic provided the extracted hash value is not altered.

4. Experimental results and comparison

In this section, a set of experiments are conducted to evaluate the embedding performance of our scheme. Some commonly used standard images are used. The message bits to be embedded in our experiments are randomly a generated by a pseudo-random binary generator. And, the embedding level is ranged from 0 to 300. Our proposed scheme is measured by two factors:

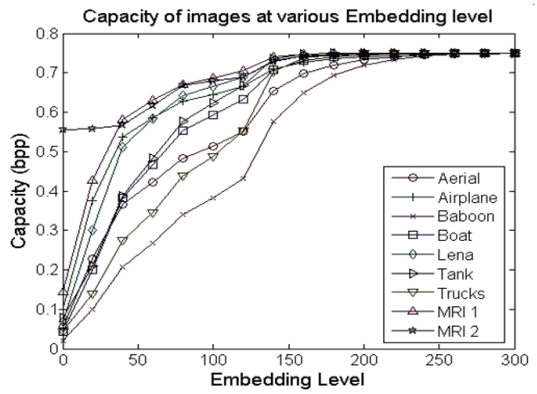

Fig. 3. Embedding capacity at various embedding levels.

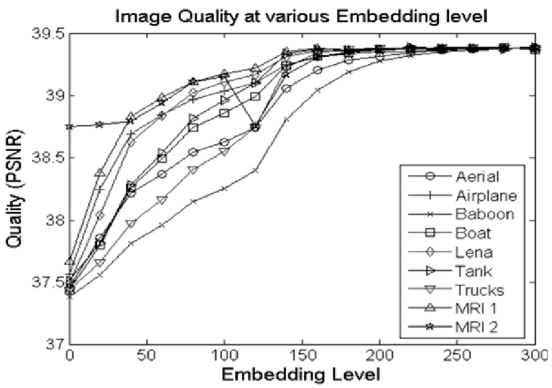

Fig. 4. PSNR for the variant images at various embedding levels.

the peak signal-to-noise ratio (PSNR) and the bits per pixel (bpp). In general, the factor bpp is used to evaluate the amount of bits that can be embedded into an image.

Fig. 3 depicts the embedding rates up to 0.75 bpp provided by varying the embedding level from 0 to 300 for the test images. When we observe the characteristic in Fig. 3, we discover that the maximal capacity is closely connected to the embedding level, that is, the larger the embedding level we set, the more wavelet coefficient differences between $[-L,L]$ can be obtained. Hence, the embedding capacity at each level increases gradually as the level pre-defined becomes larger and larger in our scheme.

To illustrate the relationship between the visual quality and the embedding level L, we also conducted a set of experiments on all the test images. Fig. 4 depicts the visual quality of the marked image provided by varying embedding level from 0 to 300 for test images on the premise that maximal bits are embedded. The result reflected in Fig. 4 indicates that the PSNR depends strongly on the embedding level. The marked image can achieve 37.6 dB at the embedding level 0, whereas the market image can achieve 39.2 dB at the embedding level of 150 for the "Airplane" test image. The principal reason for the less distortion is that the larger embedding level L can contribute less variation in the histogram of wavelet transform. Furthermore, since the middle- and high-frequency subbands incorporate less energy, the test image with larger variance between middle- and high-wavelet coefficients such as "MRI 1" and "MRI 2" can achieve higher visual quality than "Baboon" at the embedding level 0. Fig. 5 shows the marked images at various embedding capacities. The

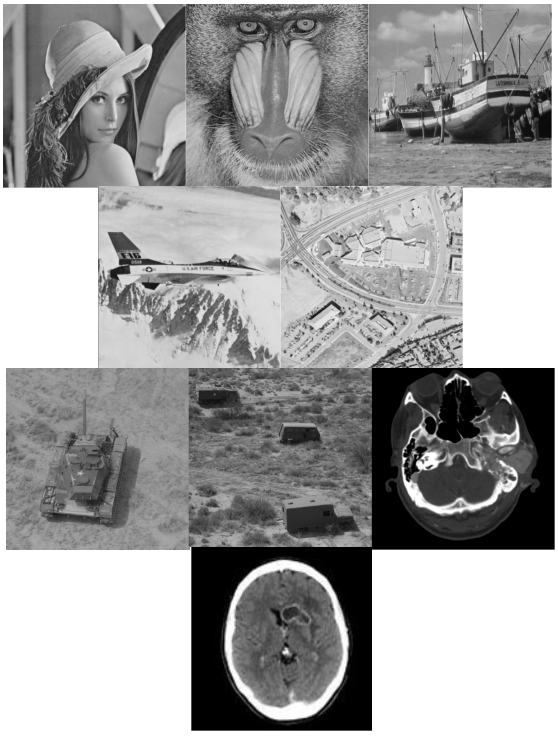

Fig. 5. The marked images: (a) 38 dB with 0.745 bpp; (b)39 dB with 0.745 bpp; (c) 39.5 db with 0.732 bpp; (d) 38 dB with 0.745 bpp; (e) 39 dB with 0.745 bpp; (f) 39.5 dB with 0.746 bpp; (g) 38 dB with 0.745 bpp; (h) 39 dB with 0.745 bpp.

results reflected in the Figs. indicate that the visual quality of the marked image is satisfactory.

5. Conclusions

This paper presents a simple and high performance reversible data hiding scheme. By utilizing the large variance of wavelet coefficient differences and the ingenious histogram shifting rules, our scheme, compared with previous schemes, can obtain a better visual quality of the marked image at the same payload. Through a joint evaluation of embedding capacity and visual quality, the PSNR after embedding process is always above 40 dB. Even when the embedding capacity reaches 0.75 bpp for the test images, the average PSNR is still higher than 39 dB. However, in the future, a multi-round scheme will be extended by considering higher capacity with low distortion performance.

References

[1] M. Awrangjeb: Proc. Sixth International Conf. on Computer and Information Technology, Jahangirnagar University, Bangladesh, p. 75-79, (2003).

[2] J. Fridrich, M. Goljan, and R. Du: Proc. of the SPIE, Security and Watermarking of Multimedia Contents, San Jose, Vol. 4314, CA, p. 197-208, (2001).

[3] M.U. Celik, G. Sharma, and A.M. Tekalp: Proc. IEEE International Conf. on Image Processing, Rochester, NY, p. 157-160, (2002).

[4] M.U. Celik, G. Sharma, A.M. Tekalp, and E. Saber,: IEEE Trans. on Image Proc. Vol. 14, No. 2, p. 253-266, (2005).

[5] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su: IEEE Transactions on Circuits and Systems for Video Technology Vol. 16, No. 3, p. 354-362, (2006).

[6] J. Hwang, J.W. Kim, and J.U. Choi: International Workshop on Digital Watermarking, Lecture Notes in Computer Science, Korea, Vol. 4283, p. 348-361, (2006).

[7] W.-C. Kuo, D.-J. Jiang, and Y.-C. Huang: International Conf. on Intelligent Computing, Lecture Notes in Artificial Intelligence, Qing Dao, China, Vol. 4682, p. 1152-1161, 2007.

[8] K.-S. Kim, M.-J. Lee, H.-Y. Lee, and H.-K. Lee: Pattern Recognition, Vol. 42, p. 3083-3096, (2009).

[9] G. Xuan, Y.Q. Shi, J. Chen, J. Zhu, and Z. Ni, W. Su: IEEE International Workshop on Multimedia Signal Processing, St. Thomas, Virgin Islands, USA, (2002).

[10] J. Tian: IEEE Trans. on Circuits and Systems for Video Technology Vol. 13, No. 8, p. 890-896, (2003).

[11] S. Lee, C.D. Yoo, and T. Kalker: IEEE Trans. on Information Forensics and Security Vol. 2, No. 3, p. 321-330, (2007).