Integrated encoding with high efficiency for digital steganography

X. Zhang, W. Zhang and S. Wang

Three different encoding mechanisms are combined to improve further steganographic embedding efficiency. They are secret-bit representation derived from the parity check coding, exploitation of the modification direction on pixel-values, and wet paper coding. The parity of least significant bit weight in each pixel-group is used to accommodate one secret bit. The weighted-sums of all pixel-groups and wet paper coding are used to select which pixels are modified and decide the way of modification as to whether to add or subtract one for carrying more secret data. It is shown that, by taking full advantage of these mechanisms, the embedding efficiency of the proposed scheme is higher than any of the previous steganographic embedding techniques.

Introduction: Digital steganographic techniques aim to embed secret messages into a carrier signal by altering its most insignificant components for covert communication [1]. A data-hider always seeks the lowest possible rate of modification to the cover signal or the highest possible embedding capacity at a given distortion level. In other words, an important task is to improve embedding efficiency. To achieve this goal, various techniques have been developed. For example, in matrix encoding [2], no more than one change of the least significant bit (LSB) is made to embed l secret bits into 2^l-1 pixels. Thus, distortion caused by data hiding is significantly lowered compared to a plain LSB technique in which secret bits are used to simply replace the LSB plane. Moreover, Dijk and Willems described some effective encoding methods derived from the cyclic coding in [3]. The matrix encoding can be viewed as a special case of this method. Steganographic encoding can also be performed in a dynamical running manner so that insertion and extraction of each secret bit are carried out in a series of consecutive cover bits, not in a block of cover bits [4].

The above-mentioned steganographic encoding techniques are independent of various cover-bit-modification approaches. It means that, when applying steganographic encoding techniques to the LSB plane of an image, adding 1 to a pixel is equivalent to subtracting 1 from the pixel in terms of flipping its LSB for carrying the secret message. In fact, the choice of addition or subtraction can also be utilised to carry more secret data. A simple application of this principle is given in [5]. In addition, Zhang and Wang [6] and Fridrich and Lisonek *et al.* [7] independently presented a same method with better performance, termed, respectively, exploiting modification direction (EMD) and grid colouring (GC for short). Using this method, $\log_2(2n+1)$ secret bits are embedded into n cover pixels and, at most, only one pixel is increased or decreased by 1. In [7], a data-hiding approach incorporating the GC method with a Hamming-derived steganographic encoding technique is also studied, which in fact belongs to the GC family as a special case. Another steganographic technique termed double-layered embedding [8] introduces a wet paper coding mechanism [9] to determine whether to add or subtract one to/from a pixel so that the second LSB can be used to accommodate additional secret data.

In this Letter we propose an integrated encoding scheme to improve further steganographic embedding efficiency, which takes full advantage of three different mechanisms: secret-bit representation derived from the parity check coding, exploitation of the modification direction on pixel-values, and wet paper coding. We show that the integrated encoding method is better than any of the previous steganographic embedding techniques.

Integrated encoding method: In the proposed integrated encoding scheme, the parity of LSB weight in each pixel-group is used to carry one secret bit. A weighted-sum function and wet paper coding mechanism are further used to select the pixels that should be modified and to decide the way of modification as to whether to add or subtract one for carrying more secret data. The detailed steganographic steps are as follows.

According to a secret key, all pixels of a cover image are permuted and divided into many groups, each containing 2^k pixels, where k is an integer no less than 0. Denote the number of pixel-groups N. In the first layer of the embedding, we insert one secret bit into each pixel-group. In other words, the parity of the LSB weight in a pixel-group is used to represent the secret bit 0 or 1. Here, LSB weight means the number of LSBs with value 1. If the secret bit to be embedded coincides with the parity of the LSB weight in the corresponding pixel-group, no modification is made. Otherwise, one LSB in the pixel-group should be flipped to change the original parity of LSB weight, and probability of this change is 1/2. Although adding and subtracting one to/from any pixel value is equivalent in embedding the secret bit, we show that selecting a suitable pixel to modify and choosing a suitable operation of addition/subtraction can be used to carry additional secret data in the second embedding layer.

Denote the pixel values in the nth pixel-group as $p(n, 1), p(n, 2), \ldots, p(n, 2^k)$, $n=1, 2, \ldots, N$, and define a weighted sum function of each pixel-group:

$$f_n = \sum_{m=1}^{2^k-1} [p(n,m)m] + g\left[p(n,2^k)\right]2^k \mod 2^{k+1} \quad (1)$$

Here, the definition of g is

$$g(x) = \lfloor x/2 \rfloor \quad (2)$$

Obviously, the value of f_n is within $[0, 2^{k+1}-1]$ so that it can be converted into a binary vector with a length $(k+1)$. If we increase or decrease the values of $p(n, m)$ by 1 $(1 \le m \le 2^k-1)$, f_n will be increased or decreased by m with module 2^{k+1}. If we increase or decrease the values of $p(n, 2^k)$ by 1, the value of f_n will be increased/decreased by 2^k with module 2^{k+1} or kept unchanged, respectively. This means that, when adding or subtracting one into/from a suitable pixel, we can obtain any desired pattern of the binary vector converted from a pixel-group.

Collect all binary converted vectors to form a concatenated vector containing a total of $N(k+1)$ bits, which will be used to carry additional cover data. For the pixel-groups with parities of LSB weights not being coincident with the secret bits to be embedded in the first layer, one pixel in each of the groups should be increased or decreased by 1 to alter the original parity. In this case, the converted vectors can be modified into any desired pattern, viz. the corresponding converted bits can be arbitrarily changed. On the other hand, the converted bits corresponding to the rest of the pixel-groups are not to be changed. A wet paper coding model [9] is used to perform the second layer embedding, in which the changeable and unchangeable converted bits are considered 'dry' and 'wet' elements, respectively. Suppose the number of changeable converted bits is N_C. By modifying only the changeable elements, we can embed on average N_C secret bits into all $N(k+1)$ converted bits. Here the expectation of N_C is $N(k+1)/2$. Although a receiver does not know the position of the changeable elements, he can still extract the embedded bits. An implementation of a wet paper encoder/decoder is given in [9].

Modification to a pixel may not be permitted if the pixel value is saturated (extreme dark or bright). To overcome this, one may change the saturated pixel that should be modified and an additional pixel in the same pixel-group by 1 in the allowable direction and try to perform embedding again. For example, an original pixel-group is [255 255 254 255] with $k=2$ and $f_n=3$. Assume that the corresponding secret bit in the first embedding layer is 0 so that one pixel in the pixel-group should be modified by one, meaning that the converted bits are 'dry' elements, and they should be changed to [100] in the second embedding layer. To obtain a suitable parity of LSB weight and the desired pattern of converted bits, the first pixel should be increased by one, but this operation is not allowable. Then, decrease the first and second pixel by one to make the group [254 254 254 255] with $f_n=0$ and try to perform embedding again. This requires an increase of the fourth pixel that is still prohibitive. Then, modify the fourth and first pixels to make the group [255 254 254 254] with $f_n=1$. In this case, the third pixel can be successfully increased by one. Therefore the stego-pixel-group becomes [255 254 255 254] with a suitable parity of LSB weight and converted bits [100]. Although in the case of saturation more modifications may be required, the overall performance is not affected since saturated pixels in a natural image are rare.

Performance analysis: As in [6], two parameters are used to measure the performance of the proposed integrated encoding scheme: embedding efficiency E, the ratio between the number of embedded bits and the distortion energy caused by data hiding, and embedding rate R that is the amount of secret bits embedded in each cover pixel. As

mentioned above, the cover image possesses $N\ 2^k$ pixels, among which on average $N/2$ pixels are increased or decreased by 1. In the first embedding layer, N pixel-groups carry N secret bits, while in the second layer, on average $N(k+1)$ converted bits carry $N(k+1)/2$ secret bits. Thus,

$$E = \frac{N + N(k+1)/2}{N/2} = k + 3 \tag{3}$$

and

$$R = \frac{N + N(k+1)/2}{N\,2^k} = \frac{k+3}{2^{k+1}} \tag{4}$$

Comparison of performance has been made between the matrix encoding [2], running coding [4], EMD method [6], double-layered embedding in [8], and the integrated encoding scheme proposed in this Letter. The results are shown in Fig. 1. The abscissa represents the embedding rate, and the ordinate is the embedding efficiency. It is observed that the integrated encoding scheme is best among these steganographic embedding techniques.

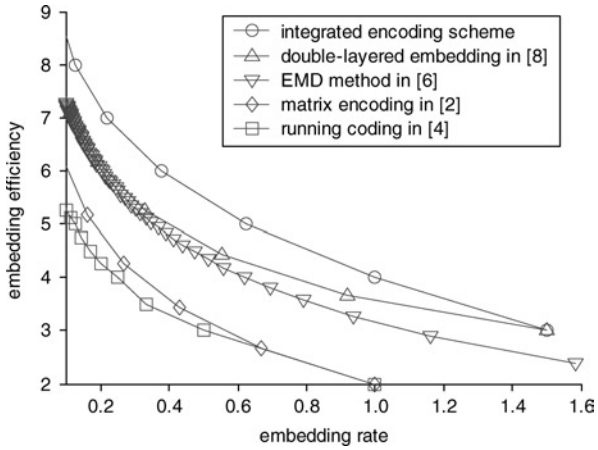

Fig. 1 *Performance comparison between various steganographic embedding techniques*

Acknowledgment: This work was supported by the National Natural Science Foundation of China (no. 60502039), Shanghai Rising-Star Program (no. 06QA14022), and Key Project of Shanghai Municipality for Basic Research (no. 04JC14037).

1 June 2007
Electronics Letters online no: 20071619
doi: 10.1049/el:20071619

X. Zhang, W. Zhang and S. Wang (*School of Communication and Information Engineering, Shanghai University, Shanghai 200072, People's Republic of China*)

E-mail: xzhang@shu.edu.cn

W. Zhang: Also with Department of Information Research, Information Engineering Institute, Zhengzhou, China

References

1 Wang, H., and Wang, S.: 'Cyber warfare: steganography vs. steganalysis', *Commun. ACM*, 2004, **47**, (10), pp. 76–82
2 Westfeld, A.: 'F5 – a steganographic algorithm'. 4th Int. Workshop on Information Hiding, *Lect. Notes Comput. Sci.*, **2137**, Springer-Verlag, 2001, pp. 289–302
3 Dijk, M., and Willems, F.: 'Embedding information in grayscale images'. Proc. 22nd Symp. Information Theory in the Benelux, The Netherlands, 2001, pp. 147–154
4 Zhang, X., and Wang, S.: 'Dynamical running coding in digital steganography', *IEEE Signal Process. Lett.*, 2006, **13**, (3), pp. 165–168
5 Mielikainen, J.: 'LSB matching revisited', *IEEE Signal Process. Lett.*, 2006, **13**, (5), pp. 285–287
6 Zhang, X., and Wang, S.: 'Efficient steganographic embedding by exploiting modification direction', *IEEE Commun. Lett.*, 2006, **10**, (11), pp. 781–783
7 Fridrich, J., and Lisonek, P.: 'Grid colorings in steganography', *IEEE Trans. Inf. Theory*, 2007, **53**, (4), pp. 1547–1549
8 Zhang, X., Zhang, W., and Wang, S.: 'Efficient double-layered steganographic embedding', *Electron. Lett.*, 2007, **43**, (8), pp. 482–483
9 Fridrich, J., Goljan, M., Lisonek, P., and Soukal, D.: 'Writing on wet paper', *IEEE Trans. Signal Process.*, 2005, **53**, (10), pp. 3923–3935