Embedding in Two Least Significant Bits with Wet Paper Coding

Xin Liao
liaoxinbupt@gmail.com

Qiao-yan Wen
wqy@bupt.edu.cn

（State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China）

Abstract

In this paper, we present three embedding schemes for extensions of least significant bit overwriting to both of the two lowest bit planes in digital images. Our approaches are inspired by the work of Fridrich et al. [8] who proposed wet paper coding as an efficient method for steganographic schemes. Our new works generalize it to the embedding in two least significant bits, that is to say, combine two novel extensions of least significant bits embedding and the double-layered embedding developed in [16] with wet paper coding, respectively. The proposed schemes improve steganographic security and are less vulnerable to steganalytic attacks compared with original schemes with shared selection channels between the sender and the recipient.

1. Introduction

Digital steganography is a technique for embedding secret messages into host media by altering its most insignificant components for covert communication [1]. Generally speaking, a good steganographic technique should have good visual/statistical imperceptibility and a sufficient payload [2]. LSB replacement embeds a message into the cover image by replacing the LSBs of the cover image with secret message bits to arrive at the stego image. It can be detected by the current detection methods due to the imbalance, which exists in the embedding distortion in the stego image. LSB matching has been introduced, and it also modifies the LSBs of the cover image for messages embedding. If the message bit does not match the LSB of the cover image, then one is either added or subtracted randomly from the value of the cover pixel [3-5]. In this paper, the LSB embedding method we refer to is realized by simply matching the LSBs of the cover image with the secret message bits.

The modification placement of embedding changes in the cover object is called "the selection channel" [6]. An obvious problem here is that the recipient may not be able to determine the same selection channel because he does not have access to the cover object or any side information [7]. The wet paper coding (WPC) was proposed as a solution to a scenario called "writing on wet paper" which frequently occurs in steganography [8-12]. A total of bits can be embedded and received successfully using the wet paper coding without sharing the knowledge about the positions of constraints between the sender and the recipient.

To explain the metaphor, imagine that the cover object X is an image that was exposed to rain and the sender can only slightly modify the dry spots of X but not the wet spots. During transmission, the stego image Y dries out and thus the recipient does not know which pixels were used by the sender for information hiding (the recipient has no information about the dry pixels). The task of wet paper coding is to enable both parties to exchange secret messages under the above scenario [8-12].

The remaining sections are organized as follows. In the next section we will give a brief introduction to wet paper coding of LSB embedding and three embedding schemes in two least significant bits. Section 3 proposes three new embedding schemes with wet paper coding, and then compares them. Conclusion is drawn in the last section.

2. Preliminaries

2.1. Wet paper coding of LSB embedding reviewed

Wet paper coding was previously proposed as a method for construction of steganographic schemes with arbitrary selection channels [8-12]. We stress that the selection channel is not shared with the recipient. The changeable pixels may be modified independently from each other to communicate secret data to the recipient, while the remaining pixels are not modified during embedding. To decode the secret messages, the recipient does not know which pixels were used by the sender for information hiding. Furthermore, it's mentionable that the recipient doesn't need to know the length of the secret data. A detailed implementation was given in [8].

In this paper, we apply wet paper coding method to embedding schemes for extensions of least significant bit overwriting to both of the two lowest bit planes, while currently existing applications of this method are about only the first LSB plane, such as in [8].

2.2. Embedding in two LSBs

Generally speaking, the following two obvious schemes may be taken for embedding a payload by overwriting the two lowest bit planes of the cover image [13].

1) For embedding in the two LSBs, bits are embedded in the cover image by selecting pixels and replacing both of the two LSBs of each pixel. We will abbreviate this as 2LSB embedding.

2) As an alternative scheme in the two LSBs, bits can be embedded in the cover image by selecting pixels and replacing only the second LSB of each pixel then repeating with a new selection of pixels of which only the LSB is used. Therefore, changes occur in the first and second LSB planes independently. We will abbreviate this as I2LSB embedding (letter "I" signifies the independence of the effects on the two lowest bit planes).

The above-mentioned methods are independent of cover-bit-modification approaches, adding 1 to a pixel is equivalent to subtracting 1 from the pixel. In fact, the choice of addition or subtraction will be determined in the second layer embedding. So another steganographic method called "double-layered embedding" (DLE) was proposed [14-16]. It shows that the second LSB plane could be used to accommodate additional secret data by selecting suitable operations of addition/subtraction. If a pixel value is even, adding and subtracting one keeps and flips the second LSB, respectively. On the other hand, if a pixel value is odd, the two operations cause opposite results in the second LSB. A detailed implementation was given in [16].

3. Proposed Schemes

Referring to the description of wet paper coding in [8-12], we assume that the cover image X consists of n elements $\{x_j\}_{j=1}^{n}$, $x_j \in J$, where J is the range of discrete values for x_j. For example, for an 8-bit grayscale image represented in the spatial domain, $J = \{0,1,...,255\}$. The sender selects k changeable elements x_j, $j \in C \subset \{1,2,...,n\}$, $|C| = k$, which is the selection channel. The changeable elements may be modified independently from each other by the sender to communicate secret messages to the recipient, while the remaining elements are not modified. We further assume $FL(x)$ denote the first LSB of x, $SL(x)$ denote the second LSB of x. The vectors of the cover image symbols $b = (FL(x_1), FL(x_2), ..., FL(x_n))^T$ and $a = (SL(x_1), SL(x_2)..., SL(x_n))^T$, which denote the first and second LSBs of all the pixels, respectively ("T" signifies transposition). We introduce the following schemes to fully exploit the wet paper coding in two least significant bits.

3.1. 2LSB scheme

In this section, we present a novel 2LSB scheme with wet paper coding. In this scheme, the selections in the first and second LSB planes are identical, so we make use of WPC method in the first and second LSB simultaneously.

Encode:

The sender and the recipient share a secret key, which can generate a pseudo-random binary matrix D of dimensions $m \times n$. Then it can communicate $2m$-bit data $S = (s_1, ..., s_{2m})$. The sender first divides the hidden data into two shares with the same length,

$$S = S^{(1)} + S^{(2)} = (s_1, ..., s_m) + (s_{m+1}, ..., s_{2m}) \quad (1)$$

During the embedding, the first and second LSBs of some x_j, $j \in C$ are modified together, it means that the sender either leaves the changeable elements unmodified or flips $FL(x_j)$ and $SL(x_j)$. The vector of cover image symbols b and a change to b' and a' at the same time, so that the modified binary column vectors b' and a' satisfies

$$D[a', b'] = [S^{(1)}, S^{(2)}] \quad (2)$$

Here $[a', b']$ denotes a binary matrix of dimensions $n \times 2$, which means the combination of the first and second LSBs of the pixels, $[S^{(1)}, S^{(2)}]$ denotes a binary matrix of dimensions $m \times 2$, which consists of $2m$-bit hidden data.

Decode:

The recipient receives the modified stego object, decodes very easily, first forms the vectors b' and a', then obtains the $2m$-bit hidden data by performing a matrix multiplication with the shared matrix D.

The maximal length of the data that can be embedded is related to the expected rank of the shared matrix D, which determines if the system $D[a', b'] = [S^{(1)}, S^{(2)}]$ has a solution or not for an arbitrary message S. Given k, which is the number of changeable pixels, according to the formulation in [8], we can know that the sender will be able to communicate approximately $2k$ bits to the recipient in this scheme.

3.2. I2LSB scheme

In this section, an I2LSB scheme with wet paper coding is proposed. In this scheme, the selections in the first and second LSB planes are independent, so we take advantage of WPC method in both the first and second LSB. We suppose C_1 is the set of k_1 changeable elements for the first LSB embedding, while C_2 is the set of k_2 changeable elements for the second LSB embedding.

Encode:

The sender and the recipient share two secret keys, which can generate two pseudo-random binary matrices D_1 and D_2 of dimensions $m_1 \times n$ and $m_2 \times n$, respectively. Then it can communicate $(m_1 + m_2)$ -bit data $S = (s_1, ..., s_{m_1+m_2})$. The sender first divides the hidden data into two parts,

$$S = S^{(1)} + S^{(2)} = (s_1, ..., s_{m_1}) + (s_{m_1+1}, ..., s_{m_1+m_2}) \quad (3)$$

During the first LSB embedding, the first LSBs of some x_j, $j \in C_1$ are modified, the sender either leaves the changeable elements unmodified or flips $FL(x_j)$. The vector of cover image symbols b changes to b', so that the modified binary column vector b' satisfies

$$D_1 b' = S^{(1)} \quad (4)$$

Then it can communicate m_1 -bit data $S^{(1)}$.

During the second LSB embedding, the second LSBs of some x_i, $i \in C_2$ are modified. The sender either leaves the changeable elements unmodified or flips $SL(x_i)$. Note that the sets of changeable elements in the first and second LSB embedding are independent, so the selections are independent and usually different. The vector of cover object symbols a changes to a', so that the modified binary column vector a' satisfies

$$D_2 a' = S^{(2)} \quad (5)$$

Then it can communicate m_2 -bit data $S^{(2)}$.

Decode:

The recipient receives the stego object, first forms the vector b' and a', then obtains the $(m_1 + m_2)$ -bit hidden data using the shared matrices D_1 and D_2.

3.3. Double layered embedding scheme

In this section, applying the wet paper coding to DLE in the first and second LSB embedding, we propose the double layered embedding scheme with wet paper coding.

In this scheme, the selection in the second LSB embedding is determined by that in the first one, so we should apply WPC to the first LSB embedding at first. We suppose C_1 is the set of k_1 changeable elements for the first LSB embedding. Wet paper coding can be used to perform the second LSB embedding, in which the modified and unmodified of changeable elements in the first LSB embedding are considered as "dry" and "wet" elements, respectively. The second LSB of the "dry" elements could be used to accommodate additional secret messages by selecting suitable operations of addition/subtraction. We further suppose C_2 is the set of k_2 changeable elements for the second LSB embedding, obviously, $C_2 \subseteq C_1$ and the expectation of k_2 is $k_1 / 2$. Without loss of generality, assume $k_1 / 2$ is an integer, we can embed on average of $k_1 / 2$ secret message bits in the second LSB embedding.

Encode:

The sender and the recipient share two secret keys, which can generate two pseudo-random binary matrices D_1 and D_2 of dimensions $m_1 \times n$ and $(k_1 / 2) \times n$, respectively. Then it can communicate $(m_1 + k_1 / 2)$ -bit data $S = (s_1, ..., s_{m_1+k_1/2})$. The sender first divides the hidden data into two parts,

$$S = S^{(1)} + S^{(2)} = (s_1, ..., s_{m_1}) + (s_{m_1+1}, ..., s_{m_1+k_1/2}) \quad (6)$$

During the first LSB embedding, the first LSBs of some x_j, $j \in C_1$ are modified. The sender either leaves the changeable elements unmodified or flips $FL(x_j)$. The vector of cover object symbols b changes to b', so that the modified binary column vector b' satisfies

$$D_1 b' = S^{(1)} \quad (7)$$

Then it can communicate m_1 -bit data $S^{(1)}$.

During the second LSB embedding, the sender modifies the second LSBs of some x_i, $i \in C_2$. The sender either leaves the changeable elements unmodified or flips $SL(x_i)$. The vector of cover object symbols a changes to a', so that the modified binary column vector a' satisfies

$$D_2 a' = S^{(2)} \quad (8)$$

Then it can communicate $(k_1 / 2)$ -bit data $S^{(2)}$.

Decode:

The recipient receives the stego object, first forms the vector b' and a', then obtains the $(m_1 + k_1 / 2)$ -bit hidden data using the shared matrices D_1 and D_2.

3.4. Comparisons

From the precise formulation in [8], it can be shown that the expected maximum number of bits that can be embedded approaches the number of changeable pixels.

The comparisons among 2LSB, I2LSB and DLE schemes are given by the same value of the number of changeable pixels, which is denoted *k*. In the 2LSB and I2LSB schemes, we can both embed *2k*-bit secret message, while *3k/2*-bit secret message will be embed in the DLE scheme. We also concern about the distortion energy caused by data embedding. The comparison results are listed in Table 1.

As is shown in Table 1, one can see that DLE with WPC scheme is significantly more efficient than other proposed schemes.

Table 1. Comparisons among the proposed schemes

Scheme	Embedded bits	Distortion
2LSB with WPC	*2k*	*k*
I2LSB with WPC	*2k*	*k*
DLE with WPC	*3k/2*	*k/2*

4. Conclusion

In this paper, we present three embedding schemes in two least significant bits with wet paper coding. Furthermore, all of them improve steganographic security and are less vulnerable to steganalytic attacks compared with original schemes with shared selection channels. So they can be used widely, especially in communication environments, which require higher security.

Acknowledgements

This work is supported by the National High Technology Research and Development Program of China, Grant No. 2006AA01Z419; the Major Research Plan for the National Natural Science Foundation of China, Grant No. 90604023; and the Natural Science Foundation of Beijing, Grant No. 4072020. Special thanks belong to Prof. X. Zhang for many useful discussions.

References

[1] H. Wang and S. Wang, "Cyber warfare: steganography vs. steganalysis", Commun. of the ACM, vol. 47, no. 10, 2004, pp. 76-82.

[2] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity", IEEE Signal Process. Lett., vol.12, no. 1, Jan. 2005, pp. 67–70.

[3] A. Ker, "Improved detection of LSB steganography in grayscale images", in Proc. Information Hiding Workshop, vol. 3200, Springer LNCS., 2004, pp. 97–115.

[4] T. Sharp, "An implementation of key-based digital signal steganography", in Proc. Information Hiding Workshop, vol. 2137, Springer LNCS., 2001, pp. 13–26.

[5] J. Mielikainen, "LSB matching revisited", IEEE Signal Process. Lett., vol. 13, no. 5, 2006, pp. 285–287.

[6] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Commun., vol. 16, 1998, pp. 474−481.

[7] A. Westfeld and R. Böhme, "Exploiting Preserved Statistics for Steganalysis", in Proc. Information Hiding Workshop, Springer LNCS., vol. 3200, 2004, pp.67–81.

[8] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper", IEEE Trans. Signal Process., vol. 53, no. 10, Oct. 2005, pp. 3923–3935.

[9] J. Fridrich, M. Goljan, and D. Soukal, "Efficient wet paper codes", in Proc. Information Hiding Workshop, Springer LNCS, 2005, pp. 204–218.

[10] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Perturbed Quantization Steganography with Wet Paper Codes", in Proc. ACM Multimedia and Security Workshop. Magdeburg Germany, 2004, pp. 4–15.

[11] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency", IEEE Trans. Information Forensics and Security, vol. 1, no. 1, Mar. 2006, pp. 102–110.

[12] H. Gou and M. Wu, "Improving embedding payload in binary images with super-pixels", ICIP 2007, vol. 3, no.1, Oct. 2007, pp. 277–280.

[13] A. Ker, "Steganalysis of embedding in two least-significant bits", IEEE Trans. Information Forensics and Security, vol. 2, no.1, Mar. 2007, pp. 46–54.

[14] X. Zhang, W. Zhang, and S. Wang, "Efficient double-layered steganographic embedding", Electronics Lett., vol. 43, no. 8, Oct. 2007, pp. 482–483.

[15] X. Zhang, W. Zhang, and S. Wang, "Integrated encoding with high efficiency for digital steganography", Electronics Lett., vol. 43, no. 22, Oct. 2007, pp. 1191–1192.

[16] X. Zhang, W. Zhang, and S. Wang, "A double layered "plus-minus one data embedding scheme", IEEE Signal Process. Lett., vol. 14, no. 11, Nov. 2007, pp. 848–851.