J. Vis. Commun. Image R. 22 (2011) 1–8

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

A steganographic method for digital images with four-pixel differencing and modified LSB substitution

Xin Liao [a,*], Qiao-yan Wen [a], Jie Zhang [b]

[a] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

ARTICLE INFO

Article history:
Received 13 December 2009
Accepted 22 August 2010
Available online 27 August 2010

Keywords:
Steganography
Four-pixel differencing
Modified LSB substitution
Data hiding
Pixel-value differencing
Error block
Embedding capacity
Imperceptible

ABSTRACT

To improve the embedding capacity and provide an imperceptible visual quality, a novel steganographic method based on four-pixel differencing and modified least significant bit (LSB) substitution is presented. The average difference value of a four-pixel block is exploited to classify the block as a smooth area or an edge area. Secret data are hidden into each pixel by the k-bit modified LSB substitution method, where k is decided by the level which the average difference value falls into. Readjustment will be executed to guarantee the same level that the average difference value belongs to before and after embedding, and to minimize the perceptual distortion. By proving that the readjusting procedure works, a theoretical proof is given to justify our method succeeded in embedding and extracting. Our experimental results have shown that the proposed method not only has an acceptable image quality but also provides a large embedding capacity.

1. Introduction

Internet is a popular communication channel nowadays. Transmitted data are easy to be copied or destroyed by unauthorized persons. Therefore, how to transmit data secretly by internet becomes an important topic. Encryption may provide a safe way, which transforms data into a ciphertext via cipher algorithms [1]. However, it makes the messages unreadable and suspicious enough to attract eavesdroppers' attention. To overcome this problem, steganography offers different approaches to transmitting secret messages [2,3]. Steganography is a technique that imperceptibly hides secret data into cover media by altering its most insignificant components for covert communication, such that an unauthorized user will not be aware of the existence of secret data [4].

The most common and well-known steganographic method is called least significant bit (LSB) substitution, which embeds secret data by replacing k LSBs of a pixel with k secret bits directly [5]. Many optimized LSB methods have been proposed to improve this work [6–8]. The human perceptibility has a property that it is sensitive to some changes in the pixels of the smooth areas, while it is not sensitive to changes in the edge areas. Not all pixels in a cover image can tolerate equal amount of changes without causing noticeable distortion. Hence, to improve the quality of stego images, several adaptive methods have been proposed in which the amount of bits to be embedded in each pixel is variable [9–16]. In 2003, Wu and Tsai proposed a novel steganographic method that uses the difference value between two neighboring pixels to determine how many secret bits should be embedded [9]. Chang and Tseng proposed a side match approach to embed secret data, where the number of bits to be embedded in a pixel is decided by the difference between the pixel and its upper and left side pixels [10]. In 2005, Wu et al. presented a novel steganographic method, which combined pixel-value differencing and LSB substitution [11]. Park et al. proposed a new method based on the difference value between two pixels adjacent to the target pixel [12]. In 2006, Yang and Weng proposed a multi-pixel differencing method that uses three difference values in a four-pixel block to determine how many secret bits should be embedded [13]. The method in [14] provided the combination of multi-pixel differencing and LSB substitution to improve the work in [13], but the embedding capacity is far less than that of Wu et al.'s method. In 2008, Wang et al. presented a steganographic method that utilizes the remainder of two consecutive pixels to record the information of secret data [15]. Yang et al. proposed an adaptive LSB steganographic method using the difference value of two consecutive pixels to distinguish between edge areas and smooth areas [16]. All pixels are embedded by the k-bit modified LSB substitution method, where k is decided by the range which the difference value belongs to [16].

However, some of them seem not to consider the features of edge sufficiently [9,11,15,16]. The methods in [10,12] have overcome the drawback, but unfortunately they would result in the

* Corresponding author.
E-mail address: liaoxinbupt@gmail.com (X. Liao).

1047-3203/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jvcir.2010.08.007

propagated error and lower embedding capacity. In order to provide better stego-image quality and larger embedding capacity, a novel steganographic method improving the multi-pixel differencing based on modified LSB substitution is presented in this paper. Similar to [13,14], a four-pixel block with three difference values is sufficiently considered. The average value of three difference values is exploited to distinguish between edge areas and smooth areas, and to estimate how many secret bits will be embedded into the block. Embed secret bits into each pixel in the block by modified LSB substitution method. Readjustment will be executed to extract secret data exactly and to minimize the perceptual distortion resulted from embedding. The experimental results show that our proposed method provides a large embedding capacity, and the quality of the stego image is improved as well.

The remainder of this paper is organized as follows. In Section 2, the embedding and extracting algorithms of the proposed method is presented. In the next section, we show that the proposed method succeed in embedding and extracting by proving that the readjusting procedure works. The experimental results will be in Section 4. Finally, conclusions are given in Section 5.

2. The proposed method

The proposed method conforms to the issues that are mentioned before. The pixels in edge areas can tolerate much more changes without making perceptible distortion than smooth areas. The range of average difference value is partitioned into two different levels, low level and high level. The division of smooth and edge areas is predefined by users. Pixels located in the block are embedded by the k-bit modified LSB substitution method, where k is decided by the level which the average difference value belongs to. Low level will use a lower value k_l, while high level uses k_h. The perceptual distortion can be minimized by readjustment, which, at the same time, guarantees the same level that the average difference value belongs to before and after embedding. The embedding and extracting algorithms are presented in the following subsections.

The concept of modified LSB substitution is to increase or decrease the most significant bit (MSB) part by 1 in order to improve the image quality [17,18]. For instance, secret data is $m = 000_{(2)}$, then a pixel $p = 1100111_{(2)}$ is embedded by the 3-bit common LSB substitution method and have a result $p' = 1100000$. The MSB part of p' is increased by 1, so the result of modified LSB substitution method is $p' = 1101000_{(2)}$, reducing the difference between p and p'.

2.1. The embedding algorithm

All the pixels in the cover image are 256 gray values. The cover image is partitioned into non-overlapping four-pixel blocks. For each block, there are four neighboring pixels $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j}$, $p_{i+1,j+1}$, and their corresponding gray values are y_0, y_1, y_2 and y_3, respectively. The detailed embedding steps are as follows.

Step 1: Calculate the average difference value D, which is given by

$$D = \frac{1}{3}\sum_{i=0}^{3}(y_i - y_{min}) \qquad y_{min} = min\{y_0, y_1, y_2, y_3\} \tag{1}$$

Step 2: Our proposed method adaptively embeds messages using two levels (lower-level and higher-level), and threshold value T is used to partition the range of D into two levels. If $D \leqslant T$, D belongs to "lower-level" (i.e., the block belongs to a smooth area), then $k = k_l$. Otherwise, D belongs to "higher-level" (i.e., the block belongs to an edge area), then $k = k_h$. In order to succeed in the readjusting procedure, we apply the restrictions $2^{k_l} \leqslant T \leqslant 2^{k_h}$ and $1 \leqslant k_l, k_h \leqslant 5$.

Step 3: Verify whether the block belongs to "Error Block". If not, continue to next step. Otherwise, restart from Step 1.

Definition 1. Assume $y_{max} = max\{y_0, y_1, y_2, y_3\}$, the block is called "Error Block" if and only if $D \leqslant T$ and $y_{max} - y_{min} > 2T + 2$.

For instance, assume $T = 6$. A block with four neighboring pixel values (139,140,140,154) belongs to "Error Block", because $D = \frac{17}{3} < 6$ and $154 - 139 = 15 > 2 \times 6 + 2 = 14$. "Error Block" is *NOT* used to embed secret bits, which will be explained in Section 3.

Step 4: Convert y_i to be y'_i by the k-bit common LSB substitution method ($0 \leqslant i \leqslant 3$), respectively.

Step 5: Apply the k-bit modified LSB substitution method to y'_i, and let y''_i be the result ($0 \leqslant i \leqslant 3$), respectively.

Step 6: This step is called "readjusting procedure". Let $\widehat{y_i} = y''_i + l \times 2^k, 0 \leqslant i \leqslant 3, l \in \{0, 1, -1\}$, and search $(\widehat{y_0}, \widehat{y_1}, \widehat{y_2}, \widehat{y_3})$ such that
(1) $\widehat{D}$ and D belong to the same level, where $\widehat{D} = \frac{1}{3}\sum_{i=0}^{3}(\widehat{y_i} - \hat{y}_{min})$, $\hat{y}_{min} = min\{\widehat{y_0}, \widehat{y_1}, \widehat{y_2}, \widehat{y_3}\}$.
(2) The final stego block $(\widehat{y_0}, \widehat{y_1}, \widehat{y_2}, \widehat{y_3})$ does not belong to "Error Block".
(3) The value of $\sum_{i=0}^{3}(\widehat{y_i} - y_i)^2$ is minimized.

After the replacement of (y_0, y_1, y_2, y_3) by $(\widehat{y_0}, \widehat{y_1}, \widehat{y_2}, \widehat{y_3})$ in the block, the purpose of $4k$-bit secret data hiding have been achieved. Repeat Steps 1–6 until all the secret data are embedded in the cover image, and the stego image is obtained.

For example, suppose we have a block with four neighboring pixel values (139,146,137,142), and the secret data are 000111111101. Assume $T = 5$, $k_l = 2$ and $k_h = 3$. Calculate the average difference value $D = \frac{16}{3} > T = 5$, then $y_i (0 \leqslant i \leqslant 3)$ are embedded by the 3-bit common LSB substitution method at first, $y'_0 = 136, y'_1 = 151, y'_2 = 143$ and $y'_3 = 141$. After applying the 3-bit modified LSB substitution method, $y''_0 = 136$, $y''_1 = 143$, $y''_2 = 135$ and $y''_3 = 141$. Readjustment is executed resulting in $\widehat{y_0} = 136$, $\widehat{y_1} = 151$, $\widehat{y_2} = 135$ and $\widehat{y_3} = 141$.

2.2. The extracting algorithm

In the extraction process, we can quickly extract secret data without the original image. Partition the stego image into four-pixel blocks, which is identical with the embedding algorithm. For each block $(p_{i,j}, p_{i,j+1}, p_{i+1,j}, p_{i+1,j+1})$, the following steps are executed to extract the secret data.

Step 1: Calculate the average difference value D by Eq. (1).

Step 2: Use the threshold value T to find out the level which D belongs to. If D belongs to the "lower-level", $k = k_l$, otherwise $k = k_h$.

Step 3: Verify whether the block belongs to "Error Block". If not, extract $4k$-bit secret data from the k-bit LSB of $y_i (0 \leqslant i \leqslant 3)$. Otherwise, restart from Step 1.
For instance, we extract the embedding example (136,151,135,141), which is shown in the above subsection. Since $T = 5$, $D = \frac{23}{3}$ belongs to "higher-level", then $k = k_h = 3$. We extract 3-bit LSB of $y_i (0 \leqslant i \leqslant 3)$, respectively. Secret data 000111111101 can be obtained.

3. Theoretic analyses and discussions

Secret data can be directly extracted as the least k bits of the pixel values, because Step 4 and Step 5 in the embedding algorithm