Displays 42 (2016) 36–42

Contents lists available at ScienceDirect

Displays

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

An improved least-significant-bit substitution method using the modulo three strategy ☆

Wen-Long Xu [a], Chin-Chen Chang [b,*], Tung-Shou Chen [c], Liang-Min Wang [a]

[a] School of Computer Science and Technology, Anhui University, Hefei 230601, China
[b] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan
[c] Department Computer Science and Information Engineering, Notational Taichung University of Science and Technology, Taichung 40401, Taiwan

ARTICLE INFO

Article history:
Received 7 December 2015
Received in revised form 17 February 2016
Accepted 3 March 2016
Available online 12 March 2016

Keywords:
High embedding capacity
Modulo three strategy
LSB scheme
Steganalysis

ABSTRACT

In this paper, we proposed a novel method to embed a series of ternary secret data into a cover image based on an improved Least-Significant-Bit (LSB) scheme using the modulo three strategy. Our new method can hide two ternary numbers into each grayscale pixel, normally only modify the two LSBs of the pixel, while it may cause overflow/underflow and a carry/borrow. We solve these problems by adding 1 to the pixel or subtracting 1 from the pixel before embedding. The embedding capacity of our method can be 3.1699 bpp. At the same time, the quality of the stego image of our new method also is better than traditional LSB scheme when the embedding capacity is greater than 3 bpp with a Peak Signal-to-Noise Ratio (PSNR) greater than 37 dB. Extensive experimental results indicated that our new method is capable of getting a higher PSNR than traditional LSB scheme when the embedding capacity is greater than 3 bpp, and it has higher resistance ability against the chosen steganalysis algorithm when the embedding capacity is low.

1. Introduction

In recent years, with the rapid development of multimedia and computer networks, Internet is becoming popular and popular. Because of the popularity of the Internet, more and more people are transmitting large amounts of data via networks. However, the risk of illegal access and the loss of sensitive information have increased rapidly [1,2]. One of the most important reasons is that digital media are transmitted in an open channel.

Data hiding is one of the most popular technologies to prevent the loss of sensitive information. In data hiding, secret data are protected by embedding them in an ordinary original image, called the *cover image*, to create a so-called *stego image* [1]. Data hiding consists of two parts, i.e., the embedding process and the extraction process. Just as its name implies, the embedding process is to embed secret data into a cover image, and the extraction process is to extract the secret data from the stego image.

Data hiding also can be classified by whether the stego image can be restored after the secret data have been extracted. If the cover image can be restored, then it is called *reversible*, and this process often is used for military and medical images. Otherwise, the process is said to be *irreversible*. The premise of data hiding is that all of the data embedding operations on cover images should be imperceptible, i.e., illegal observers should not be able to perceive the distortion when a stego image is delivered to the receiver. In addition, the secret data must not be modified [3]. If the embedding methods are used inappropriately and changed some statistics of cover images, some abnormal phenomena that cannot be detected with the naked eye often can be detected by using appropriate statistical testing and analysis, this statistical analysis on test and analysis technique known as steganalysis [4–6].

Over the past decades, many data hiding methods have been proposed by scholars to address the issue of information security [7–19]. These methods generally can be classified into three types, i.e., the spatial domain [7–11], the frequency domain [12–14], and the compressed domain [15–19]. The most popular criteria for measuring the performance of data hiding are PSNR and embedding capacity. PSNR measures the difference between the cover image and the stego image. If one hiding method can maintain a quality stego image with low distortion, which is visually identical to the cover image, then its PSNR must be high. We consider this method to be a good image hiding method. However, we also want

☆ This paper was recommended for publication by Pen-Cheng Wang.

* Corresponding author at: Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 407, Taiwan. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.

E-mail addresses: xwlsunny@gmail.com (W.-L. Xu), alan3c@gmail.com (C.-C. Chang), tschen966@gmail.com (T.-S. Chen), jasonwanglm@gmail.com (L.-M. Wang).

http://dx.doi.org/10.1016/j.displa.2016.03.002
0141-9382/

to get a high embedding capacity. Embedding capacity refers to the maximum number of bits of secret data that can be embedded per pixel (bpp) in a cover image, and the higher this number is, the better the process is.

Bender et al. [20] first proposed the concept of data hiding, a form of steganography, which embeds data into digital media for the purpose of identification annotation and copyright. In their paper, they proposed an LSB scheme that just replaced the least significant bits of the cover image with the secret data. This method is used extensively due to its low computational complexity and a high embedding capacity. Chen et al. [21] introduced a data hiding method with high payload using the LSB and hybrid edge detection steganography mechanism. They simply constructed a hybrid edge detector using a fuzzy edge detector and the Canny edge detector, and their method achieved both high embedding capacity and high quality of the stego image through our human visual system (HVS). Wang et al. [22] used a genetic algorithm to generate a substitution table to improve the quality of the stego image. Chang et al. [23] improved upon Wang's method by proposing a dynamic programming method to efficiently pick out the best substitution table, thereby achieving a better performance. In order to get a high embedding capacity, Wang [24] used the modulus value as a threshold value to decide the number of bits of the secret data could be incorporated into the cover image, and they obtained a higher embedding capacity.

Although many scholars have proposed different methods to deal with binary secret data, the studies seldom have focused on data hiding methods for ternary secret data. Using ternary numbers has many advantages over the use of binary numbers. Ternary secret data can be carried by each pixel by doing nothing, by adding one to the grayscale value, or subtracting one from the grayscale value [25]. When the binary secret message is encoded in the ternary format, it becomes shorter, and we potentially can hide more data in the cover image [26]. Jheng et al. [27] proposed two data hiding methods, i.e., ternary data hiding (TDH) and coded-ternary data hiding (C-TDH) over ternary computers. They stated in their paper that the TDH method can provide a higher PSNR and that the C-TDH method can increase the embedding capacity. Chiou et al. [28] proposed an efficient side match vector quantization (SMVQ) based reversible data hiding method. They translated the secret data into a ternary string and embedded the ternary string into the cover image. This approach was more efficient, and it was capable of hiding a larger amount of secret data. Chen et al. [29] formulated a theoretical model of reversible data hiding over a special ternary cover and proposed the construction of a code to achieve reversible data hiding over the ternary cover, which provided both high embedding capacity and improved image quality.

Based on the LSB scheme and the good performance of the ternary number approach, in this paper, we proposed a new method to embed a series of ternary secret data into a cover image. In our new method, to achieve a high embedding capacity, we embedded two ternary numbers into each pixel, and we normally modified two LSBs of the pixel. However, our method may cause a carry/borrow and result in overflow/underflow problem. To solve these problems, we added a preprocessing with addition and subtraction 1 operation, which is discussed in Section 2.3. The embedding capacity of our method was greater than 3 bpp, and the quality of the stego image also was better than that of the traditional LSB schemes when the embedding capacity was greater than 3 bpp and the PSNR was greater than 37 dB.

In the following sections, in Section 2, a detailed description of the embedding and extracting is provided for our new method. The experimental results and analyses are in Section 3, and our conclusions are represented in Section 4.

2. Proposed method

In this section, the details of the proposed method are provided. Like other methods, our new method is divided into two parts, i.e., the embedding procedure and the extracting procedure.

2.1. Embedding procedure

Based on the traditional LSB scheme and the modulo three strategy, our improved data embedding algorithm is illustrated in this section.

Since gray values are integers, the gray image can be represented by one $m \times n$ dimensional space, defined as $I = \{v_{ij} | 0 \leqslant v_{ij} \leqslant 255, 0 \leqslant i < m, 0 \leqslant j < n\}$. The secret data are in the form of a ternary string which consists of 0, 1 and 2, such as 011210120221.

We embed two ternary data into one pixel, and the embedding procedure can be represented by following steps:

Initialization: Let the secret data be $S = \{s_w | 0 \leqslant w < |S|\}$, $I = \{v_{ij} | 0 \leqslant v_{ij} \leqslant 255\}$, $s_k, s_{k+1} \in S$, $i, j = 0$.

Step 1. Convert the pixel value v_{ij} to binary $b_7 b_6 \ldots b_0$, according to Eq. (1).

$$v_{ij} = \sum_{r=0}^{7} b_r \times 2^r. \tag{1}$$

Step 2. Divide $v_{ij} = b_7 b_6 \ldots b_0$ into two sub-segments, i.e., $sub1_{ij} = b_7 b_6 \ldots b_2$ and $sub2_{ij} = b_1 b_0$ according to Eq. (2).

$$\begin{aligned} sub1_{ij} &= v_{ij}/2^2, \\ sub2_{ij} &= \mathrm{mod}(v_{ij}, 2^2). \end{aligned} \tag{2}$$

Step 3. Embed the first ternary secret number s_k according to Eq. (3).

$$sub1_{ij}^{stego} = \begin{cases} sub1_{ij} & if \ \ \mathrm{mod}(sub1_{ij}, 3) = s_k, 1 \leqslant k \leqslant |S|, \\ sub1_{ij} + 1 & if \ \ \mathrm{mod}(sub1_{ij} + 1, 3) = s_k, 1 \leqslant k \leqslant |S|, \\ sub1_{ij} - 1 & otherwise. \end{cases} \tag{3}$$

Step 4. Connect $sub1_{ij}^{stego}$ generated in **Step 3** and $sub2_{ij}$ to construct v'_{ij}; then, embed the second ternary secret number s_{k+1} according to Eqs. (4) and (5).

$$v'_{ij} = sub1_{ij}^{stego} \times 2^2 + sub2_{ij}, \tag{4}$$

$$v_{ij}^{stego} = \begin{cases} v'_{ij} & if \ \ \mathrm{mod}(v'_{ij}, 3) = s_{k+1}, \\ v'_{ij} + 1 & if \ \ \mathrm{mod}(v'_{ij} + 1, 3) = s_{k+1}, \\ v'_{ij} - 1 & otherwise, \end{cases} \tag{5}$$

where v_{ij}^{stego} is the pixel value of the stego image located at coordinates (i,j).

Step 5. $k = k + 2$, move (i, j) to the next pixel and repeat **Steps 1–4** until all secret data are embedded in the cover image.

2.2. Extracting procedure

Similarly, the extracting procedure consists of two parts, i.e., extracting the secret message from both of the sub-segments of each pixel.

2.2.1. Extract the message from the first six bits

Assume that v_{ij}^{stego} is the value of a pixel in the stego image and, convert it into binary format, divided into $sub1_{ij}$ and $sub2_{ij}$, according to Eq. (2). Next, convert $sub1_{ij}$ to a decimal number, and the result of modulo 3 is the first ternary data, s_k, which we embedded earlier, as shown in Eq. (6):