The Journal of Systems and Software 84 (2011) 669–678

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

A data hiding scheme using the varieties of pixel-value differencing in multimedia images

Cheng-Hsing Yang[a], Chi-Yao Weng[b], Hao-Kuan Tso[c], Shiuh-Jeng Wang[d,*]

[a] Department of Computer Science, National Pingtung University of Education, Pingtung 900, Taiwan
[b] Department of Computer Science, National Tsing-Hua University, Hsinchu 300, Taiwan
[c] Department of Computer Science and Communication Engineering, Army Academy R.O.C., Chungli, Taoyuan 320, Taiwan
[d] Department of Information Management, Central Police University, Taoyuan 333, Taiwan

ARTICLE INFO

Article history:
Received 10 May 2010
Received in revised form 8 November 2010
Accepted 8 November 2010
Available online 4 December 2010

Keywords:
Capacity
Pixel-value differencing
Image quality

ABSTRACT

In this paper, a capacity promoting technique is proposed for embedding data in an image using pixel-value differencing (PVD). The PVD scheme embeds data by changing the difference value between two adjacent pixels so that more data is embedded into two pixels located in the edge area, than in the smooth area. In order to increase the embedding capacity, a new approach is proposed in this paper by searching edge area more flexibly. Instead of processing a pair of pixels at a time as proposed by Wu and Tsai, two pairs of pixels in a block are processed at the same time. In addition, we proposed a pixel-value shifting scheme to further increase the chances for embedding data. Our scheme exploits the edge areas more efficiently, thus leading to an increase in embedding capacity as shown by experimental results compared to Wu and Tsai's method. Also, the embedding result of our scheme passes the Fridrich et al.'s detection. Besides, according to the distribution of difference values, more practical range partitions are suggested for improving capacity.

1. Introduction

Nowadays, the Internet has become a common communication channel. Communicating in public system means that some problems need to be faced, such as data security, copyright protection, etc. Ciphering is a well-known method for security protection (Chu and Chang, 1999; Highland, 1997), but it has the disadvantage of making a message unreadable thereby attracting the attention of eavesdroppers. This makes steganography which hides data within data a good choice for secret communications (Bender et al., 1996; Anderson and Peticolas, 1998; Artz, 2001; Lee and Chen, 2000; Yu et al., 2005).

One of the best-known steganographic methods is the least-significant-bit (LSB) substitution (Chan and Chen, 2004; Chang et al., 2002; Li et al., 2009). The simple LSB substitution method replaces the length-fixed LSB with the fixed length bits. Although the technique is efficient, it is rather easy to create a noticeable distortion for the human eye or can be detected by some programs (Lee and Chen, 2000; Fridrich et al., 2001; Ker, 2007). Therefore, several adaptive methods have been proposed for steganography in order to decrease the distortion caused by the LSB substitution (Li et al., 2009; Yang and Wang, 2006; Yang, 2008). In addition, some methods use the concept of human vision to avoid the detection of programs (Wu and Tsai, 2003; Chang and Tseng, 2004).

Recently, Wu and Tsai proposed a "pixel-value differencing" steganographic method that used the difference value between two adjacent pixels in a block in order to determine the number of embeddable secret bits (Wu and Tsai, 2003). This difference value is adjusted so as to embed the secret bits, and the difference between the original and new difference values is adjusted between the two pixels. To check the proposed method, author applies the dual statistics method (Fridrich et al., 2001), called as RS-diagram, to detect the function of embedding method. In RS-diagram, first of all, the discrimination and flipping functions are applied to define pixel groups: Regular (R), Singular (S), and Unusable (U). Then, the percentages of all groups of Regular and Singular with masks $m = [0\,1\,1\,0]$ and $-m = [0\,-1\,-1\,0]$ are computed, in which they are represented as R_m, R_{-m}, S_m, and S_{-m}, respectively. Finally, the RS-diagram applied hypotheses of $R_m \cong R_{-m}$ and $S_m \cong S_{-m}$ to present the detected resultant.

In 2005, Wu et al.'s proposed a method which combines the pixel-value differencing and LSB replacement method. Their approach provides higher capacity than pixel-value differencing, but it does not pass the detection of RS-diagram, the reason is shown in (Yang et al., 2007). Consequently, Liu and Shih proposed generalized pixel-value differencing method in 2008. Their approach not only provides high capacity but also passes the detection of RS-diagram (Fridrich et al., 2001).

* Corresponding author. Fax: +886 3 3272038.
E-mail address: sjwang@mail.cpu.edu.tw (S.-J. Wang).

0164-1212/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2010.11.889

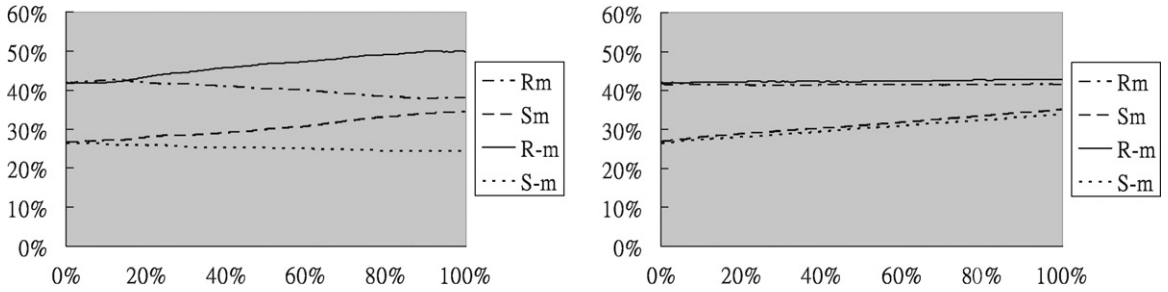

Fig. 1. RS-diagrams yielded by the dual statistics method by Fridrich et al. (2001) for experimental of stego-images by two methods. (a) Conventional 2-bits LSB substitution; (b) pixel-value difference method.

In this paper, we propose an efficient steganographic scheme to hide data imperceptibly in gray-level images. This scheme is based on the property of human eye, which is more sensitive to the change in the smooth area than the edge area (Lee and Chen, 2000; Wu and Tsai, 2003; Chang and Tseng, 2004; Wang et al., 2008; Yang et al., 2008). In this paper, we process a block of four neighboring pixels simultaneously. The number of secret bits to be embedded in a block depends on the degree of smoothness or sharpness. Each four-pixel block is divided into two two-pixel groups, and each group is processed using the approach of pixel-value differencing. In order to extract the embedded data correctly, some schemes are designed cleverly to differentiate which pixels belonging to different groups. In Wu and Tsai's (2003) method, some conditions will cause a block to be abandoned without embedding. To overcome this obvious drawback, a new technique known as pixel-value shifting is proposed. Experimental results show that our scheme not only provides higher embedding capacity than that of Wu and Tsai but also passes through Fridrich et al.'s (2001) detection.

The paper is organized as follows. Wu and Tsai's method is introduced in Section 2. Our scheme is presented in Section 3. The experimental results are shown in Section 4. Some analyses and discussions are given in Section 5. Finally, the conclusions are provided in Section 6.

2. Literature reviews

Wu and Tsai's steganographic method hides secret data in gray-level images by pixel-value differencing. First, the host image is partitioned into non-overlapping consecutive two-pixel blocks by scanning all the rows of the host image in a zigzag manner. A difference value d is calculated from the two pixels, say p_i and p_{i+1}, of each block. By symmetry, only the possible absolute values of d (0 through 255) are considered and they are classified into a number of contiguous ranges, called as R_i, where $i = 1, 2, 3, \ldots, n$. The width of R_i is $u_i - l_i + 1$, where u_i is the upper bound of R_i and l_i is the lower bound of R_i. The width of each range is taken as a power of 2. This restriction of width facilitates the embedding of binary data. If d falls in smooth area, less secret data will be hidden in the block. On the other hand, if d falls in sharp area, then the block has higher tolerance and thus more secret data can be embedded inside it. Suppose that d falls into the range R_k. The number of embedding bits is determined by the width of R_k. Therefore, the embedding operation is to replace d with a new difference value d', which is the sum of the embedded value and the lower bound of R_k. Finally, an inverse calculation from d' is performed to generate the new gray values of the two pixels in the block. Note that the new gray values of the two pixels must lie in between the range [0, 255]. Therefore, if the new gray values are created by value u_k, which are the maximally possible value of d', falling outside the range [0, 255], the block must be abandoned for embedding data.

In the extracting phase, the secret data are extracted from the blocks of the stego-image in the same order as the embedding phase. The number of secret bits to be embedded in a two-pixel block is determined by the range R_k, which is the range of the difference value between two pixels. In addition, the value of the embedded data in the block is calculated by subtracting the lower bound of R_k from the difference value of the block. Therefore, the embedded bits in the block can be reconstructed. To verify the security of the proposed method, authors apply statistic steganalytic technique (Fridrich et al., 2001) which is called RS-diagram, in order to prove that the method is undetected. The results are shown in Fig. 1.

3. Our approach

In this section, we introduce our steganographic scheme based on blockwise embedding. We use the idea of pixel-value differencing, but we process four pixels simultaneously in spite of two at a time. In the pixel-value differencing approach of Wu and Tsai, each time two pixels are grouped for embedding secret data. Fig. 2(a) shows the only grouping result of Wu and Tsai's method for a four-pixel block. However, as shown in Fig. 2(b), there are three kinds of possible grouping results. In order to embed data more efficiently, we have considered different grouping results in our approach. Moreover, new techniques are proposed in order to avoid the additional information needed for recording the selected grouping data. The grouping, embedding, and extracting procedures of our approach are described in the following subsections.

3.1. Pairwise grouping of a block

The host images used in our scheme are 256 gray value. Two difference values d_1 and d_2 are computed from each non-overlapping block with four neighbor pixels, say $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j+1}$, and $p_{i+1,j}$, of a given host image. The strategy of partitioning the host image into four-pixel blocks is to run through all the rows in a raster scan. The four pixels $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j+1}$, and $p_{i+1,j}$ are then renamed as p_1, p_2, p_3, and p_4, and their corresponding gray values g_1, g_2, g_3, and g_4 satisfy the condition $g_1 \le g_2 \le g_3 \le g_4$. The four-pixel block is partitioned into two two-pixel groups (g_1, g_4) and (g_2, g_3). The group which belongs to $p_{i,j}$ is defined as *group*1, and the other is defined as *group*2. In our scheme, the two group differences are computed as $(g_4 - g_1)$ and $(g_3 - g_2)$. The group difference of *group*1 is denoted as d_1, and the group difference of *group*2 is denoted as d_2. The difference value d_i (where $i = 1$ or 2) may be in the range from 0 to 255. The range from 0 to 255 is partitioned into a number of con-

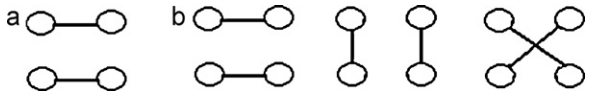

Fig. 2. Grouping results of a four-pixel block: (a) the only grouping result used by Wu and Tsai's method; (b) all possible grouping results.