Signal Processing: *Image Communication* 29 (2014) 375–384

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

A PVD-based data hiding method with histogram preserving using pixel pair matching

Jeanne Chen*

National Taichung University of Science and Technology, Department of Computer Science and Information Engineering, Taichung 406, Taiwan

ARTICLE INFO

Article history:
Received 3 March 2012
Received in revised form
31 October 2012
Accepted 9 January 2014
Available online 18 January 2014

Keywords:
Pixel value difference
Pixel pair
Difference histogram
Histogram analysis
Steganalysis

ABSTRACT

This paper proposed a Pixel Value Difference (PVD) based method to embed unequal amounts of secret information using pixel complexity. In previous PVD methods, embedding was sequential. Therefore, secret information can be easily accessed by a third party by the sequence. These methods are also easily detected by difference histogram analysis since their difference histograms showed unnatural shapes when compared to the cover image. The IMF-PVD method has a smoother and more natural difference histogram but its payload is not improved over the other PVD-based methods. In the proposed method, secret information was embedded in 2×2 embedding cells which were composed with randomized embedding units to reduce the falling-off-boundary problem and to eliminate sequential embedding. Comparison results with IMF-PVD showed that the proposed method significantly had higher payload and image quality. Furthermore, the payload size may be adjusted by reference tables and threshold. Results also showed that the embedded information is not easily detected by the difference histogram analysis and chi-square test.

1. Introduction

Data hiding is the research about embedding secret information into a digital media. The human vision cannot easily identify slight adjustments to the digital media. Therefore, a lot of applications have been proposed for embedding information into digital media such as watermarking [1], authentication [2] and data hiding [3]. Watermarking protects the intellectual property rights, authentication guarantees the integrity of transmitted data, and data hiding ensures the safe transfer of secret information. The digital media could be text, audio, image and video. In digital image, performances of data hiding are determined by the amount of data embedded and the quality of the image. When less data is embedded in the cover image, the quality of the stego image is high. A higher quality image or image close to the cover image is less likely to arouse the interest of hackers and not easy to detect by steganalysis.

The most common data hiding technique is the Least Significant Bit (LSB) replacement method [4]. The LSB method involves replacing the least significant bits with secret data. Although LSB is comparatively easy, it has lower image quality and is easily detected by LSB-based steganalysis. Chan et al. [5] proposed the Optimal Pixel Adjustment Process (OPAP) to improve the image quality of LSB replacement. However, when payload in OPAP was reduced to 1 bpp, the image quality could not be improved any further and the embedded data was also easily detected.

Both LSB and OPAP used one pixel as a unit to embed the secret data. The Pixel Pair Matching (PPM) [6] used two pixels as a unit for embedding. Examples of which are LSB matching revisited (LSB-MR) proposed by Mielikainen [7] and Exploring Modification Direction (EMD) proposed by Zhang and Wang [8]. LSB-MR made use of paired pixels and by either adding or subtracting one to embed a 4-ary digit. EMD was proposed to enhance LSB-MR by using paired pixel to embed a 5-ary digit. EMD produced higher

* Tel.: +886 4 2219 6617; fax: +886 4 2219 6341.
E-mail addresses: jeanne@nutc.edu.tw, jeanne.m.chen@gmail.com

0923-5965/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.image.2014.01.003

image quality but the largest payload is 1.16 bpp. Chao et al. [9] proposed the Diamond Encoding (DE) and manipulated a k value to embed an M-ary digit into two pixels ($M=2k^2+2k+1$). More secret data can be embedded by increasing k. Although DE improves the low payload of EMD, there are distortions in the high payload images.

Wu et al. [10] proposed the Pixel-Value Differencing (PVD) which was based on the human visual sensitivity to the complex and smooth areas of an image. Each pixel was embedded with different amounts of data by the complexity level of an image. The order of embedding by PVD is fixed. Any statistical change to the image will drastically modify the original shape of the difference histogram. Wang et al. [11] proposed the Modulus Function Pixel-Value Differencing (MF-PVD) method to embed secret data by the difference of paired pixels and a range table. Although MF-PVD can embed more information than PVD, the peak region of the difference histogram is significantly increased. The significant change is easily detectable by the difference histogram analysis. Yang et al. [12] proposed the Adaptive Edge Pixel-Value Differencing (AE-PVD) data hiding method to embed more information on the edges of an image. Although more secret data can be embedded than MF-PVD, the proposed AE-PVD integrated the OPAP method for embedding. OPAP originated from the traditional LSB replacement which can be statistically detected [13]. Joo et al. [14] proposed the IMF-PVD to improve on MF-PVD by embedding different amounts of data based on pixel pair complexity. Tests on IMF-PVD showed that the difference histogram had a shape closer to the cover image which was difficult to detect by histogram analysis. IMF-PVD can improve the problems of the shapes in the difference histogram but its payload is not higher than the MF-PVD method. The embedding order for IMF-PVD is different for the odd and even embedding areas. However, it is not secure and the hiding locations are easily located.

This paper proposed a new embedding method based on PVD which could increase the amount of embedding based on Pixel Pair Matching (PPM). In the proposed method the image will be partitioned into 2×2 blocks called embedding cells. The amount of secret data to embed is dependent on the complexity of each embedding cell. Each embedding cell has two embedding units. One of the two embedding units is chosen as the Pivot Embedding Unit (PEU), while the other is the Non-Pivot Embedding Unit (NPEU). The arrangements of PEU and NPEU are called embedding arrangements. The embedding arrangement is randomly assigned. An unauthorized person would find it hard to retrieve the embedded information due to the random assignment. The difference value of the paired pixels in PEU is calculated to determine the complexity of the pair and to determine the amount of secret bits to embed. More bits will be embedded in the complex area and less in the smooth area. The human visual is less sensitive to changes in the complex areas than the smooth areas. The aim is to embed more data, improve image quality over the IMF-PVD method, secure the embedded secret information, and prevent detection by difference histogram analysis.

The following sections of this paper will be arranged as follows: Section 2 will discuss critical elements in Joo's proposed IMF-PVD; Section 3 will discuss in detail the proposed method; Section 4 will present and analyze the experimental results; and Section 5 will present the final conclusions.

Table 1
R (lower and upper range) and the number of embedding bits.

Lower–upper	0–7	8–15	16–31	32–63	64–127	128–255
Hiding bits	3	3	4	5	6	7

2. Improved modulus function for PVD

In Joo et al.'s [14] Improved Modulus Function for PVD (IMF-PVD), unequal amount of information were embedded based on pixel values difference. The cover image I was first partitioned into unit blocks of two pixels. The difference between the two pixels of each block was calculated and evaluated for the amount of bits to be embedded in the block. A range table R determines the amount to hide (see Table 1).

As seen in Table 1, three bits could be embedded for difference values within the range from 0 to 7. The amount of embedding bits is the same for the difference values from 8 to 15. Four bits could be embedded for difference values from 16 to 31. The amount of embedding bits is based on Table 1 for the difference values from 0 to 255. Blocks with odd or even values will be processed differently. The steps for IMF-PVD embedding process is described as follows.

Input: cover image I, secret information S and range table R.

Output: length $|S|$ and stego image I'.

Step 1: Partition I into blocks of two pixels ($B_{i,1}$,$B_{i,2}$) as a set $\{B_i\}_{i=0}^{N-1}$, where N is the total number of blocks, i is the location of the block. Assume $\mathrm{mod}(i,2)=1$ as odd block, and $\mathrm{mod}(i,2)=0$ as even block.

Step 2: Calculate the absolute difference value $d_i=|B_{i,1}-B_{i,2}|$ for each of the block. From the range table R, d_i can be used to determine the number of bits to embed. We assume the number of bits to embed is k.

Step 3: Extract k bits from the secret information S. Convert the k-bits into decimal v, and calculate the value of m using the following equation:

$$m=\begin{cases} v-F_{rem}, & |v-F_{rem}|\le 2^{k-1},\\ v-F_{rem}-2^{k-1}, & (v-F_{rem})>2^{k-1},\\ v-F_{rem}+2^{k-1}, & (v-F_{rem})<-2^{k-1},\end{cases}$$

where $F_{rem}=\mathrm{mod}(B_{i,1}+B_{i,2},2^k)$.

Step 4: m is then applied to the following equation to calculate a set of new pixel values ($B'_{i,1}$, $B'_{i,2}$). The set is determined by the odd/even location i.

$$(B'_{i,1},B'_{i,2})=\begin{cases}(B_{i,1}+s_1,B_{i,2}+s_2), & \text{if } i \text{ is an odd number;}\\ (B_{i,1}+s_2,B_{i,2}+s_1), & \text{if } i \text{ is an even number;}\end{cases}$$

where $s_1=\lceil m/2\rceil$, $s_2=\lfloor m/2\rfloor$.