The Journal of Systems and Software 86 (2013) 315–323

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

Histogram-shifting-imitated reversible data hiding

Zhi-Hui Wang[a,1], Chin-Feng Lee[b,*], Ching-Yun Chang[c]

[a] Department of Software, Dalian University of Technology, Dalian, China
[b] Department of Information Management, Chaoyang University of Technology, Taichung, Taiwan
[c] Computer Laboratory, University of Cambridge, Cambridge, UK

ARTICLE INFO

Article history:
Received 1 January 2012
Received in revised form 17 May 2012
Accepted 13 August 2012
Available online 23 August 2012

Keywords:
Image authentication
Lossless watermarking
Reversible data hiding
Steganography

ABSTRACT

This paper proposes a novel reversible data hiding scheme based on the histogram-shifting-imitated approach. Instead of utilizing the peak point of an image histogram, the proposed scheme manipulates the peak points of segments based on image intensity. The secret data can be embedded into the cover image by changing the peak point pixel value into other pixel value in the same segment. The proposed method uses a location map to guarantee the correct extraction of the secret data. Since the modification of the pixel value is limited within each segment, the quality of the stego image is only related to the size of the segmentation, which means after embedding data into the cover image, it can be reused to do the multi-layer data embedding while maintaining the high quality of the final stego image. The experimental results of comparison with other existing schemes demonstrate the performance of the proposed scheme is superior to the others.

1. Introduction

Steganography is the art and science of writing hidden messages with reliability in such a way that no one can be aware of the existence of the concealed messages. The advantage of steganography over cryptography alone is that the hidden messages do not attract any attention. Therefore, cryptography protects the content of a message, but steganography can be said to protect the content of messages as well as the communicating parties. In steganography, media camouflaging information is called cover media, and the information to be hidden and communicated covertly is called the payload. The carrier with hidden payload is called stego media or covert message.

In steganographic schemes (Alattar, 2004; Carli et al., 2006; Celik et al., 2005; Chan and Cheng, 2004; Chang and Kieu, 2010; Chang and Lu, 2006; Chang et al., 2010; Diljith and Jeffrey, 2007; Fridrich et al., 2002; Kim et al., 2008; Lee et al., 2008, 2010a,b; Lee and Chen, 2010; Lin et al., 2009; Luo et al., 2011; Mielikainen, 2006; Ni et al., 2003; Tai et al., 2009; Thodi and Rodríguez, 2007; Tian, 2002, 2003; Tsai et al., 2009; Tseng and Hsieh, 2009), the cover media will undergo some permanent destruction no matter which watermarking scheme or steganographic scheme is used. Often, this distortion of the media that is caused by embedding a message is small, but it is irreversible. The original cover media cannot be recovered after the hidden messages have been extracted. In many applications, it is not the only situation providing the fidelity of cover media and stego-media perceptually equivalent; the loss of cover media is not prohibitive because even the slightest media distortion may result in an incorrect final decision. For this reason, reversible data hiding schemes have been developed and proposed in the past decade. Although reversible data hiding schemes, like other data hiding methods, introduce embedding distortions to the cover media, they are also able to remove the distortion and restore the media exactly to its original and lossless format after the embedded information has been extracted. Embedding capacity and stego-image quality are often used to evaluate the performance of reversible data hiding schemes. Nevertheless, embedding more information usually creates greater distortion in the existing methods.

Our main goal here is to present a new and simple steganographic scheme with reversibility designed for digital images. The key issues that we have considered are embedding capacity, the perceived quality of the stego-image, the complexity of secret extraction and image restoration, and security. The proposed scheme uses a reversible data hiding scheme based on histogram-shifting-imitated reversible data hiding to embed data by using the *pixel shifting strategy*. To carry a k-bit secret value each time, each segment-peak is replaced by another value that also belongs to the same segment as the segment-peak. Therefore, a small segment has a tiny change between the cover pixel and the

* Corresponding author at: Department of Information Management, Chaoyang University of Technology, Taiwan. No.168, Jifeng E. Rd., Wufeng District, Taichung, 41349, Taiwan, ROC. Tel.: +886 4 23323000 4293; fax: +886 4 23742337.
E-mail addresses: wangzhihui1017@gmail.com (Z.-H. Wang), lcf@cyut.edu.tw (C.-F. Lee), Ching-Yun.Chang@cl.cam.ac.uk (C.-Y. Chang).

[1] Supported by the Fundamental Research Funds for the Central Universities (No. 1600-852013). Supported by the Postdoctoral Science Foundation of China (No. 20110491529).

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.08.029

stego-pixel. This property offers image values that are highly perceptible to the human eye and also provides significant superiority in multiple-layer embedding without loss in image fidelity, because the segment confines the degree of pixel modification. According to the experimental results, our method produces insignificant visual distortion and provides a higher embedding capacity compared with other reversible data hiding schemes, such as Kim et al. (2008), Mielikainen (2006), Ni et al. (2003), Thodi and Rodríguez (2007), Tian (2003), and Tsai et al. (2009). In addition, the embedding or extracting process of the proposed scheme is time-efficient because of the simple function, i.e., pixel shifting mapping with a private key, which also provides the desired security.

The rest of this paper is organized as follows. The typical reversible data hiding schemes based on difference expansion and histogram shifting are briefly described in Section 2. The proposed scheme is introduced in Section 3. Experimental results and discussion are presented in Section 4. Finally, conclusions are presented in Section 5.

2. Background

Reversible data hiding schemes can be classified into two typical categories: reversible data hiding by difference expansion (called DE-based technique for short) and reversible data hiding by histogram shifting.

In the DE-based reversible watermarking method (Tian, 2002, 2003), the differences between pixel pairs are to be expandable by 1 bit of watermark data. Since the overflow or underflow problem may be invoked after data embedding, the compressed bit-stream of locations of expanded difference numbers (known as the location map) is generated to indicate whether the pixel pair is expanded or not. Tian's DE-based technique can provide an embedding capacity of almost 0.5 bit per pixel (bpp); however, there is significant degradation of image quality due to bit-replacements of gray scale pixels. Besides, the DE-based scheme is not suitable for multiple embedding, which accumulates dramatic image degradation between pixel pairs. In contrast with Tain's DE-based scheme, Ni et al. (2003) manipulated the peak and zero (or minimum) points of the histogram that corresponds to a cover image. Data are concealed by means of shifting pixels between the peak and zero (or minimum) points. The histogram-shifting-based scheme offers invisible image distortions with little auxiliary information. However, the embedding capacity is limited by the frequency of the peak-pixel values in the histogram.

To date, many reversible data hiding schemes (Alattar, 2004; Celik et al., 2005; Chan and Cheng, 2004; Chang and Kieu, 2010; Chang and Lu, 2006; Chang et al., 2010; Diljith and Jeffrey, 2007; Fridrich et al., 2002; Kim et al., 2008; Lee et al., 2008, 2010a,b; Mielikainen, 2006; Ni et al., 2003; Tai et al., 2009; Thodi and Rodríguez, 2007; Tian, 2002, 2003; Tsai et al., 2009; Tseng and Hsieh, 2009) that extend the DE-based scheme or the histogram-based scheme have been developed to enhance hiding capacity or reduce the distortion of the stego-image. Alattar (2004) extended Tain's scheme using a vector of cover pixels instead of a pixel pair to increase the hiding ability. Thodi and Rodríguez (2007) proposed a prediction-error expansion (PE) scheme which utilizes a predictive method to generate the predictive pixel of the cover pixel, and then a secret bit is embedded by expanding the difference error between the predictive pixel and the cover pixel. Tsai et al. (2009) combined a linear prediction technique and histogram shifting to improve the embedding capacity of Ni et al.'s scheme. The cover image is divided into many sequential, non-overlapping blocks. The secret data are embedded into the difference values between the center pixel and others pixels in a block. Ni et al. (2003) offered a multi-level, reversible, data hiding scheme to achieve large hiding capacity. Tseng and Hsieh (2009) proposed a reversible data hiding scheme that extended the scheme proposed by Tian (2002, 2003). Their scheme was based on perdition-error expansion, which differs from most DE-based schemes in that the location map is not required.

3. Proposed scheme

In this paper, we are proposing a histogram-shifting-imitated reversible data hiding scheme. The proposed scheme divides the range of the intensity into non-overlapping segments, and finds the peak point pixel value having the highest number of occurrences in the histogram of each segment. Only peak pixel values are embeddable, except for the first peak pixel value that is encountered within a segment. Each embeddable segment-peak can carry k-bit data where 2^k is the segment size. All non-peak values are unembeddable. A location map LM_i corresponding to the ith segment is a bit map in which bit "1" indicates that the pixel is the segment-peak point, and bit "0" indicates the others. The bit map can be compressed losslessly by a JBIG1 compression (JBIGI, 2010). Details of the embedding phase are presented below.

The intensity of an image pixel is expressed within a given range between a minimum and a maximum, inclusive. For a grayscale image, this range is represented in a discrete way as a range from 0 (total absence, black) and 255 (total presence, white). Let PV be an intensity set corresponding to an image and $|PV|$ be the size of the image intensity set. Let I and I' stand for a cover image and a stego-image, respectively, with a size of $H \times W$ where H and W denote the height and width of the cover image and the stego-image. Let $I(x, y)$ and $I'(x, y)$ be denoted as a cover pixel value located at the position (x, y) of the cover image I and stego-pixel I', where $1 \le x \le W$, $1 \le y \le H$; both $I(x, y)$ and $I'(x, y) \in PV$.

Divide the PV set into N uniformly equal-sized segments S_i for $i = 1, 2, \ldots, N$. Let $|PV|$ stand for the size of the PV set; then segment size defined as the number of elements in each segment is $|PV|/N$. Thus, if a cover image I is an 8-bit grayscale image, then $PV = \{0, 1, 2, \ldots, 255\}$ and $|PV| = 256$, for instance. Assume that $N = 4$, four segments for an 8-bit grayscale image I are $S_1 = \{0, 1, 2, \ldots, 63\}$, $S_2 = \{64, 65, 66, \ldots, 127\}$, $S_3 = \{128, 129, 130, \ldots, 191\}$, and $S_4 = \{192, 193, 194, \ldots, 255\}$, respectively, and the segment size is 64. In typical practical applications, payload data are embedded and extracted as binary strings, thus secret message $SM = \{s_b | s_b \in \{0, 1\}$, for $b = 1, 2, \ldots, k \times l\}$, where $k \times l$ is the length of SM. For achieving the purpose that one k-bit secret value at a time is to be embedded into an embeddable segment-peak, the secret message will first be rearranged to form a sequence of decimal values and each value is converted from k-bit data. Let s_d' stand for the transformed decimal value which falls within the range of $[0, 2^k - 1]$ and the original secret message of binary representation is thus transformed as $SM^{(k)}$ and represented as:

$$SM^{(k)} = \{s_d | s_d \in \{0, 1, 2, \ldots, 2^k - 1\}, \quad \text{for} \quad d = 1, 2, \ldots, l\}.$$

The mapping between secret message SM and the transformed message $SM^{(k)}$ can be derived as follows:

$$s_d = \sum_{j=1}^{k} s_{(b-1)k+j} \times 2^{k-j} \quad \text{for} \quad b = 1, 2, \ldots, k \times l \quad \text{and} \quad d = 1, 2, \ldots, l. \tag{1}$$

Next, each secret value sd is to be hidden by exploiting the following *pixel shifting strategy*. A secret key $Key^{(i)}$, which is a random number created by the sender, is used as the seed to generate a mapping of segment S_i among a cover pixel value, one k-bit of decimal data and a stego-pixel value. The inputs are an embeddable peak pixel and one k-bit of decimal secret data, s_d; the output is a corresponding pixel belonging to the same segment. Let us call the