Contents lists available at ScienceDirect

The Journal of Systems and Software

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

Controversy Corner

A high stego-image quality steganographic scheme with reversibility and high payload using multiple embedding strategy

The Duc Kieu, Chin-Chen Chang [*]

Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan, ROC

ARTICLE INFO

Article history:
Received 2 November 2008
Received in revised form 7 April 2009
Accepted 9 May 2009
Available online 18 May 2009

Keywords:
Reversible data embedding
Difference expansion (DE)
Information hiding
Steganography

ABSTRACT

Tian's method is a breakthrough reversible data embedding scheme with high embedding capacity measured by bits per pixel (bpp) and good visual quality measured by peak signal-to-noise ratio (PSNR). However, the embedding capacity and visual quality of this method can be significantly improved. Thus, we propose a simple reversible steganographic scheme in spatial domain for digital images by using the multiple embedding strategy. The proposed method horizontally and vertically embeds one secret bit into one cover pixel pair. The experimental results show that the proposed reversible steganographic method achieves good visual quality and high embedding capacity. Specifically, with the one-layer embedding, the proposed method can obtain the embedding capacity of more than 0.5 bpp and the PSNR value greater than 54 dB for all test images. Especially, with the five-layer embedding, the proposed method has the embedding capacity of more than 2 bpp and the PSNR value higher than 52 dB for all test images. Therefore, the proposed method surpasses many existing reversible data embedding methods in terms of visual quality and embedding capacity.

1. Introduction

The rapid advances of network technologies and digital devices make information exchange fast and easy. However, distributing digital data over public networks such as the Internet is not really secure due to copy violation, counterfeiting, forgery, and fraud. Therefore, protective methods for digital data, especially for sensitive data, are highly demanded. Traditionally, secret data can be protected by cryptographic methods such as DES (Davis, 1978) or RSA (Rivest et al., 1978). The drawback of cryptography is that cryptography can protect secret data in transit, but once they have been decrypted, the content of the secret data has no further protection (Cox et al., 2007). In addition, cryptographic methods do not hide the very existence of the secret data. Alternatively, confidential data can be protected by using information hiding techniques. Information hiding embeds secret information into cover objects such as written texts, digital images, adios, and videos (Bender et al., 1996). For more secure, cryptographic techniques can be applied to an information hiding scheme to encrypt the secret data prior to embedding.

In general, information hiding (also called data hiding or data embedding) technique includes digital watermarking and steganography (Petitcolas et al., 1999). Watermarking is used for copyright protection, broadcast monitoring, transaction tracking, etc. A watermarking scheme imperceptibly alters a cover object to embed a message about the cover object (e.g., owner's identifier) (Cox et al., 2007). The robustness (i.e. the ability to resist certain malicious attacks such as common signal processing operations) of digital watermarking schemes is critical. In contrast, steganography is used for secret communications. A steganographic method undetectably alters a cover object to embed a secret message (Cox et al., 2007). Thus, steganographic methods can hide the very presence of covert communications. Information hiding techniques can be performed in three domains (Bender et al., 1996), namely, spatial domain (Zhang and Wang, 2006), compressed domain (Pan et al., 2004), and frequency (or transformed) domain (Kamstra and Heijmans, 2005; Wu and Frank, 2007; Zhou et al., 2007). Each domain has its own advantages and disadvantages in terms of embedding capacity, execution time, storage space, etc.

Two main factors that really affect an information hiding scheme are visual quality of stego images (also called visual quality for short), embedding capacity (or payload). An information hiding scheme with low image distortion is more secure than that with high distortion because it does not raise any suspicions of adversaries. The second important factor is embedding capacity (also called capacity for short). An information hiding scheme with high payload is preferred because more secret data can be transferred. However, embedding capacity is inversely proportional to visual quality. Thus, the tradeoff between the two factors above varies from application to application, depending on users' requirements

[*] Corresponding author. Address: Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.
E-mail addresses: ktduc0323@yahoo.com.au (T.D. Kieu), ccc@cs.ccu.edu.tw (C.-C. Chang).

0164-1212/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2009.05.028

and application fields. Consequently, different techniques are utilized for different applications. Therefore, a class of data hiding schemes is needed to span the range of possible applications.

Embedding the secret data into an image causes the degradation of image quality. Even though small image distortion is unacceptable in some applications such as law enforcement, military image systems, and medical diagnosis. If a data embedding scheme is irreversible (also called lossy), then a decoder can extract secret data only and the original cover image cannot be restored. In contrast, a reversible (also called invertible, lossless, or distortion-free) data embedding scheme allows a decoder to recover the original cover image completely upon the extraction of the embedded secret data. A reversible data hiding scheme is suitably used for some applications such as the healthcare industry and online content distribution systems.

To our best knowledge, the first reversible data embedding scheme was proposed in 1997 (Barton, 1997). Macq (2000) extended the patchwork algorithm (Bender et al., 1996) to achieve the reversibility. This method encounters the underflow and overflow problem (i.e., grayscale pixel values are out of the allowable range $[0, 255]$). Honsinger et al. (2001) used modulo arithmetic operation to resolve the underflow and overflow problem. Consequently, Honsinger et al.'s method raises the salt-and-pepper effect. Fridrich et al. (2001) also proposed the reversible data embedding method for the authentication purpose so the embedding capacity of this method is low. Later on, De Vleeschouwer et al. (2003) proposed the circular interpretation of bijective transforms to face the underflow and overflow problem. However, the salt-and-pepper problem still remains in De Vleeschouwer et al.'s method. As a whole, the problem with the aforementioned methods is either the salt-and-pepper problem or low embedding capacity.

Tian (2003) proposed the reversible data embedding scheme with high embedding capacity and good visual quality of embedded images (also called stego images). Tian's scheme is of a fragile technique meaning that the embedded data will be mostly destroyed when some common signal processing operations (e.g., JPEG compression) are applied to a stego image. Tian's method uses the difference expansion (DE) operation to hide one secret bit into the difference value of two neighboring pixels. Thus, the embedding capacity of the DE method is at most 0.5 bpp for one-layer embedding. Tian also suggested the multiple-layer embedding to achieve higher embedding capacity. Alattar (2004) generalized Tian's method to embed $n-1$ secret bits into a group of n cover pixels. Thus, the embedding capacity of Alattar's method is at most $(n-1)/n$ bpp. Kamstra and Heijmans (2005) also improved Tian's method in terms of visual quality at low embedding capacities. The maximum embedding capacity of Kamstra and Heijmans' method is 0.5 bpp. Chang and Lu (2006) exploited Tian's method to achieve the average embedding capacity of 0.92 bpp and the average PSNR of 36.34 dB for one-layer embedding. Next, Thodi and Rodriquez (2007) improved Tian's scheme and proposed the novel method called prediction error expansion (PEE) embedding. The PEE method embeds one secret bit into one cover pixel at a time. However, at its maximum embedding capacity (i.e., around 1 bpp), the visual quality of the PEE method is always less than 35 dB for all test images. Then, Kim et al. (2008) improved Tian's method by simplifying the location map to achieve higher embedding capacity while keeping the image distortion the same as the original DE method. Lou et al. (2009) improved the DE method by proposing the multiple layer data hiding scheme. Lou et al.'s method reduces the difference value of two neighboring cover pixels to enhance the visual quality. The problem with the aforementioned schemes is that the PSNR value becomes very low (i.e., less than 30 dB) at high embedding capacity (i.e., more than 1 bpp).

From the aforementioned considerations, with the purpose of improving the visual quality and the embedding capacity of Tian's method, we propose a novel reversible data embedding scheme with good visual quality and high embedding capacity by using multiple embedding strategy. The proposed method horizontally and vertically embeds one secret bit into one cover pixel pair of a grayscale cover image. The details of the proposed method are described in Section 3. The rest of this paper is organized as follows. Tian's method is briefly reviewed in Section 2. The proposed scheme is detailed in Section 3. The experimental results and discussions are shown in Section 4. Some conclusions are drawn in Section 5.

2. Tian's method

Tian (2003) proposed a reversible data embedding using a difference expansion (DE). Tian's method embeds a secret bit stream S with the length LS into a grayscale cover image O sized $H \times W$ to obtain the embedded image X. Specifically, the cover image O is scanned in raster scan order (i.e., from left to right and top to bottom) to group two neighboring pixels into a pixel pair (x, y). Next, each secret bit b in S is embedded into the difference value d of each cover pixel pair (x, y) at a time until the whole secret bit stream S is embedded into O. The DE method is detailed as below.

2.1. The embedding phase

Firstly, the integer average m and the difference value d of x and y are computed by

$$m = \lfloor (x+y)/2 \rfloor, \tag{1}$$

$$d = x - y, \tag{2}$$

where the notation $\lfloor x \rfloor$ is the floor function meaning the greatest integer less than or equal to x. Secondly, the secret bit b is embedded into d by the difference expansion (DE) operation to obtain the new difference value d' as follows

$$d' = 2 \times d + b. \tag{3}$$

Finally, the embedded pixel pair (x', y') (i.e., embedded with a secret bit) is calculated by

$$x' = m + \lfloor (d'+1)/2 \rfloor, \tag{4}$$

$$y' = m - \lfloor d'/2 \rfloor. \tag{5}$$

The above embedding process is repeatedly applied to embed each secret bit b in S into each cover pixel pair (x, y) in O until the whole secret bit stream S is completely embedded into O to obtain the embedded image X. Then, the embedded image X is sent to the expected receivers.

2.2. The extracting phase

With the received embedded image X, a decoder can extract each embedded secret bit b of S and recover each original cover pixel pair (x, y) in O from each embedded pixel pair (x', y') in X as follows. First, the integer average m' and the difference value d' are computed by using (1) and (2). That is, $m' = \lfloor (x'+y')/2 \rfloor$ and $d' = x' – y'$. Second, the embedded secret bit is extracted by $b = LSB(d')$, where $LSB(x)$ is the function taking the least significant bit (LSB) of x. The extracted secret bits b's are concatenated to form the original secret bit stream S. Next, according to (3), the original difference value is calculated by $d = \lfloor d'/2 \rfloor$. Then, the original cover pixel pair (x, y) is restored by using (4) and (5). That is, $x = m' + \lfloor (d+1)/2 \rfloor$ and $y = m' - \lfloor d/2 \rfloor$. The restored pixel pairs (x, y)'s are collected to form the original cover image O.

It is noted that the DE operation used in (3) can cause the underflow and overflow problem. That is, the embedded pixel pair