The Journal of Systems and Software 85 (2012) 2395–2404

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

High capacity reversible data hiding scheme based upon discrete cosine transformation

Yih-Kai Lin*

Department of Computer Science, National Pingtung University of Education, No. 4-18 Minsheng Rd., Pingtung City 90003, Taiwan

ARTICLE INFO

Article history:
Received 2 November 2011
Received in revised form 7 January 2012
Accepted 8 May 2012
Available online 6 June 2012

Keywords:
DCT
Data hiding
Histogram shifting

ABSTRACT

In this paper, we propose a reversible data hiding scheme based on the varieties of coefficients of discrete cosine transformation of an image. Cover images are decomposed into several different frequencies, and the high-frequency parts are embedded with secret data. We use integer mapping to implement our 2-dimensional discrete cosine transformation. Thus, the image recovered from the modified coefficients can be transformed back to the correct data-hidden coefficients. Since the distribution of 2-dimensional DCT coefficients looks close to Gaussian distribution centralized at zero, it is a natural candidate for embedding secret data using the histogram shifting approach. Thus, our approach shifts the positive coefficients around zero to the right and the negative coefficients around zero to the left in order to leave a space to hide the secret data. The experimental comparisons show that, compared to Chang et al. and Lin et al.'s method, the embedding capacity and quality of the stego-image of the proposed method is a great improvement.

1. Introduction

In reversible data hiding techniques (Yang et al., 2011; Chang et al., 2011), after the embedded secret data are extracted, the cover images can be completely recovered from the stego-images. The reversible data embedding approach can be classified into three categories. They are the spatial-domain methods, frequency-domain, and other compression types, including vector quantization and JPEG. In the spatial-domain approach, the secret data are embedded into the pixels of a given cover image. In the frequency-domain approach, the cover image is transformed to frequency coefficients, and the secret data is embedded into these coefficients. In the compression types, e.g., vector quantization, the secret data is embedded into the unused code space. The simple spatial-domain approach involves hiding the secret data in the least-significant-bit (LSB) of the pixels of an image (Celik et al., 2002; Chan and Chen, 2004; Ker, 2007; Li et al., 2009). The LSB substitution method is simple to implement and easily obtains high hiding capacity, but it is also easily detected by human vision and programs. In 2002, Celik et al. (2002) proposed a generalized least significant bit method. In 2003, Tian (2003) proposed a difference expansion data hiding approach. In his method, the difference values of two neighboring pixels are calculated. The secret data is embedded in the difference values. In 2006, Ni et al. (2006) proposed a reversible hiding scheme to utilize the histogram of the pixels of the cover image. Their method shifts the part of the histogram between the peak point and the minimum point to the right side to create a space for hiding secret data. In these histogram-based data hiding schemes, the maximal hiding capacity is dependent on the number of pixels in the peak point of the histogram.

To look for the proper pixels for hiding data without being noticed by humans, transform-based schemes are another choice. In these schemes, cover images are transformed by some kind of frequency-oriented mechanism, e.g., *discrete cosine transform* (*DCT*) and *discrete wavelet transform* (*DWT*). Then, the secret data are embedded into the frequency-form images by modifying the coefficients. In 2001, Fridrich et al. (2001) proposed an LSB-based reversible data hiding scheme. The secret data is embedded in the LSB of the quantized DCT coefficients. In 2002, Chang et al. (2002) presented a steganographic method based on the JPEG format. They modify the quantization table to get quantized DCT coefficients and to hide the secret data in the least-two-significant bits of the middle-frequency of the quantized DCT coefficients. To improve the embedding capacity, Tseng and Chang (2004) proposed a high capacity hiding method based on the adaptive least-significant bit substitution method. Later, Chang et al. (2007) presented a reversible hiding scheme for hiding secret data in quantized DCT coefficients. In 2010, Lin and Shiu (2010) extended Chang et al.'s idea (2002, 2007) and presented a high capacity data hiding strategy that also embeds data into the coefficients in the middle frequency of the quantized DCT coefficients. That is, Chang et al.

* Tel.: +886 8 722 6141x33559; fax: +886 8 721 5034.
E-mail address: yklin@mail.npue.edu.tw

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.05.032

(2002, 2007), Tseng and Chang (2004), Lin and Shiu (2010) utilize the redundancy in the quantized DCT coefficients. In other words, their method modifies the quantization stage of JPEG compression and stores the stego-image in JPEG format.

Since human vision is insensitive to the varieties of high-frequency components of an image, the secret data can be hidden in the high-frequency parts of an image. To improve the quality of the stego-image, we utilize the concept of decomposition of images. In the proposed method, images are decomposed into several different frequencies, of which the high-frequency parts contain hidden data. A similar idea has been used to compress images in JPEG. In JPEG compression, the information loss due to fixed-precision data storing and computing in the domain transformation stage and also in the quantization stage creates a huge compression rate.

In this paper, we propose a method which directly embeds secret data into the DCT coefficients of the cover image. Since the distribution of 2-dimensional DCT coefficients looks close to Gaussian distribution centralized at zero, it is a natural candidate for embedding secret data using the histogram shifting approach. Thus, our approach shifts the positive coefficients around zero to the right and the negative coefficients around zero to the left in order to leave a space to hide secret data. Compared with Ni et al.'s (2006) method, our method does not need to restore the peak point and minimum point for retrieving the hidden data. The overhead of sending this information to the retrieving end is eliminated. The major problem of hiding data in the DCT coefficients is that when we transform the modified DCT coefficients back to the spatial-domain, because the pixels of the image are stored in integer form, rounding errors will be added into the spatial-domain image, and thus cannot be transformed back to the correct modified DCT coefficients when extracting the embedded data. We use one of the forms of integer mapping Hao and Shi (2001) to implement our DCT transformation which maps integer to integer for solving the problem of rounding errors. Thus, if the modified DCT coefficients remain as integers, the image recovered from the modified coefficient can be transformed again to the correct modified coefficient, and the embedded data can be extracted. Instead of hiding the secret data in the quantized coefficients, our method directly embeds the secret data into the pixels of the cover image. Compared with the methods (Chang et al., 2002, 2007; Tseng and Chang, 2004; Lin and Shiu, 2010) mentioned above which embed secret data into quantized spatial-domain coefficients, our stego-image stays in its raw image form instead of some special form of quantized coefficients e.g., JPEG-formatted.

2. Preliminaries

An $M \times N$ digital image is defined by function $f : (\mathbb{N}, \mathbb{N}) \mapsto \mathbb{N}$ where $\mathbb{N}$ denotes the set of nature numbers. For convenience, a traditional matrix is used to denote a digital image: $\boldsymbol{X} = [x_{i,j}]$ where $x_{i,j} = f(i, j)$ for $1 \le i \le M$ and $1 \le j \le N$. A real number b can be rounded (denoted by angled brackets $\langle \cdot \rangle$) to an integer $\langle b \rangle$ by rounding-down, rounding-up, or by using some other methods. Given an $N \times N$ matrix $\boldsymbol{A}$, the kth order *leading principal* of $\boldsymbol{A}$ is a sub-matrix formed by deleting the last $N-k$ columns, say column $k+1, k+2, \ldots, N$ and the last $N-k$ rows, row $k+1, k+2, \ldots, N$. The kth order *leading principal minor* of $\boldsymbol{A}$ is the determinant of a $k \times k$ principal sub-matrix. The data needing to be hidden are called the *secret data* and are a sequence of bits denoted by $\mathfrak{M}$. The *cover image* is the image for carrying the hidden secret data. The *stego-image* is the image containing the hidden secret data. The *image quality* refers to the similarity of the cover image and the stego-image. The *capacity* refers to the total bits of hidden secret data.

3. The proposed scheme

The proposed reversible data hiding scheme based on discrete cosine transformation is described in this section. A given cover image $\boldsymbol{X}$ is first transformed into a sequence of DCT coefficients $\boldsymbol{Y}$. Then we present a hiding algorithm to embed the secret data into $\boldsymbol{Y}$, benefiting from the centralization of the frequency coefficients of images. The secret data $\mathfrak{M}$ is directly embedded in the high-frequency coefficients part of $\boldsymbol{Y}$ to produce the modified frequency-domain image $\boldsymbol{Y}'$. Then the modified frequency-domain image $\boldsymbol{Y}'$ is transformed back to the spatial-domain to get the stego-image $\boldsymbol{X}'$. Because the general DCT coefficients are in the real domain, one major problem is to ensure that the secret data can be extracted when the stego-images are stored in a small range of integers, e.g., 0 to 255. That is, with the unavoidable error in floating-point number calculation with fixed-precision computing architecture, the image $\boldsymbol{X}'$ in the spatial domain needs to be transformed exactly back to $\boldsymbol{Y}'$. Therefore, the secret data $\mathfrak{M}$ and original cover image $\boldsymbol{Y}$ can be extracted from $\boldsymbol{Y}'$. Our proposed scheme is shown in Fig. 1.

3.1. Reversible decomposition

As mentioned above, cover image $\boldsymbol{X}$ is transformed into coefficient matrix $\boldsymbol{Y} = \boldsymbol{AX}$ by transform matrix $\boldsymbol{A}$. Based on the theorems from Hao and Shi (2001), matrix $\boldsymbol{A}$ has a factorization $\boldsymbol{PS}_N \boldsymbol{S}_{N-1} \cdots \boldsymbol{S}_0$ if and only if the minors of the leading principal sub-matrices of $\boldsymbol{A}$ are all 1s, where $\boldsymbol{P}$ is a permutation matrix, $\boldsymbol{S}_m = \boldsymbol{I} + \boldsymbol{e}_m \boldsymbol{s}_m^T$ for $m = 1, 2, 3, \ldots, N$, $\boldsymbol{S}_0 = \boldsymbol{I} + \boldsymbol{e}_N \boldsymbol{s}_0^T$, $\boldsymbol{e}_m$ is the mth column vector of the identity matrix, and $\boldsymbol{I}$ is the identity matrix. Consider an integer column vector $\boldsymbol{x}$ of $\boldsymbol{X}$; the linear transformation $\boldsymbol{Ax} = \boldsymbol{y}$ can be computed by $\boldsymbol{PS}_N \boldsymbol{S}_{N-1} \cdots \boldsymbol{S}_1 \boldsymbol{S}_0 \boldsymbol{x} = \boldsymbol{y}$ where $\boldsymbol{y}$ is a column vector of $\boldsymbol{Y}$. Consider the linear transformation $\langle \boldsymbol{S}_m \boldsymbol{x} \rangle = \boldsymbol{y}$ for $m = 0, 1, 2, 3, \ldots, N$,

$$
\langle \boldsymbol{S}_m \boldsymbol{x} \rangle = \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \langle s_{m,1} \rangle & \cdots & 1 & \cdots & \langle s_{m,N} \rangle \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_m \\ \vdots \\ x_N \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ \langle \sum_{i=1}^{m-1} s_{m,i} x_i \rangle + x_m + \langle \sum_{i=m+1}^{N} s_{m,i} x_i \rangle \\ \vdots \\ x_N \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_m \\ \vdots \\ y_N \end{bmatrix} = \boldsymbol{y}
$$

where $\langle\rangle$ denotes integer conversion. The reverse transformation is