Pattern Recognition 42 (2009) 1597 – 1603

Contents lists available at ScienceDirect

Pattern Recognition

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

A lossless data embedding technique by joint neighboring coding

Chin-Chen Chang[a,*], The Duc Kieu[a], Wen-Chuan Wu[b]

[a]Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC
[b]Department of Computer and Information Science, Aletheia University, Tamsui Taipei 25103, Taiwan, ROC

ARTICLE INFO

Article history:
Received 24 January 2007
Received in revised form 16 October 2008
Accepted 27 November 2008

Keywords:
Information hiding
Reversible data embedding
Vector quantization

ABSTRACT

Information hiding methods are currently exploited by many researchers for various applications. Proposing an efficient and feasible information hiding method is valuable. This paper presents a new reversible information hiding method for vector quantization (VQ)-compressed grayscale images by using joint neighboring coding (JNC) technique. The proposed method embeds secret data by using the difference values between the current VQ-compressed index and left or upper neighboring indices. The experimental results show that the proposed method achieves the best visual quality of reconstructed images compared with the two related works. In addition, the proposed method obtains as high embedding capacity as Lin and Chang's method, followed by Yang et al.'s method. As for execution speed, Yang et al.'s method is fastest, followed by the proposed method, and then Lin and Chang's method. With respect to bit rate, the proposed method has a little higher bit rate in comparison with the two related works.

1. Introduction

Secure communications can be protected by using cryptographic methods and steganographic methods. Cryptographic methods, however, do not hide the existence of secret communications in fact. In contrast, steganographic methods make secret communications invisible (or imperceptible). That is, they hide the very existence of secret communications. In general, information hiding (also called data hiding or data embedding) technique includes digital watermarking and steganography [2,9]. Digital watermarking techniques are suitable for applications relevant to the protection of digital contents where the amount of secret data, such as ownership information, needed to be embedded into cover media is small. 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 to embed secret data into cover media imperceptibly for the purpose of secret communications. Cover media can be written texts, images, digital sound files, videos, and so on. For security purpose, cryptographic techniques can be applied to an information hiding scheme to make secret communications more secure. Secret data, for example, can be encrypted using cryptographic techniques before the data embedding.

Three factors that really affect an information hiding scheme are visual quality (or image distortion), embedding capacity (or payload), and efficiency [9]. An information hiding scheme with low image distortion is more secure than that with high distortion because it does not raise any suspicions. Therefore, image quality factor is the first important one. The second important factor is embedding capacity (called capacity for short). An information hiding scheme with high payload is preferred because more secret data can be transferred. In nature, embedding capacity is inversely proportional to visual quality. That is, if capacity is increased then visual quality is reduced. The tradeoff between the two factors above is made by users, depending on users' purposes and application fields.

The third worthy factor needed to consider is the efficiency of an information hiding scheme. The efficiency refers to the simplicity of the embedding and extracting algorithms and the small transmitted data quantity. Simple embedding and extracting algorithms (i.e. low complexity) are preferred because their execution speed is fast. The small transmitted quantity is achieved by using data embedding methods with a low bit rate and using compressed cover media such as compressed images. Actually, efficient data embedding methods are particularly meaningful to large-scale and real-time applications on the Internet where transmission speed is critical. Furthermore, data embedding methods with the small transmitted data quantity contribute to avoiding the network congestion.

The tradeoff among image distortion, embedding capacity, and efficiency varies from application to application. Consequently, different techniques are employed for different applications. Three embedding classes are information hiding techniques in spatial domain [1,2,11], in transformed domain (e.g. using DCT, DFT, or DWT) [5], and in compressed domain [3,4,6,7,10]. Information hiding techniques in spatial domain/transformed domain embed secrets by modifying

[*] Corresponding author. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.
E-mail addresses: ccc@cs.ccu.edu.tw (C.-C. Chang), ktduc0323@yahoo.com.au (T.D. Kieu), au4387@email.au.edu.tw (W.-C. Wu).

0031-3203/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2008.11.040

spatial characteristics (i.e. pixel amplitude)/transformed coefficients of cover media. These techniques, however, are not robust enough to lossy compressions. Information hiding techniques in compressed domain (such as using vector quantization, VQ, compression method [8]) can make the transmitted data smaller [6] although there is a bit less data quantity to be embedded.

In some sense, information hiding schemes can be further categorized into two types, namely irreversible data embedding schemes and reversible (or lossless) data embedding schemes. With respect to an irreversible data embedding scheme, receivers can extract secret data only, no cover media restoration. In contrast, with a reversible data embedding scheme, receivers can extract secret data and recover cover media completely [10]. A reversible hiding scheme is suitably used for the healthcare industry and online content distribution systems.

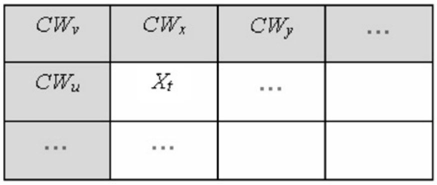
By integrating an information hiding method with the VQ compression, some data embedding methods were proposed such as Lin and Wang's method [7], and Jo and Kim's method [4]. These methods both embed secrets by modifying VQ-compressed indices. However, these methods are irreversible, low embedding capacity, and have a little high image distortion. To achieve reversibility, Yang et al. [10] proposed a new information hiding method in VQ-compressed domain by using a modified fast correlation based VQ (MFCVQ) technique. However, this method achieves very low payload. To improve Yang et al.'s weakness, Lin and Chang [6] proposed an information hiding method in the VQ-compressed domain by using dissimilar pairs of the codebook. But this method is only nearly reversible.

Achieving low image distortion (i.e. it reduces the suspicion of adversaries), high data embedding capacity, reversibility, and efficiency are the desires of most information hiding system designers. Since no method is applicable of achieving all these goals, a class of data hiding schemes is needed to span the range of possible applications. From the aforementioned considerations, with the purpose of improving the visual quality of reconstructed images, achieving high embedding capacity and fast execution speed at the cost of a little higher bit rate, we propose a fully lossless data embedding scheme for the steganographic application (i.e. secret communications) by using joint neighboring coding (JNC) for VQ-compressed images. The proposed method embeds secrets into VQ-compressed indices by using the difference values between the current index and left or upper neighboring indices. The rest of this paper is organized as follows. The review of some previous works is presented in Section 2. The proposed scheme is explored in Section 3. Section 4 presents the experimental results and discussions. Some conclusions are made in Section 5.

2. Related works

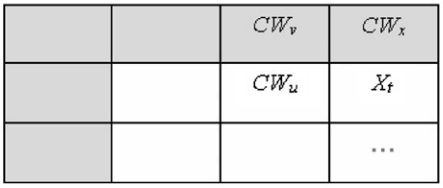
VQ is a lossy data compression method based on the principle of block coding. First, the representative codebook C containing Nk-dimensional codewords CW_i's is generated by using the LBG clustering algorithm [8], where $i=0,1,\ldots,N-1$. At the beginning of the embedding process, an $R \times S$-sized grayscale image I is divided into non-overlapping $r \times s$ image blocks X_t's, where $r \times s = k$. Then, each image block is encoded to an index value i of a codeword CW_i. Finally, put these index values into the $(R/r) \times (S/s)$-sized index table $P=\{p_{h,c}\}$ at the position $(h,\, c)$ (i.e. $p_{h,c}=i$). As for block decoding, the original image I is easily reconstructed from the index table P and the codebook C by using the simple table-lookup operation.

In both Yang et al.'s method [10] and Lin and Chang's method [6], the original image blocks located at the first row and the first column of the cover image I are encoded by using the ordinary VQ. These VQ-compressed indices are kept unchanged during the data embedding process. This means that there is no data embedding in this area. This area is called the seed area.



CW_v	CW_x	CW_y	…
CW_u	X_t	…	
…	…		

Fig. 1. Four encoded neighbors of X_t.



		CW_v	CW_x
		CW_u	X_t
			…

Fig. 2. Three encoded neighbors of X_t.

2.1. Yang et al.'s scheme

For the embedding process, from the cover image I and the codebook C, the secret data are embedded by using the MFCVQ encoding as follows. The current 4×4 image block X_t is encoded by using its four neighboring encoded 4×4 image blocks CW_u, CW_v, CW_x, and CW_y as shown in Fig. 1. When the block X_t is located at the last column of I, it is encoded by using its three neighboring encoded 4×4 image blocks CW_u, CW_v, and CW_x as shown in Fig. 2.

Firstly, calculate the Euclidean distances between the block X_t and its four neighboring encoded 4×4 image blocks $d_u = \mathrm{D}(CW_u, X_t)$, $d_v = \mathrm{D}(CW_v, X_t)$, $d_x = \mathrm{D}(CW_x, X_t)$, and $d_y = \mathrm{D}(CW_y, X_t)$, where

$$\mathrm{D}(X,Y) = \sqrt{\sum_{i=1}^{16}(x_i - y_i)^2}, \quad X = (x_1, x_2, \ldots, x_{16}) \quad \text{and} \quad Y = (y_1, y_2, \ldots, y_{16}). \tag{1}$$

Secondly, find the smallest distance $d_{min} = \min\{d_u, d_v, d_x, d_y\}$. Thirdly, if $d_{min} \leqslant$ the predefined threshold TH , then the current block X_t is *embeddable*. Otherwise, the current block X_t is *non-embeddable*.

For an *embeddable* X_t, read the next secret bit b_t. Next, send a flag bit "0" to the binary code stream. Then, calculate the mean vector $C_m = (CW_u + CW_v + CW_x + CW_y)/4$. Find the best-matched code vector CW_{mb} of C_m out of $\{CW_u, CW_v, CW_x, CW_y\}$. If the secret bit $b_t = 0$, then the block X_t is encoded by the code vector CW_{mb}. Otherwise (i.e. $b_t = 1$), find the best-matched code vector CW_X of the block X_t out of $\{CW_u, CW_v, CW_x, CW_y\}$. The block X_t is then encoded as the code vector CW_X. For a *non-embeddable* X_t, send a flag bit "1" to the binary code stream. Next, find the best-matched code vector CW_{mb} of the block X_t out of the whole codebook C and encode block X_t by the code vector CW_{mb}. There is no secret data embedding when X_t is non-embeddable.

2.2. Lin and Chang's scheme

In Lin and Chang's scheme, they used the principal component analysis (PCA) algorithm [6] to sort the codebook C so that they can use dissimilar pairs for the embedding process. First, dissimilar pairs $(CW_i,\ CW_{((N-2)/2)+i})$'s, where $1 \leqslant i \leqslant (N-2)/2$, are created. This means that the first and the last codewords CW_0 and CW_{N-1} are not used in the VQ encoding process. The codeword CW_i located at the position $(h,\, c)$ in the VQ image is denoted as $CW_i^{(h,c)}$. Second,