Expert Systems with Applications 40 (2013) 1132–1142

Contents lists available at SciVerse ScienceDirect

Expert Systems with Applications

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

Color local complexity estimation based steganographic (CLCES) method

Blanca E. Carvajal-Gamez, Francisco J. Gallegos-Funes *, Alberto J. Rosales-Silva

National Polytechnic Institute of Mexico, Mechanical and Electrical Engineering Higher School, Av. IPN s/n, ESIME SEPI-Electronica, Lindavista, 07738 Mexico, D.F., Mexico

ARTICLE INFO

Keywords:
Steganographic method
Local complexity estimation
Steganalysis
Color spaces

ABSTRACT

In this paper we present the color local complexity estimation based steganographic (CLCES) method that is able of both preventing visual degradation and providing a large embedding capacity. A preprocessing stage is applied in the proposed scheme to improve the steganography security. The embedding capacity of each pixel is determined by the local complexity of the cover image, allowing good visual quality as well as embedding a large amount of secret messages. We classify the pixels using a threshold based on the standard deviation of the local complexity in the cover image to provide a compromise between the embedding capacity and the image visual quality. The experimental results demonstrated that the algorithm CLCES proposed produces insignificant visual distortion due to the hidden message. It provides a high embedding capacity that is superior respect to the offered by the existing schemes. The proposed method is a secure steganographic algorithm; it can resist the image quality measures (IQM) steganalysis attack. The RGB, YCbCr, and HSV color spaces are incorporated in the proposed scheme to ensure that the difference between the cover image and the stego-image which is indistinguishable by the human visual system (HVS). Finally, the proposed scheme is simple, efficient, and feasible for the adaptive steganographic applications.

1. Introduction

Steganography is the science that involves the secret communications of data in an appropriate multimedia carrier, such as, audio, image, and video files (Cheddad, Condell, Curran, & Mc Kevitt, 2010). It comes under the assumption that if the secret data is visible, the point of attack is evident (Cheddad et al., 2010; Petticolas, 2000), thus the goal here is to conceal the existence of the embedded data. In the case of image files (the most widespread research area), a steganographic method employs innocent-looking media called host or cover image to imperceptibly carry hidden data to an intended recipient (Cheddad et al., 2010; Petitcolas, Anderson, & Kuhn, 1999; Petticolas, 2000). The image embedded with the hidden data (i.e., secret data, copyright notice, serial number) is called the stego-image and it looks as a normal image. Unintended recipients of a stego-image are unaware of the existence of the hidden data. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data (Petitcolas et al., 1999). The steganalysis techniques detect the existence of secret data in digital media, these refers to the techniques that are designed to distinguish between the cover and stego images (Kharrazi, Sencar, & Memon, 2006; Luo, Wang, Wang, & Liu, 2008).

There are several approaches in the classification of the steganographic methods. The steganographic techniques can be classified into three categories (Cheddad et al., 2010): spatial, frequency, and adaptive methods. The *spatial methods* generally use a technique to replace the direct least significant bit (LSB) substituting a redundant part of a cover image with a secret message. A disadvantage of the LSB algorithms is when data is embedding in the 1st LSB and up to the 4th LSB, it can be seen that embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as "non-natural", it is a tradeoff between the payload and the cover image distortion; therefore the payload (embedding up to the 1st, 2nd, 3rd, or 4th LSB) is analogous with respect to the recovered embedded image (Cheddad et al., 2010). The *methods based in frequency domain*, such as the Fourier transform (FT), the discrete cosine transform (DCT), and the discrete wavelet transform (DWT) embed secret information in the frequency domain of a cover image. These methods hide messages in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping, and some image processing, than the LSB approach (Cheddad et al., 2010). Recently there exist methods such as perceptual masking (PM) or adaptive steganography (AS) which can be applied in the spatial or frequency domain (Cheddad et al., 2010). The *adaptive steganography* takes statistical features of the image before attempting to interact with its LSB/DCT coefficients. The statistics dictate where

* Corresponding author. Address: National Polytechnic Institute of Mexico, Mechanical and Electrical Engineering Higher School – Mexico, Av. IPN s/n, U.P. Zacatenco, SEPI-ESIME, Edif. Z, Acceso 3, 3er piso, Col. Lindavista, 07738 Mexico, D.F., Mexico. Tel./fax: +52 55 57296000x54622.

E-mail address: fgallegosf@ipn.mx (F.J. Gallegos-Funes).

0957-4174/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.eswa.2012.08.024

to make the changes. It is characterized by a random adaptive selection of the pixels depending on the cover image and the selection of the pixels in a block with a large local standard deviation. It is meant to avoid areas of uniform color (smoothareas). For instance, since high-energy wavelet coefficients correspond to the signal features of sharp variation like edges and textures, and low-energy corresponds to the smooth regions, during the steganographic process the current wavelet kernel is compared to a prescribed threshold level to identify the signal- or noise-dominant regions in a scale. It is proven to be robust with respect to compression, cropping and image processing (Cheddad et al., 2010).

A second classification is divided into six categories according to the cover image modifications applied in the embedded process (Petitcolas et al., 1999; Petticolas, 2000): the *substitution systems*, they substitute redundant parts of a cover image with a secret message (i.e., LSB substitution, pseudorandom permutations, palette-based images, etc.). The *transform domain techniques* embed secret information in a transformed space of the signal (i.e., in the frequency domain). The *spread spectrum techniques* adopt ideas from spread spectrum communication. The *statistical methods* encode information by changing several statistical properties of the cover image and use the hypothesis testing in the extraction process. The *distortion techniques* store information by the signal distortion and measure the deviation from the original cover image in the decoding step. The *cover generation methods* encode information in the way the cover image is created for the secret communication.

A steganographic technique is evaluated in terms of a large embedding capacity and excellent stego-image visual quality (Lou, Wub, Wang, Lin, & Tsai, 2010). Unfortunately, the fact is the visual quality degradation in proportion of the embedding capacity, the better embedding capacity the worse visual quality. The more reasonable way to deal with this trade-off situation is probably to strike a balance between the embedding capacity and the loss of visual quality. Judging by whether the human vision sensitivity is considered in the design of the embedding algorithms, a third classification is realized into three types (Lou et al., 2010): *high embedding capacity schemes with acceptable image quality*, the mechanism of capacity estimation in the embedding procedure functions on a pixel-by-pixel basis without taking the local texture into consideration (i.e., the LSB technique). *High image quality schemes with moderate embedding capacity*, where the embedding capacity estimation of a pixel depends on the variation (local texture) among the immediate neighbor pixels. *High embedding efficiency schemes with slight distortion*, they focus on how to minimize the image distortion when embedding relatively small amounts of messages, normally less than or equal to two bits per pixel.

On the other hand, the wavelet analysis is an important tool in the spectral analysis due to its multi-resolution and localization capability both in time and frequency domain. Wavelet decompositions at different scales (frequencies) reveal underlying low and high frequency components that may be present in the observed series and help in localizing these features in time (Maheswaran & Khosa, 2012). The wavelet decomposition has been applied successfully on the classification and analysis of images (Huang & Aviyente, 2006). This decomposition is determined by one mother wavelet function and its dilation and shift versions (Lo, Li, & Freedman, 2003). There are a lot of wavelet families published in the literature; researchers commonly have difficulty in selecting an optimal wavelet for a specific image processing application (Lo et al., 2003). The choice of the optimal wavelet function depends on different criteria in several applications and in some of the distinctive properties of the wavelet function (Lo et al., 2003; Maheswaran & Khosa, 2012): (a) its region of support, it implies that the length span of a wavelet affects its feature localization capabilities as it is understandable that along and widely distributed wavelet function will compute the instantaneous process amplitude while, at the same time, it spans a wider window of the underlying process resulting in a higher degree of the averaging of the process states, and (b) the number of vanishing moments, this limits the ability of the wavelet to suitably represent information of a signal or polynomial behavior (Maheswaran & Khosa, 2012).

The most common approach of the wavelet decomposition is to decompose an image to extract energy values for all subbands as features for the subsequent classification. It is suitable to select a set of subbands for sparse representation in image classification applications. For a better classification of the results, it is desired that the energy features correspond to the areas of the selected subbands independent from each other as possible (Huang & Aviyente, 2006). The Daubechies wavelet family is generally applicable for image compression, watermarking, and steganography (Lo et al., 2003; Nafornita & Isar, 2009). These wavelets are compactly supported wavelets with extreme phase and a higher number of vanishing moments for a given support width. The Daubechies wavelets have associated scaling filters with minimum-phase, where both are orthogonal and biorthogonal, and do not have an explicit analytic expression except for the Haar wavelet, written as db1, as a special case (Maheswaran & Khosa, 2012). The Haar wavelets are symmetric and noncontinuous wavelets and the number of vanishing moments in this case is equal to one. The Haar wavelets have been found appropriate for applications in signals that have sharp changes because of its relatively narrow span over which its energy is distributed (Maheswaran & Khosa, 2012).

In this paper we present a robust steganographic scheme realized in whole its steps in the wavelet domain using the advantages of wavelet decomposition presented above, and according to the approaches of the adaptive steganography and the high image quality schemes with a moderate embedding capacity. The proposed method is capable of preventing visual degradation and providing a large embedding capacity. We introduce a wavelet domain preprocessing step before applying the proposed scheme, it is done to improve the steganography security (Gallegos-Funes, Martinez-Valdes, & de-la-Rosa-Vazquez, 2007; Sajedi & Jamzad, 2010). The embedding capacity for each pixel is determined by the local complexity of the cover image, allowing good visual quality as well as embedding a large amount of secret messages. We classify the pixels using a threshold based on the standard deviation of the local complexity of the cover image (Gallegos-Funes et al., 2007). Three different versions of the proposed method are presented using different criteria to hide data to provide a compromise between embedding capacity and image visual quality. The experimental results demonstrated that the proposed steganographic algorithm produces insignificant visual distortion due to the hidden message. It provides high embedding capacity superior to that offered by the existing schemes. The proposed method is a secure steganographic algorithm due it can resist the image quality measures (IQM) steganalysis attack (Avcibas, Mmon, & Sankur, 2003; Kharrazi et al., 2006; Luo et al., 2008). We also incorporate in the proposed scheme different color spaces such as the RGB, the YCbCr, and the HSV to ensure that the visual artifacts appeared in the stego-image are imperceptible, and the differences between the cover and the stego image are indistinguishable by the human visual system (HVS) (Cheddad et al., 2008; Liu, 2010). Finally, the proposed scheme is simple, efficient, and feasible for the adaptive steganographic applications.

2. Proposed steganographic method

The proposed color local complexity estimation based steganographic (CLCES) method is described in this section. The proposed