The Journal of Systems and Software 83 (2010) 1236–1248

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

A novel adaptive steganography based on local complexity and human vision sensitivity

Der-Chyuan Lou [a], Nan-I Wu [b], Chung-Ming Wang [b], Zong-Han Lin [b], Chwei-Shyong Tsai [c,*]

[a] Department of Computer Science and Information Engineering, Chang Gung University, Kweishan, Taoyuan 33302, Taiwan, ROC
[b] Institute of Computer Science and Engineering, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan, ROC
[c] Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan, ROC

ARTICLE INFO

Article history:
Received 6 March 2008
Received in revised form 30 December 2009
Accepted 30 January 2010
Available online 10 February 2010

Keywords:
Steganography
Local complexity analysis
Human vision sensitivity

ABSTRACT

This paper presents a novel adaptive steganographic scheme that is capable of both preventing visual degradation and providing a large embedding capacity. The embedding capacity of each pixel is dynamically determined by the local complexity of the cover image, allowing us to maintain good visual quality as well as embedding a large amount of secret messages. We classify pixels into three levels based on the variance of the local complexity of the cover image. When determining which level of local complexity a pixel should belong to, we take human vision sensitivity into consideration. This ensures that the visual artifacts appeared in the stego image are imperceptible, and the difference between the original and stego image is indistinguishable by the human visual system. The pixel classification assures that the embedding capacity offered by a cover image is bounded by the embedding capacity imposed on three levels that are distinguished by two boundary thresholds values. This allows us to derive a combination ratio of the maximal embedding capacity encountered with at each level. Consequently, our scheme is capable of determining two threshold values according to the desired demand of the embedding capacity requested by the user. Experimental results demonstrated that our adaptive steganographic algorithm produces insignificant visual distortion due to the hidden message. It provides high embedding capacity superior to that offered by a number of existing schemes. Our algorithm can resist the RS steganalysis attack, and it is statistically invisible for the attack of histogram comparison. The proposed scheme is simple, efficient and feasible for adaptive steganographic applications.

1. Introduction

Steganography is a way of secret communication carried out by using some digital multimedia to convey the critical messages, and therefore the major demand here is for both a high embedding capacity and good imperceptibility (Petitcolas et al., 1999; Wu and Hwang, 2007). In contrast to watermarking, the robustness is not a major concern with steganography (Petitcolas et al., 1999). The term steganography means 'cover writing,' indicating there is some unknown or secret written information under cover. The earliest modern scientific study on steganography was proposed by Simmons (1983). Simmons specified the motives and purposes of steganographic efforts with the so-called prisoners' problem. Generally speaking, steganography is all about the establishment of a form of secret communication between two parties. Since the typical ciphertext produced by a crypto-system appears so saliently distinct from normal text as if it were saying out load to potential attackers that there is something good, secret and confidential, to intercept here. From this perspective, only plaintext, i.e. a natural file that looks meaningful such as an image, audio or video, has a better chance of safely passing through an insecure communication channel instead of arousing the attention of an attacker. Therefore, steganography can serve its purpose of secure secret communication by using a plaintext cover to conceal the existence of the secret message, and a crypto-system can also be used to turn the confidential information from its original plaintext form into ciphertext to further raise the security level. Generally, the object that we intend to embed secret message is called the cover object, host object, or original object, indicating that it has not yet concealed the secret message.

A steganographic technique is usually evaluated in terms of the visual quality and the embedding capacity; in other words, an ideal steganographic scheme should have a large embedding capacity and excellent stego object visual quality. Unfortunately, the fact is the visual quality degradation is in proportion to the embedding capacity, and to push one to the limit really means to totally sacrifice the other. The more reasonable way to deal with this trade-off

* Corresponding author. Tel.: +886 4 22857540; fax: +886 4 22857173.
E-mail address: tsaics@nchu.edu.tw (C.-S. Tsai).

0164-1212/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2010.01.050

situation is probably to strike a balance between the two (Wu and Hwang, 2007).

Since the pixel value of a grayscale image has a higher tolerance for steganographic modification in terms of human visual perception, many steganographic schemes have been developed that use grayscale images as the cover objects. Judging by whether the human vision sensitivity is considered in the design of the embedding algorithm, we can categorize the schemes into three types: (1) high embedding capacity schemes with acceptable image quality (Chan and Cheng, 2004; Lin and Tsai, 2004; Thien and Lin, 2003; Wang, 2005; Wu et al., 2005), (2) high image quality schemes with a moderate embedding capacity (Chang and Tseng, 2004; Wang et al., 2008; Wu and Tsai, 2003; Yang et al., 2008; Zhang and Wang, 2005), and (3) high embedding efficiency schemes with a slight distortion (Mielikainen, 2006; Zhang and Wang, 2006a,b).

In the first type of schemes, the mechanism of capacity estimation in the embedding procedure functions on a pixel-by-pixel basis without taking the local texture into consideration. In other words, for these schemes, the hiding capacity of each pixel in a cover image is the same wherever the pixel is located, whether it is a rough area or smooth. The most common embedding algorithm the first type has is the least significant bit substitution (LSBs) technique, where the secret messages are hidden into the pixel LSBs to create a stego image. Therefore, they are also referred to as the simple LSBs schemes. For the human eye, the differences in the pixels are extremely hard to tell when it is the LSB planes that get manipulated. As a matter of fact, the LSBs approach also can be applied to the processing of 3D models, documents, binary images, etc. (Huang et al., 2009; Liu and Tsai, 2007; Yang and Kot, 2007). To date, many schemes have been proposed that focus on how to improve the stego image quality simple LSBs schemes offer at the same embedding capacity level. Since these embedding algorithms are built on the basis of the LSBs structure, the schemes also belong to the family of LSBs-based techniques. The maximum embedding capacity the schemes offered by is the ability of hiding three bits into the LSB planes of a pixel, while keeping acceptable visual quality (PSNR value above 40 dB). As for the embedding capacity, LSBs-based schemes are capable of hiding more secret information than the other data hiding techniques.

The second type is the adaptive steganographic schemes (Chang and Tseng, 2004; Wang et al., 2008; Wu and Tsai, 2003; Yang et al., 2008; Zhang and Wang, 2005), where the embedding capacity estimation of a pixel depends on the variation among the immediate neighbor pixels. That is to say, adaptive schemes take the local texture, or human vision sensitivity, into account when deciding the embedding capacity of each pixel. Hence, the overall embedding capacity of an image can vary if the picture has different local texture characteristics. A common strategy for adaptive steganography is to convey more secret messages in an image area with higher complexity, but conceal less on the area of lower complexity. It is worth mention that the some steganalytic techniques employed this strategy to detect whether any message is hidden in a host image. For example, Liu et al. (2008) proposed a feature mining and pattern recognition approach for steganalysis of LSB matching steganography that outperforms other well-known feature sets.

Basically, the great embedding capacity performance offered by LSBs-based schemes is not a major concern when we consider the adaptive schemes. Instead, we focus on improving the stego image quality produced by the LSBs-based schemes that conveyed the same embedding capacity. The visual artifacts produced by adaptive schemes are simply invisible because the characteristics of the original image have already been preserved so that the local textures keep unchanged through the embedding process. In Section 2, we shall detail how these adaptive schemes work.

Finally, the third type is the high embedding efficiency schemes. 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. Zhang and Wang (2006b) introduced the embedding efficiency as the ratio between the number of embedded bits and the distortion energy caused by data embedding. Mielikainen (2006) presented a LSB matching mechanism which utilizes a binary function to embed two bits of message into two pixels, the capacity being equivalent to 1.0 bpp. The expected mean square error is 0.375 per pixel, leading to the embedding efficiency of 8/3. The embedding efficiency is higher than that produced by 1-bit LSB embedding scheme, whose expected mean square error is 0.5 per pixel, leading to a lower embedding efficiency of 2.0. Zhang and Wang (2006b) introduced a novel embedding algorithm that exploits modification directions, which turned out with a better performance than their predecessors (Mielikainen, 2006; Zhang and Wang, 2006a).

The major concern of this study focuses on the second type of steganography. In particular, we intend to improve adaptive steganography. We propose a new scheme for grayscale images that can both efficiently assign dynamic embedding capacity and produce a stego image visually indistinguishable from the original cover image. In our scheme, the standard deviation is adopted to analyze the local complexity so as to estimate numbers of bits that can be concealed in a block of image. A higher standard deviation means the texture of the block is rougher and therefore the block can carry more secret data without causing artifacts that is identifiable by the human eyes, and vice versa. This way, the stego image quality can be ensured.

The remainder of this paper is organized as follows. In Section 2, we shall review three well-accepted adaptive data-embedding schemes. Then, In Section 3, we shall present our new ideas and new approach. The experimental results and discussions will be covered by Section 4, followed by the conclusion in the last section.

2. Background and motivation

In this section, we shall briefly review some previous techniques that inspired us, and we shall also discuss the motives that have brought us to our new design. In 2003, Wu and Tsai proposed the pixel-value differencing (PVD) approach that decides the size of embedding capacity by using the difference value between two consecutive pixels (Wu and Tsai, 2003). In their scheme, all difference values are graded and assigned to several different degrees, where a higher degree indicates a larger difference value, and vice versa. Basically, a larger difference value between a pixel pair means that the pixels can allow a greater modification for hiding more data. On the contrary, if a pixel pair has a small difference value, suggesting that the pixel pair is probably located in a smooth area, then only a small amount of data should be hidden so that no obvious distortion is created. The primary concept the PVD scheme relies on is to exploit the difference values to record the secret message (i.e. the size of the difference value implies the secret message) and to keep the degree of the difference value unchanged after hiding data. Similar to the PVD scheme, another scheme proposed by Chang and Tseng is also an adaptive one, but it counts on side match to do the job (Chang and Tseng, 2004). The embedding capacity estimation of a pixel depends on its two, three, or four immediate neighboring pixels, and the size of the embedding capacity also depends on the difference value. Like what happens in Wu and Tsai's scheme, Chang and Tseng's embedding process counts on the difference value to convey the secret message, and the degree is kept unchanged after the embedding of the secret data.

To make a difference, Zhang and Wang (2005) utilize the concepts of multiple-base notational system and human vision sensitivity to develop a novel adaptive method by the name of