Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Pattern Recognition 39 (2006) 1155–1167

PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY

www.elsevier.com/locate/patcog

Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels

Chin-Chen Chang[a, b, *], Chi-Shiang Chan[a], Yi-Hsuan Fan[a]

[a] Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 621, ROC
[b] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan, ROC

Received 6 August 2005; received in revised form 26 November 2005; accepted 18 December 2005

Abstract

In this paper, we shall propose a novel image-hiding scheme. Our new scheme classifies the host image pixels into two groups of pixels according to the pixel values. For each group of pixels, the corresponding secret pixel values go through an optimal substitution process and are transformed into other pixel values by following the dynamic programming strategy. Then, we can embed the transformed pixel values in the host pixels by using the modulus functions and obtain the stego-image. Extensive experimental results demonstrate that our new method is capable of offering better stego-image quality than a number of well-accepted schemes.

Keywords: Image hiding; The least-significant-bit substitution technique; Modulus function

1. Introduction

In recent years, data encryption [1,2] and information-hiding techniques [3–8] have become popular fields of research. Although they are both focused on the protection of secret data, there is a major difference between the two fields of research: the appearance of the final product. After data encryption, the secret data appears to be a total chaos of seemingly meaningless bits, and it can only be recovered after the proper decryption process. On the other hand, the product of an information-hiding technique is a seemingly unimportant but meaningful image or any form of multimedia data with the secret data hidden in. To be more specific, data encryption is a method to encrypt secret data into cipher texts by using an encryption algorithm and a secret key so as to prevent illegal users from learning the secret information, because only the legal user who holds the secret key can decode the cipher texts. On the other hand, data-hiding techniques work by embedding the secret data into an image or a piece of multimedia data so that illegal users will not notice the very existence of the secret data.

Security is the major criterion to use when data encryption schemes are to be evaluated, while capacity and invisibility are the major concerns when it comes to building quality data-hiding schemes. The capacity of a data-hiding scheme refers to the quantity of the secret data that can be embedded into the carrier medium, and the term invisibility indicates how imperceptible the fact is to illegal users that the carrier medium has been manipulated and turned into a stego-medium. To sum up, an ideal data-hiding technique should be able to hide as large a number of secret bits as possible, and the quality of the stego-medium should be as little degraded as possible.

To add security to capacity and invisibility, however, data-hiding techniques can come along with data encryption. In other words, before the secret data embedding procedure begins, the secret bits can be encrypted by using encryption methods like DES or AES. This way, the safety of the secret data is doubled.

[*] Corresponding author. Department of Information Engineering and Computer Science, Feng Chia University, 100 Wenhwa Road, Seatwen, Taichung 40724, Taiwan, ROC. Tel.: 886 4 24517250x3790; fax: 886 4 27066495.

E-mail addresses: ccc@cs.ccu.edu.tw (C.-C. Chang), cch@cs.ccu.edu.tw (C.-S. Chan), fyh93@cs.ccu.edu.tw (Y.-H. Fan).

0031-3203/$30.00 © 2006 Pattern Recognition Society. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2005.12.011

Digital images are the most popular multimedia applications in our daily lives; therefore, they naturally make the most suitable host media for data-hiding techniques. Data-hiding techniques that take digital images as host media are usually referred to as image-hiding techniques.

Before going further, we talk about watermarking techniques [9–16]. Sometimes, watermarking techniques are treated as image-hiding techniques because they embed a watermark into some special areas of images, such as edges [12], regions [11,16] and layers [15]. However, the most important mission the watermarking techniques must accomplish is to keep any attacker from removing the watermark from embedded images. To achieve this purpose, the size of the embedded watermark is usually quite small, that is, the embedding capacity is usually very small. On the other hand, the major purpose of image-hiding techniques is to fool grabbers out of perceiving the existence of the secret data. Therefore, quantity and quality are two major criteria for image-hiding techniques.

The quantity refers to the maximum size of the secret data that can be embedded, and the quality indicates the degree of host image degradation after the embedding. Until now, there exist some different kinds of image-hiding techniques. For example, in [17–19], the secret data is hidden into halftone images. In [20,21], the methods use the image compression method to do secret data hiding. However, the quantity of the hidden secret data in those methods is quite limited. Another approach to data hiding is the methodology least-significant-bit (LSB) techniques [4,5,7,22].

The least-significant-bit (LSB) substitution technique is the simplest way to hide secret data into digital images. As the name suggests, the basic idea of the LSB substitution technique is to replace some least significant bits of the host pixels with the secret data. Although the LSB substitution technique is simple and easily applicable, the embedded secret data may seriously degrade the image quality.

To improve the quality of the stego-image, in 2001, Wang et al. [7] employed a genetic algorithm to generate a substitution table. According to this substitution table, the value of the piece of secret data to be embedded into each host pixel is transformed to another value in advance that is closer to the original value of the host pixel. This way, after the embedding of all the transformed values into the host pixels, the quality of the stego-image remains almost the same as it originally was. Wang et al. used a genetic algorithm to create a good substitution table; however, owing to the nature of a genetic algorithm, although the substitution table is good, it may not be the optimal solution. In order to obtain the optimal solution, in 2003, Chang et al. [4] proposed their dynamic programming strategy to efficiently pick out the best from all the possible substitution tables.

Another way to do data hiding is to use modulus functions as suggested by Thien and Lin [5]. In order to hide as many secret data bits as possible, Wang [22] classifies the host pixels into two groups and embeds different numbers of secret data bits into the host pixels according to the groups that the host pixels belong to. In this paper, we shall offer a novel method that finds the optimal substitution table for Wang's method. Transforming the secret data according to the optimal substitution table and embedding the transformed secret data into the host image by using Wang's method, we guarantee to obtain the least degraded stego-image quality.

The rest of this paper is organized as follows. In Section 2, we shall review some related works. Then, in Section 3, we shall present our new scheme. In Section 4 that follows, the experimental results shall be given to demonstrate the performance of the proposed scheme. Finally, the conclusions will be made in Section 5.

2. Related work

In this section, we shall provide some background knowledge of our new scheme by reviewing several related works. To begin with, in Section 2.1, we shall go over the dynamic programming strategy [7]. Then, in Section 2.2, we shall briefly discuss applying the modulus function technique on partitioned pixels [22].

2.1. Image hiding by using dynamic programming strategy

The most intuitive way to do image hiding is probably embedding the secret image into the least-significant bits of the cover image pixels. To do so, first of all, the secret image is decomposed into k-bit units, and then k least significant bits of each host pixel are replaced with a k-bit unit. In other words, the value k indicates the total number of secret bits that are embedded into each host pixel.

Although replacing the least-significant bits of each host pixel with secret data is a simple, easy straightforward way to do data-hiding, the quality of the product, namely the stego-image, may be significantly degraded. In 2001, Wang et al. [7] proposed an image hiding scheme with a substitution table to improve the quality of the stego-image. The function of the substitution table is to indicate to which k-bit value each secret k-bit unit should be transformed. In Wang et al.'s image hiding method, the substitution table takes the shape of an $N \times N$ matrix, $ST_{N\times N} = \{st[i][j] | 0 \leqslant i, j \leqslant 2^k - 1\}$, where the value of N is equal to 2^k. Moreover, the value of $st[i][j]$ is either 1 or 0. If the value of $st[i][j]$ is 1, then it means the secret k-bit unit with value i must be transformed into the value j.

Here is an example of how the substitution table works. Suppose the host image H contains four pixels, where each pixel contains eight bits.

$$H = \begin{bmatrix} 249 & 235 \\ 24 & 2 \end{bmatrix}_{10} = \begin{bmatrix} 11111001 & 11101011 \\ 00011000 & 00000010 \end{bmatrix}_2.$$

We assume that k is equal to 2; that is, two secret bits will be embedded into each host pixel. The secret data are