Available online at www.sciencedirect.com
ScienceDirect
Pattern Recognition 41 (2008) 2674–2683
PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY
www.elsevier.com/locate/pr

Inverted pattern approach to improve image quality of information hiding by LSB substitution

Cheng-Hsing Yang*

Department of Computer Science, National Pingtung University of Education, Pingtung 900, Taiwan

Received 13 October 2005; received in revised form 13 December 2007; accepted 21 January 2008

Abstract

Capacity and invisibility are two targets of the methods for information hiding. Because these two targets contradict each other, to hide large messages into the cover image and remain invisible is an interesting challenge. The simple least-significant-bit (LSB) substitution approach, which embeds secret messages into the LSB of pixels in cover images, usually embeds huge secret messages. After a large message is embedded, the quality of the stego-image will be significantly degraded. In this paper, a new LSB-based method, called the inverted pattern (IP) LSB substitution approach, is proposed to improve the quality of the stego-image. Each section of secret images is determined to be inverted or not inverted before it is embedded. The decisions are recorded by an IP for the purpose of extracting data and the pattern can be seen as a secret key or an extra data to be re-embedded. The experimental results show that our proposed method runs fast and has better results than that of previous works.

Keywords: LSB substitution; Information hiding; Image-processing; Security

1. Introduction

For the fast development of internet and digital techniques, plenty of data can be downloaded from servers to clients or transmitted between users every day. Because internet is a public environment, transmitted data are easy to be copied or destroyed by eavesdroppers. Therefore, how to transmit data secretly by internet becomes an important topic. One of the main techniques of achieving this task is data encryption [1], which transforms data into a ciphertext via cipher algorithms. Because ciphertexts resemble a stream of meaningless codes, they easily attract grabbers, who may try to either recover them or simply destroy them. To overcome this problem, information hiding offers different approaches to transmitting secret data [2]. Information hiding is a method of embedding secret messages into multimedia data, such as images, videos, or movies, such that an unauthorized user will not be aware of the existence of the hidden messages. In this paper, we take an image to be a carrier of secret messages and then refer to it as a cover image. After embedding the secret message into the cover image, the output image with the secret message embedded in it is called a stego-image.

Many approaches to information hiding have been proposed for different attributes, such as capacity [3], imperceptibility [4], undetectability [5], robustness [6], and reversibility [7]. These attributes are used for various applications, such as secret communication [8,9], copyright protection [10,11], tampering detection [12,13], and other human-centered approaches [14]. Besides, information hiding techniques can be categorized into two types: methods in the spatial domain and methods in the frequency domain. In the spatial domain, the secret messages are embedded by changing image pixels directly [4,5]. On the other hand, in the frequency domain, the image is first transformed into its frequency domain [6,11], and then the secret messages are embedded in the transformed coefficients.

For the object of transmitting secret data, good approaches to information hiding must provide two attributes: high capacity and high quality. Lots of papers have been aimed at this subject [15–28]. Most of them perform the embedding operations in the spatial domain. Moreover, three kinds of approaches are

* Tel.: +886 8 7226141; fax: +886 8 7215034.
E-mail addresses: chyang@mail.npue.edu.tw, cathy8.wang@msa.hinet.net (C.-H. Yang).

0031-3203/$30.00 © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2008.01.019

common used and sometimes combined: LSB-based [15–22], PVD-based [23–26], and mod-based [27,28] approaches. In LSB-based approaches, secret data are embedded by directly replacing the least-significant-bits (LSBs) with equal bits of the secret for each pixel. Also, approaches based on pixel-value differencing (PVD) adjust the difference value between a pair of pixels to fit the value of the embedded secret. Finally, mod-based approaches, which use the modular operation, are similar to k-bit LSB-based approaches if the modulus is 2^k. The concepts of the human visual system (HVS) are sometimes applied to these embedding approaches. For example, Wu and Tsai used the difference value between two neighbor pixels to determine how many secret bits should be embedded into these two pixels [23]. The concept which they applied is that edge areas can tolerate a larger amount of change than the smooth areas. Therefore, their experimental results showed that lots of secret data were embedded into the locations of edge areas. Similarly, in the side match approach proposed by Chang and Tseng, the number of bits to be embedded into a pixel is decided by the difference value between its side pixels [20]. In another example, to decide the number of bits embedded into a pixel, Lee and Chen considered the contrast of its neighboring pixels and the luminance of it [15]. The additional concept used in their method was that the greater a grayscale is, the more change of the grayscale could be tolerated. This concept was also used by Wang [28].

Some other papers applied completely different strategies to improving the quality of stego-images generated by LSB-based approaches [16–19,21,22]. These papers entirely improve the image quality without considering the HVS. However, their strategies would not conflict with the HVS-based approaches, and sometimes can be combined with the strategies of the HVS [15]. In these papers, two kinds of strategies were proposed: one processing the secret message before embedding [16,22]; the other processing the stego-image after embedding [19]. In order to improve the quality of a stego-image, Wang et al. [16] proposed an optimal LSB substitution scheme for information hiding. They used a substitution matrix to transform the secret message before the secret message was embedded into the cover image. For a k-bit LSB substitution, there are $2^N!$ substitution matrices, where $N=2^k$. For $k=4$, the exhaustive search method will take a very long time to find an optimal substitution matrix. In order to overcome the long running time, they also proposed a genetic algorithm to find an approximate solution. It should be noted that it requires $k \times 2^k$ bits to record the selected substitution matrix. Because a genetic algorithm usually takes a lot of time and does not find an optimal solution exactly, Chang et al. [18] proposed a dynamic programming strategy to take less computation time and get an optimal solution. The drawback of the dynamic programming strategy is that its time complexity is not adequate. As shown in Ref. [21], its time complexity is $O(2^N + Nm)$, where m is the image size and $N=2^k$ for a k-bit LSB substitution. To find an optimal solution more efficiently, Yang and Wang [21] proposed a matching approach with time complexity $O(N^3 + Nm)$. In the strategies of processing stego-images after embedding, Chan and Chen [19] proposed an LSB-based hiding scheme using an optimal pixel adjustment process (OPAP). Their method adjusts each pixel after the message is embedded, and their experimental results showed that their method ran fast and achieved a good quality of stego-images.

In this paper, we propose a new LSB-based approach, named as the inverted pattern (IP) LSB substitution approach, to further highlight the quality of the stego-image Before secret messages are embedded, some secret messages are transformed by inverting operation and some secret messages are not. A simple strategy is used to judge whether a section of messages is inverted, and a bit string named as the IP is used to record these inverting actions. Also, we combine the concept of the OPAP with our approach to improve image quality further. The experimental results show that our approach results in a better image quality than that of the optimal LSB substitution approach [16,18,21] and the OPAP LSB substitution approach [19].

The remainder of this paper is organized as follows. Section 2 briefly describes the simple LSB substitution and the OPAP LSB substitution. Our approach is explained in Section 3. Experimental results are given in Section 4. Finally, our conclusions are presented in Section 5.

2. Preliminaries

In this section, we introduce some preliminary information about the LSB substitution and its improvement. The simple LSB substitution approach and the OPAP LSB substitution approach are described here.

2.1. Data hiding by simple LSB substitution

Suppose that the secret message is to be embedded into the k-rightmost LSBs of the cover image. Let $H = H_0 H_1 \dots H_{m-1}$ be the 8-bit grayscale cover image with m pixels, where H_i is a 8-bit string or a pixel of H, for $i = 0, \dots, m-1$. Also, let $S = S_0 S_1 \dots S_{m-1}$ be the secret message, where S_i is a k-bit string of S, for $i = 0, \dots, m-1$. We name the bit string S as the *secret string*. As shown in Fig. 1, a pixel H_i is partitioned into two bit strings MSB_i and LSB_i, i.e., $H_i = MSB_i \| LSB_i$. For the k-bit simple LSB substitution method, LSB_i will be directly replaced by S_i, for $i = 0, \dots, m-1$.

Let the resultant stego-image be $Z = Z_0 Z_1 \dots Z_{m-1}$, where Z_i is a 8-bit string or a pixel of Z, for $i = 0, \dots, m-1$. In order to estimate the quality of the stego-image, a peak signal-to-noise ratio (*PSNR*) is proposed. The *PSNR* function is defined

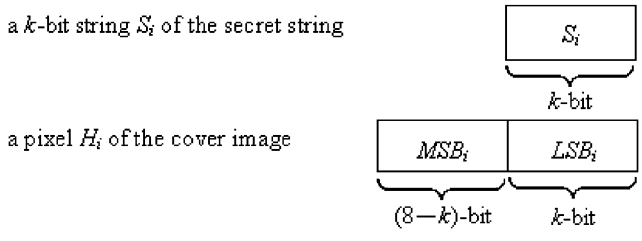

Fig. 1. For k-bit simple LSB substitution approach, the k-bit string LSB_i of a pixel H_i will be replaced by the k-bit string S_i directly.