Available online at www.sciencedirect.com

ScienceDirect

Applied Mathematics and Computation 196 (2008) 40–54

APPLIED MATHEMATICS AND COMPUTATION

www.elsevier.com/locate/amc

Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques

Wen-Yuan Chen

Department of Electronic Engineering, National Chin-Yi University of Technology, 35 Lane 215, Section 1, Chung-Shan Road, Taiping City, Taichung County 411, Taiwan, ROC

Abstract

In this research, on the basis of the differential phase-shift keying (DPSK) technique which is widely used in digital communication systems to develop a steganography scheme, we aim to hide a "secret image" into a cover image of the same size so that the resultant image has no noticeable degradation. In our approach, three strategies are used to achieve this goal: (1) Compress the secret image to reduce the number of secret bits. The set partitioning in hierarchical trees (SPIHT) codec were used to obtain a high reconstructed image quality and low bit rate image compression. (2) A neighbor block signal phase comparison (NBSPC) mechanism is used to offer the location for secret data embedding. (3) A fold phase distribution differential phase-shift keying FPDPSK mechanism is used to improve the quality of the cover image. With our contribution, we have developed the fold phase distribution DPSK concept to obtain more than 1.5 dB quality improvement and twice the noise margin than the standard DPSK technique on the same test condition.

Keywords: Steganography; Set partitioning in hierarchical trees (SPIHT); Differential phase-shift keying (DPSK); Discrete fourier transform (DFT); Discrete wavelet transform (DWT); Embedded zerotree wavelet (EZW)

1. Introduction

As the usage of the Internet becomes increasingly popular, online data exchange becomes extremely easy as well. While many gain great benefits through the Internet, they also encounter many serious problems with it. Piracy of private data serves as a good example. In order to remedy the drawback of data communication on the Internet, many data security techniques have been proposed. In general, there are two types of data security schemes, i.e. steganography and watermarking. Steganography techniques [1–6] conceal secret data into a cover image so that other people cannot find it. Watermarking techniques [7–9] usually conceal a logo in authors' works. In this paper, we propose a steganography scheme for image camouflage, in which a secret image is concealed into a cover image of the same size.

Based on an embedded zerotree wavelet compression method and bit-plane complexity segmentation skill, Spaulding et al. [10] proposed a steganography scheme. From his experimental results, it achieved a large

E-mail address: cwy@ncut.edu.tw

0096-3003/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.amc.2007.05.063

embedding capacity of around 255 of the compressed image size with little noticeable degradation in image quality. Wang [11] proposed a steganography scheme that used a modulus operation to incorporate secret data into a host image. In his paper, a half and a quarter of the chosen host image size were used to demonstrate that the secret image can totally be embedded with high image quality preservation.

Lie and Chang [12] proposed a method based on the human visual system to embed a series of secret data into a cover image. The embedding process is achieved by means of the least adaptive number of significant bits. In their approach, a higher hiding efficiency is obtained by using the concept of a self-contained number of LSBs under the constraint of human visual perception. In the extracting process, the secret data can be extracted without the original cover image.

Wang et al. [13] published a method of hiding data in images by optimal moderately significant bit (MSB) replacement. They presented a scheme consisting of ciphering, optimal substitution and pixel adjustment to implement the hiding process. However, embedding secret data in the MSB is accompanied by paying the cost of degradation of the cover images quality.

An approach, using image binary tree encoding and image smoothing to complete data hiding, was proposed by Hou and Chiao [14]. They created a binary tree code for a smooth secret image and embedded it into the cover image by bit replacement. In their approach, concealing a larger image in a smaller image becomes possible, and different types of data (image, audio, video, and text) can be used as the secret data.

Wu and Tsai [15] published an image data hiding method that employs multiple-based number conversion and lossy data compression. A stego-image is obtained by embedding secret data into selected pixels with a capacity that is determined by the difference of the cover image and the loosely processed cover image. In the extracting process, however the original cover image is required to extract the secret data.

For concealing the secret image into the same size of cover image, a kind of image compression technique with low bit rate and high reconstructed image quality is necessary. Shapiro [16] proposed the embedded zerotree wavelet (EZW), a very effective and computationally simple technique for image compression. Said and Pearlman [17] presented a new implementation based on set partitioning in hierarchical tree (SPIHT) that is an enhanced version of EZW. The SPIHT algorithm not only better performance than EZW but also features its extremely fast coding procedure provided by SPIHT. With the high reconstruction quality and low bit rate property, it is well suited secret image compression. Another SPIHT codec can be found in [18,19].

Yang et al. [20] presented a compression-domain watermarking technique based on the SPIHT coding. It is different from the conventional methods that incorporate watermarks into transformed coefficients. In their approach, a binary watermarking sequence was directly impressed on the bitstream generated in a quantization process. Meanwhile, the performance of their scheme can be enhanced with minimal complexity by a joint optimization of quantization and watermarking.

For steganography schemes, several papers have already proposed concealing large-sized images without noticeable degradation. In this paper, we use an excellent data compression scheme, a set partitioning in hierarchical trees (SPIHT) coding to achieve concealment of larger secret images without noticeable degradation. In addition, the phase of the coefficients of the DFT block was used to embed the secret data and construct a full cover image without damage. On the other hand, we develop a fold phase distribution differential phase-shift keying (FPDPSK) technique to replace the standard DPSK technique to increase the noise margin, decrease noticeable degradation, and improve the imperceptibility. The remainder of this paper is organized as follows. The codec of the set partitioning in hierarchical trees coding is presented in Section 2. The principle of differential phase-shift keying is in Section 3. The proposed data-embedding algorithm is in Section 4, the data extracting process from the stego-image is illustrated in Section 5, the empirical tests and security analysis are in Section 6, and finally Section 7 concludes this paper.

2. Set partitioning in hierarchical trees

Embedded zerotree wavelet (EZW) coding is a very effective and computationally simple technique for image compression. The set partitioning in hierarchical trees (SPIHT) coding is an improved version of the EZW. The coding and decoding procedures of SPIHT are extremely fast compared to EZW. However, some symbols must be defined in the SPIHT encoding process. A list of significant pixels (LSP) is used to store all the significant coefficients. Another list of insignificant pixels (LIP) is an un-processed coefficient