Steganography in image using discrete wavelet transformation

I. BADESCU, C. DUMITRESCU

University Politehnica of Bucharest, Independence Street, nr. 313, Bucharest, **Romania,** iulian_badescu@yahoo.com, catalindumi@yahoo.com.

Abstract: In this paper, we propose a new algorithm of steganography to allow simultaneous hiding secret message and small-size image into an large-size image. To hide the secret message in small image we use the Least Significant Bit (LSB) substitution, and the method for hiding the image in the image cover use Discrete Wavelet Transformation (DWT). The proposed method results in increasing the secret message capacity and security level. The secret message won't be visible after embedding and can be extracted later.

Key-Words: LSB, wavelet, steganography, high capacity, pixel matrix, hide message.

1. Introduction

From Wikipedia, steganography is the art or practice of concealing a message, image, or file within another message, image, or file. The word *steganography* is of Greek origin and means "covered writing" or "concealed writing". Some implementations of steganography which lack a shared secret are forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle. It combines the Greek words *steganos* (στεγανός), meaning "covered or protected", and *graphei* (γραφή) meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other *cover text*. For example, the hidden message may be in invisible ink between the visible lines of a private letter.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

The proposed algorithm has two stages of implementation. In the first stage the secret message (10,000 characters) is hidden in an image size 640 x 480 using LSB algorithm, and in the second stage the stego-image resulting is hidden in an cover-image size 1024x1024, using the decomposition of multiresolution DWT. Thus simultaneous hiding the secret message and secret images in a single cover image.

2. Wavelet

Many applications use the wavelet decomposition taken as a whole. Some of these applications are compression and denoising. Wavelet analysis allows the use of long time intervals where we want more precise low-frequency information, and shorter regions where we want high-frequency information.

The DWT [1][2] consists in splitting the signal $x[n]$ in low and high frequencies using a lowpass and a highpass filter respectively (equation 1):

$H(\omega) = \sum_n h[n]e^{-jn\omega}$ and $G(\omega) = \sum_n g[n]e^{-jn\omega}$

where H(ω) and G(ω) should be orthogonal:

$$|H(\omega)|^2 + |G(\omega)|^2 = 1 \qquad (2)$$

ISBN: 978-960-474-387-2

The signals obtained are down sampled by two, in order to reduce their size. This process can be continued for each signal obtained from the lowpass filter for a number of arbitrary times (see Fig.1). The coefficients obtained are:

$$a_{j+1}[p] = \sum_n h[n-2p]\, a_j[n]$$
$$d_{j+1}[p] = \sum_n g[n-2p]\, a_j[n] \qquad (3)$$
$$a_0[p] = x[p]$$

where $j = 0,\ldots,L$ is the resolution level (0 - high resolution, L - the lowest resolution). The coefficients $aL[p]$ are the approximation of the original signal and $dj[p]$ are the detail coefficients of $x[n]$.

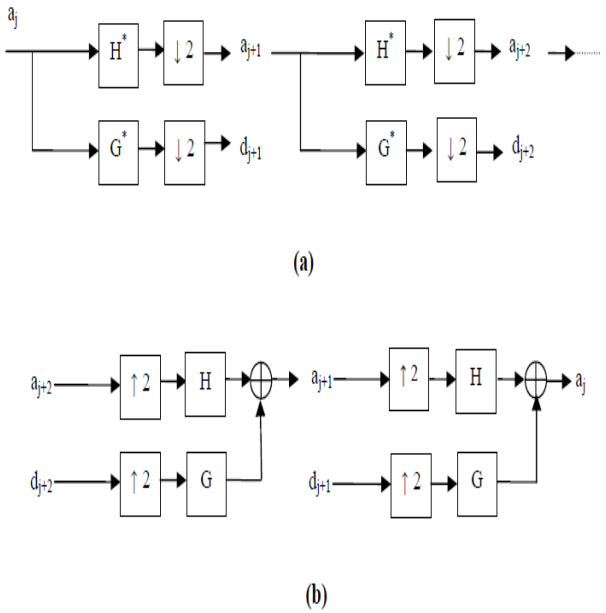

Fig. 1. The DWT (a) and the IDWT (b) of the 1D signal x[n].

The reconstruction of the original signal $x[n]$ is the inverse process of the DWT (equation 4):

$$a_j[p] = \sum_n h[p-2n]\, a_{j+1}[n] + \sum_n g[p-2n]\, d_{j+1}[n]$$

The DWT for two dimensional signals, like images, is similar to the DWT for one dimensional signals. The difference is that one has to implement separately for each dimension the DWT and IDWT respectively. The image will be decomposed for each resolution level into a high-high (HH), high-low (HL), and low-high (LH) subband, and a low-low (LL) subband for the coarsest resolution level. The LL band is also known as as the approximation subimage because it contains most of the information from the image. The HL, LH, HH sub bands are the detail sub images containing the horizontal, vertical and diagonal details (see Fig.2 and 3).

Fig.2. DWT pyramid decomposition of an image for two resolution levels.

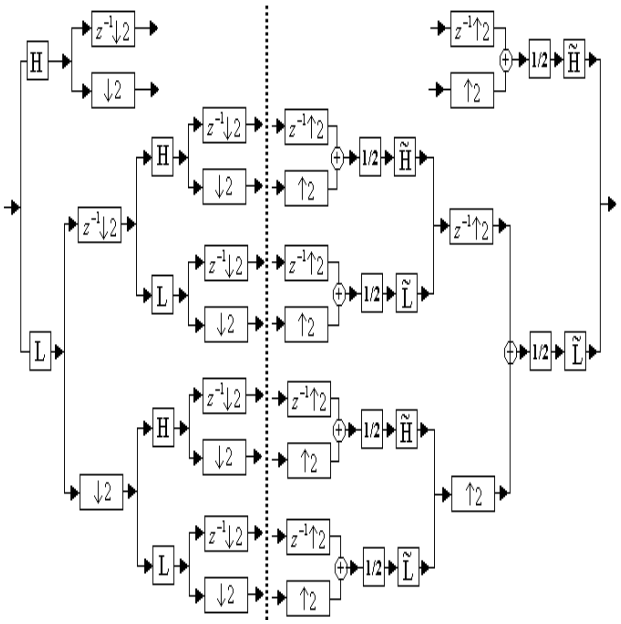

Fig.3. Wavelet transform, direct and inverse for two levels of decomposition.

3. Implementation

In Fig. 4 are presented the stages of implementation of the proposed algorithm.

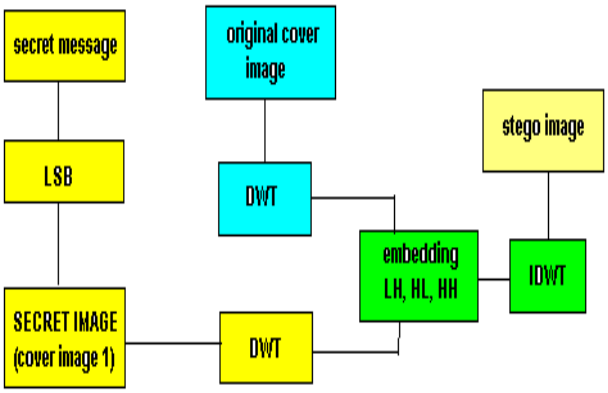

Fig.4. Stages of implementation of the proposed algorithm.

3.1 LSB substitution based steganography

Here spatial features of image are used. This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray-level image, every pixel consists of 8 bits [3]. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. The mathematical representation for LSB is:

$$X_i' = x_i - x_i \bmod 2k + m_i \quad (5)$$

The ith pixel value of the stego-image and x_i represents that of the original cover-image. M_i represents the decimal value of the ith block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as in Equation (6).

$$m_i = x_i \bmod 2k \quad (6)$$

Hence, a simple permutation of the extracted mi gives us the original confidential data. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane. In Fig. 5 shows the implementation of LSB algorithm used to hide secret message in secret image-cover image 1 (yellow blocks represented in Figure 4).

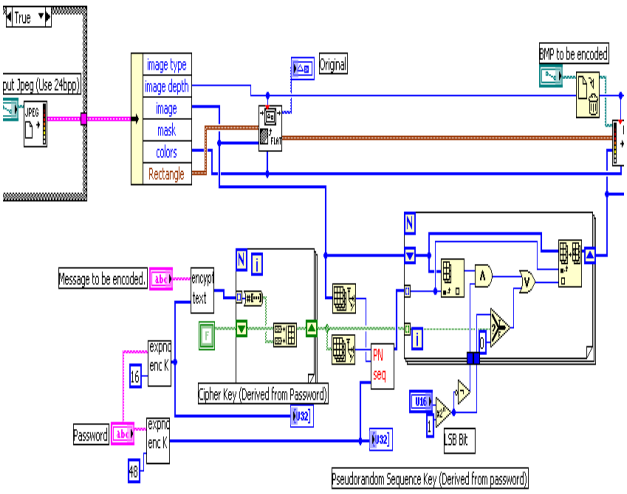

Fig.5. LSB algorithm implementation used for hiding the message.

3.2 Embedding process

Our information-hiding algorithm includes five steps:

1) Perform LSB transformation secret messages on the secret image (cover image 1).

2) Perform single level Harr wavelet decomposition both on the host image and the transformed secret image, and four components (approximate, horizontal, vertical, diagonal) of the host image and the secret image are got respectively. Denote these components as h_i and s_i, where *i 2 a; h; v; d.*

3) Quantize s_i as qs_i and encode qs_i into bit stream A_i using Raw Binary Encoding, respectively. In order to decrease additional information, more specifically, quantization table to be shared between the sender and the receiver, s_i is equally quantized. Thus, only a quantization factor should be shared between the sender and the receiver before covert communication.

4) Embed A_a into h_a using the improved LSB algorithm [4][5][6], and embed A_h, A_v, A_d into the relationship between h_h and h_a, h_v and h_a, h_d and h_a, respectively.

Four secret keys are used to choose the set of DWT coefficients for information embedding.

5) After information embedding, wavelet reconstruction is performed on the host image using modified h_a, h_h, h_v and h_d [7].

The whole embedding process is shown in Fig.4.

4. Experimental results

For our experiment we introduced a message with a length of 10,000 characters (can be encrypted by AES), in a small 640 x 480 image gray scale, the result obtained being hidden in an image of size 1024x1024.

Thus was developed an application that can hide text (secret) message and secret image at the same time the same cover image.

Fig. 6. Stego image for a variable image quality: (a) Q=20, (b) Q=50, (c) Q=75, (d) Q=85.

Table 1. Calculated result for above image

Calculation	*Result*
Compression ratio	0.9715 db
SNR	23.98 db
PSNR	28.81 db
MSE	64.14 db

5. Conclusions

In this paper, we propose an algorithm to hide information with robust and high capacity of hide. The algorithm was tested for gray images, but can be used for color images.

As a result of the experiments resulted as gray images hide capacity can increase substantially.

Starting from these considerations can develop steganography applications that allow hiding of gray images in the color image.

Subsequent developments will focus for the development of an application to hide audio files in the cover image.

References:

[1]. ***S.*** *Qian, D. Cheng, "Joint Time-Frequency Analysis",Pretince Hall 1996;*

[2].*N.* *Corina, "Digital watermarking in the wavelet domain",http://www.tc.etc.upt.ro/personal/corina/book05.pdf;*

[3]. ***P****. Nerkar,"Steganography for colored images" International Journal of Electronics, Communication & Soft Computing Science and Engineering ISSN: 2277-9477, Volume 2, Issue2, 2010;*

[4]. ***B.*** *Yang, B. Deng, "Steganography in gray images using wavelet" Technical Report 448, Departament of Statistics, Beijing University, 2011;*

[5]. ***R****. Gonzalez, R. Woods, "Digital Image Processing", 3rd Edition, 1995;*

[6]. **A.** *Jain, " Fundamentals of Digital Image Processing" Pretince/Hall International, 1987;*

[7]. ***V.*** *Strela, Multiwavelet: Theory and Applications, PhD, Thesis, MIT, 1996.*