Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 612 – 618

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

A Novel DWT based Image Securing Method using Steganography

Della Baby[a,]*, Jitha Thomas[a], Gisny Augustine[a], Elsa George[a], Neenu Rosia Michael[a]

[a]*Department of Electronics &Communication Engineering, SJCET Palai, Kerala, India*

Abstract

Steganography is a data hiding technique that is widely used in various information securing applications. Steganography transmits data by hiding the existence of the message so that a viewer cannot identify the transmission of message and hence not able to decrypt it. This work proposes a data securing technique that is used for hiding multiple color images into a single color image using the Discrete Wavelet Transform. The cover image is split up into R, G and B planes. Secret images are embedded into these planes. An N-level decomposition of the cover image and the secret images are done and some frequency components of the same are combined. Secret images are then extracted from the stego image. Here, the stego image obtained has a less perceptible changes compared to the original image with high overall security.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: Stego image; Steganography; RGB color planes; N-level DWT.

1. Introduction

Steganography [1] (hidden writing) consists of two words: Steganos which means “secret” and the graphic which means “writing”. Steganography implies hiding data into another media file such as image, text, sound or video. The main terms used in steganography are: cover message, secret message, and the embedding algorithm. The cover message is used to hide images (messages) into it. The secret messages are hidden materials in the

* Corresponding author. Tel.: +91−9446719472
*E-mail address:*mail4dellababy@gmail.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.105

steganographic process. An embedding algorithm is used to effectively carry out the message hiding process.

Steganography can be done in both spatial domain and frequency domain. The Least Significant Bit substitution is a spatial domain steganographic technique. A gray-scale image, in which each pixel is of 8 bits, can be displayed by $2^8 = 256$ variations. In LSB substitution, the private data is hidden in the least significant bits (right-most bits) so that the original pixel value is not affected by embedding procedure. LSB insertion is a simple and commonly used method to embed a data in an image in the spatial domain [2]. The negative part of this approach is that, it is prone to minor image manipulations .So this method is not safe for sending confidential data.

Data hiding can be effectively performed in the frequency domain [3]. Steganographic approach for securing image using DCT [Discrete Cosine Transform] is a widely used method. DCT [4] allows an image to be broken up into three frequency bands namely the Low-frequency band (FL), High-frequency band (FH) and Mid-frequency band (FM). In this approach, the secret data is embedded into the DCT blocks containing mid frequency (FM) sub band components whereas the high frequency sub band components remain unused [5].Using frequency domain steganography is safe, sound, and flexible approach, and these are its added advantages. It has different techniques for management. Steganography using DWT has more advantages over DCT because it provides high compression ratios and also it avoids interferences due to artifacts. So comparatively DWT is a better method for hiding confidential data.

The rest of the paper is organized as follows. Section 2 a study on Wavelet transform is done. Section 3 describes the proposed algorithm and the corresponding simulations and discussions are done in section 4. Finally section 5 concludes the paper.

2. Discrete Wavelet Transform

The Discrete Wavelet Transform [5] can identify portions of cover image where secret data could be effectively hidden. DWT splits information into its high and low frequency components. The high frequency part of the signal contain details about the edge components, whereas the low frequency part contains most of the signal information of the image which is again split into higher and lower frequency parts. For each level of decomposition in two dimensional applications, first DWT is performed in the vertical direction followed by horizontal direction.

3. Proposed Algorithm

3.1. Secret Image Hiding

1. The cover image is disintegrated into three color planes. They are R (Red) plane, G (Green) plane and B (Blue) plane in order to embed secret images into each color plane.

2. Each color plane of the cover image is then decomposed using DWT into 4 non-overlapping sub-bands. These are LL (approximation coefficients), LH (vertical details), HL (horizontal details) and HH (diagonal details).The LL sub-band is processed to obtain the next value of wavelet coefficients until some final value “N” is reached. At this stage, we have 3N+1 sub-bands. These consists of (LLX), (LHX), (HLX) and (HHX) where value of “X” ranges from 1 to “N”.