International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

New Steganography Technique

Shahbaa Mohammed

Assistant Teacher, Collage of Law, Al-Iraqia University, Msc., Computer Science, Baghdad, Iraq

Abstract: ***Recently there has been an increase in the use of the internet, people use it as a part of their daily lives. And to secure their data, steganography and cryptography are used. Here we suggest using a new steganography technique to hide multiple colored images in a single one by using Discrete Wavelet Transform (DWT). The cover image is represented by three color model which is: H (Hue), S (Saturation) and I (Intensity), and the secret images are hidden in them. Multiple levels of the cover image are decomposed and the secret images are hidden in them and some of the similar frequencies components are merged. The hidden images are extracted from the stego image. By using this technique the changes done are less noticeable on the stego image compared to the original one with increased security.***

Keywords: Stego image, Steganography, HIS, N-level DWT

1. Introduction

Steganography (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 steganographic process. An embedding algorithm is used to effectively carry out the message hiding process [1].

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].

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 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) [4]. In this technique, 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 and flexible approach, and these are its added advantages. It has different techniques to deal with. Steganography using DWT is better than DCT because it provides high compression ratios and also it avoids interferences due to artifacts. So comparatively DWT has more advantages for hiding confidential data.

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

2. Discrete Wavelet Transform

The Discrete Wavelet Transform 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 [5].

3. Proposed Technique

3.1. Secret Image Hiding

1) The cover image is disintegrated into three color model which is: H (Hue), S (Saturation) and I (Intensity) in order to embed secret images into each of them.
2) Each color model 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".
3) The division of the model is done by employing Haar filters [5]. If a DWT coefficient is altered, it will alter the region corresponding to that coefficient. Here we can see the exploitation of the masking effect of HVS(Human Visual System).
4) Secret images are also disintegrated into four sub-bands (LL, LH, HL, HH). The LL sub-band is further processed to get the next value of wavelet coefficients. Information contained in the LL sub-band of secret images is separately embedded into different bands of cover images.
5) After embedding the secret image bits into three color model of cover image, inverse transformation (IDWT) is performed to retrieve them then combined to generate the

final color stego image.

3.2. Secret Image Extraction

1) Stego image is decomposed into three color model (H, S and I).
2) Each color model of the stego image is divided into non-overlapping sub-bands. The sub-bands are LL, LH, HL and HH. The LL sub-band is processed further to obtain the next scale of wavelet coefficients using Haar DWT.
3) Secret images are extracted from the corresponding embedded frequency bands of color models.

4. Simulation and Discussions

This section provides the experimental results and analysis of the proposed scheme. This work is programmed in MATLAB (R2008a) with the system specifications - windows 7 ultimate OS, Intel i3 core processor and 32 bit operating system. This algorithm effectively embeds the secret images into the cover image and extracts it back from the stego image with an execution time of about 50s .The simulation results suggest that this technique remains good image quality. It is robust in comparison with different image processing operations. Fig.3a. shows cover image. Fig.3b. shows stego image Fig.4. shows the secret images.

Figure 3: a) lena cover image b) lena stego image

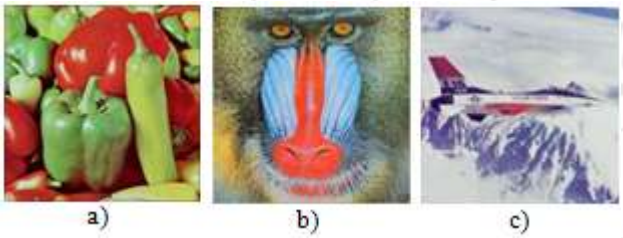

Figure 4: a) secret image1 b) secret image2 c) secret image3

4.1 PSNR

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio[6]. Larger PSNR value its mean higher image quality. On the contrary, a small PSNR value means the cover image and the stego image have less similarity. The mathematical definition for PSNR is:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

The PSNR value obtained for lena stego image is (54.4378).

Conclusion and Future Scope

Steganography transfer sensitive information through secret covers to conceal the existence of them. In areas where cryptography and strong encryption are being prohibitive, people are looking at steganography to avert such policies and transfer messages safely.

One of the good criteria for steganography is not to notice changes on the stego object by the human vision system. It is difficult to recognize the existence of a hidden data in the stego image using the existing technique, so we satisfied that criteria in our technique. This is because embedding is randomly performed in the frequency domain. Proposed technique gives a good PSNR value which establish the robustness of this work. When the results are compared with common methods, the proposed technique is found to be advanced. DWT is thus found to be a relatively better method as it growing payload of the steganographic process by data compression.

References

[1] Lou D. C, Liu J. L. Steganography Method for Secure Communications. *Elsevier Science on Computers& Security*, 21, 5: 449-460. 2002
[2] H. Arafat Ali. Qualitative Spatial Image Data Hiding for Secure Data Transmission. *GVIP Journal*, 7(1):35-43, 2007.
[3] Marghny Mohamed, Fadwa Al-Afari, Mohamed Bamatraf. Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. *International Arab Journal of e-Technology*, Vol. 2, No. 1, January 2011
[4] Blossom Kaur, AmandeepKaur, Jasdeep Singh, Steganographic Approach for Hiding Image in DCT

Domain, *International Journal of Advances in Engineering & Technology*, July 2011.
[5] Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, *International Journal of Applied Science and Engineering* 4, 3: 275-290. 2006
[6] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.