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”.

3. The division of the planes 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 planes of cover image, inverse transformation (IDWT) is performed to retrieve them. These three planes are then combined to generate the final color stego image.

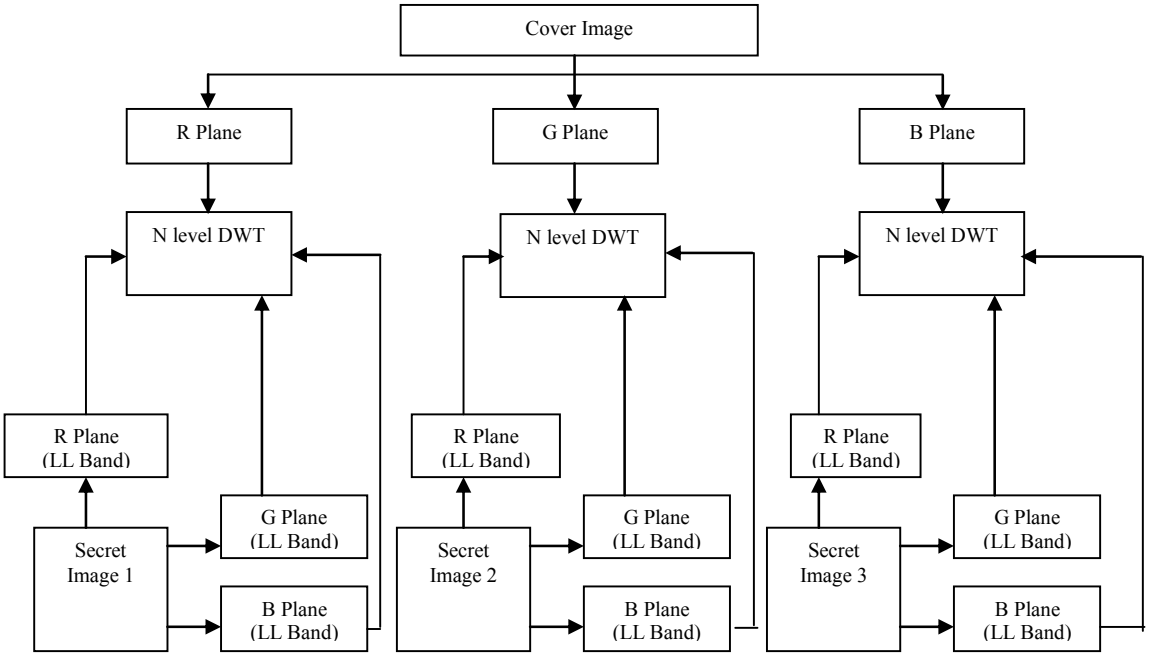

Fig.1. Embedding procedure

3.2. Secret Image Extraction

1. Stego image is decomposed into three color planes (R, G and B).

2. Each color plane 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 planes.

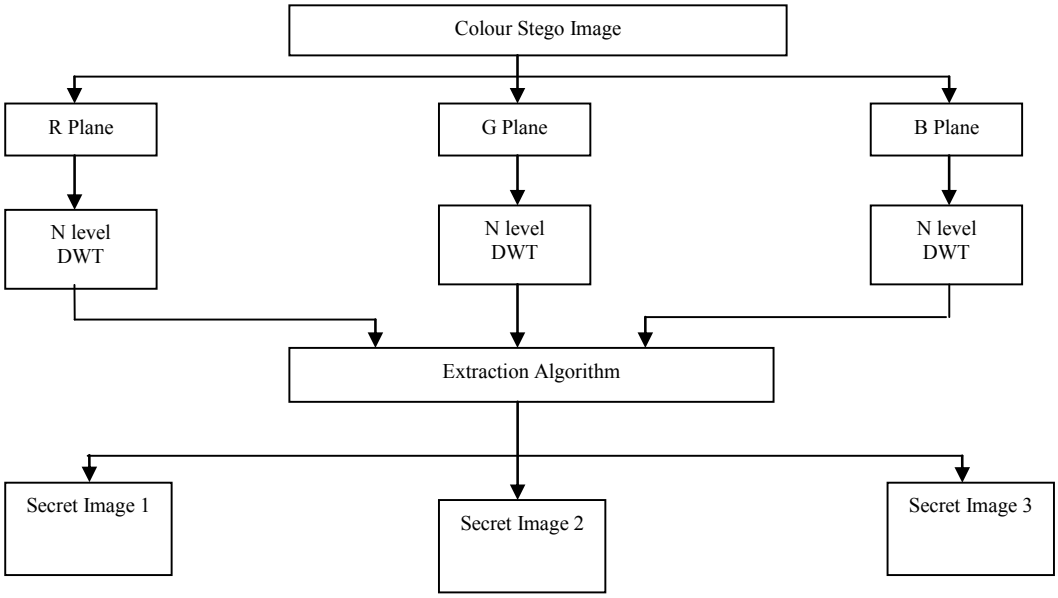

Fig .2. Extraction procedure

4. Simulations and Discussions

This section provides the experimental results and analysis of the proposed scheme. This work is programmed in MATLAB 2012a with the system specifications - windows 7 OS, Intel i3 core processor and 64 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 maintains good image quality. It is robust in comparison with different image processing operations. Fig.3. shows the original cover image. Fig.4. and Fig.5. shows the secret images and the extracted secret images respectively. Fig.6. shows final stego image.

Fig .3. Cover Image

Fig .4. Secret Images

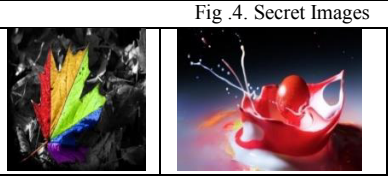

Fig .5. Extracted Secret Images

Fig .6. Stego Image

4.1. PSNR

The digital quality of an image can be calculated by using this parameter. The larger the PSNR value, the higher will be the quality of image. This means that there is least variation of stego image from cover image. On the contrary, a small PSNR value means the cover image and the stego image have less similarity. The mathematical definition for PSNR is:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \tag{1}$$

The average PSNR value obtained for the stego image is 55.53. The average MSE (Mean Square Error) value obtained for stego image is around 5-10.

Table 1. PSNR Values of different Cover Images.

No	Cover Image	PSNR
1	Lena	54.4378
2	Monarch	54.5596
3	Peppers	56.1197
4	Tulips	55.1921
5	Clegg	56.0077
6	Frymire	55.9184
7	Sail	54.9883
8	Serrano	56.3943

4.2. SSIM (Structural Similarity Index Matrix)

SSIM is a method used to improve the conventional methods like PSNR and MSE to determine the similarity between two images. The inferences of the case study of obtained SSIM values for different cover images are given in the tabel2. The average SSIM value obtained for the stego image is 0.39465. In this technique, we embed the secret images into the main cover image. This works consists of a stego image with 3 secret images in it. In order to perform the embedding, the LL bands of each plane of the secret images are considered. Since the whole secret image into the cover image can create a distortion, a small portion of it is embedded. The factor which decides the amount of details to be embedded is called the steganographic weight. This weight is the amount of the frequency components that are given into a plane of the cover image. The optimum value of weight is obtained as 0.1, as it gives the best output when extracted back which is shown in the table3. This weight decides the embedding rate and the SSIM value in the steganographic work.

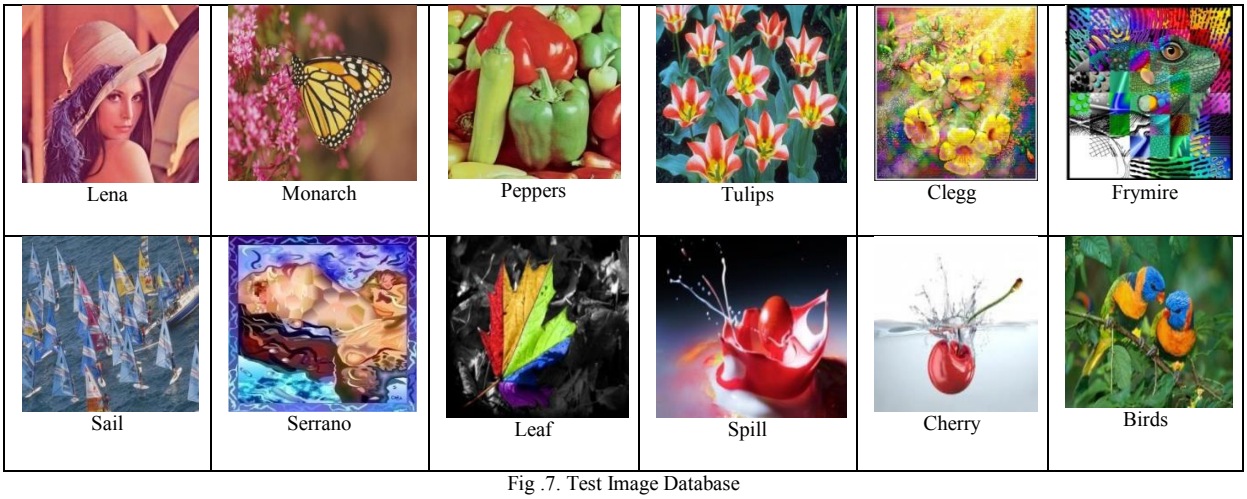

Fig .7. Test Image Database

Table 2. SSIM values for different cover images and secret images for weight 0.1

Cover Images	Stego Image	Secret Image1 Leaf	Secret Image2 Spill	Secret Image3 Cherry
Lena	0.3175	0.7004	0.8753	0.7764
Monarch	0.2927	0.7004	0.8753	0.7764
Peppers	0.4429	0.7004	0.8753	0.7764
Tulips	0.4918	0.7004	0.8753	0.7764
Clegg	0.3652	0.7004	0.8753	0.7764
Frymire	0.5779	0.7004	0.8753	0.7764
Sail	0.2187	0.7004	0.8753	0.7764
Serrano	0.4505	0.7004	0.8753	0.7764

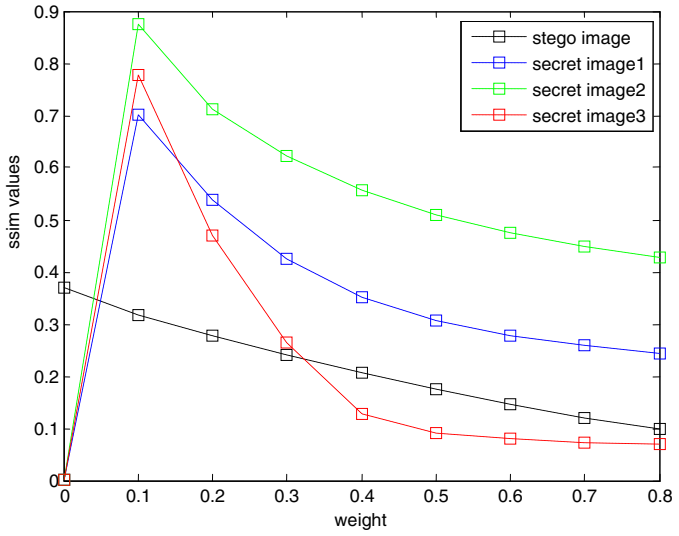

Fig.8. Graphical representation of SSIM for various weights

Table3. SSIM value corresponding to the weights

Weight	Cover Image Lena	Secret Image1 Leaf	Secret Image2 Spill	Secret Image3 Cherry
0	0.3697	0.00027	$8.7*10^{-4}$	$8.5*10^{-4}$
0.1	0.3175	0.7004	0.8753	0.7764
0.2	0.2768	0.5392	0.7127	0.4710
0.3	0.2404	0.4244	0.6212	0.2643
0.4	0.2065	0.3518	0.5556	0.1279
0.5	0.1747	0.3069	0.5087	0.0895
0.6	0.1450	0.2779	0.4743	0.0790
0.7	0.1196	0.2583	0.4480	0.0730
0.8	0.0996	0.2435	0.4270	0.0688

5. Conclusion and Future Scope

Steganography transmits secrets through confidential covers to hide the existence of them. In areas where cryptography and strong encryption are being forbidden, citizens are looking at steganography to avoid such policies and transmit messages safely.

The effectiveness of steganography is measured using three parameters. First, the steganographic technique must provide the maximum information. Second, the embedded data must not be perceptible to the viewer. Third, the hidden information should be successfully retrieved at the receiver. It is difficult to recognize the existence of a hidden data in the cover image using the existing methods. This is because embedding is randomly performed in the frequency domain. Proposed approach provides a good PSNR and SSIM value which establish the robustness of this work. The SSIM value of the secret images shows that the data is successively retrieved at the receiver. When the results are compared with prevailing methods, the proposed method is found to be advanced. DWT is thus found to be a comparatively better approach as it increases 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