Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Technique for Image Steganography Using DWT

Surajit Mandal*, Subhrajyoti Dutta, Soham Chatterjee, Subhadip Karar, Subhankar Banerjee
Department of Electronics & Communication Engineering
B. P. Poddar Institute of Management & Technology
West Bengal, India

Abstract— Steganography is the technique of concealing secret information within any media. In this paper we propose a new image steganography technique using Haar-discrete wavelet transform. Unlike other Haar-DWT steganography techniques where the payloads are embedded in the high frequency coefficients; in the proposed method all frequency components are judiciously modified to embed the information. The quality of the stego image and recovered payload are studied in terms of different image assessment parameters.

Keywords— Image steganography, security, discrete wavelet transform, Haar wavelet, peak signal to noise ratio

I. INTRODUCTION

In today's digitized world, the use of internet has become the prime mode of data transmission and subsequently digital crime becomes the major threat to its users. Therefore, it is felt desirable to have a secure data communication. One of the techniques to achieve this is to apply steganography during data transmission. The word 'steganography' is coined from two Greek words steganos (covered or secret) and graphia (writing or drawing). Steganography is the art and science of hiding secret information into another medium so that none apart from the sender and the intended recipient has the knowledge about the information. Various steganography schemes for data hiding have been reported [1-3]. The different media that are used to embed confidential data (text, image etc.) are plaintext, still imagery, audio, video, network IP datagram etc. The success and usefulness of any steganography technique depend on three important aspects that contend with each other: capacity, security, and robustness. Capacity is a measure of the amount of secret information that can be embedded in the cover medium without degrading the quality of the cover medium significantly. Security relates to an eavesdropper's inability to extract secret information from the stego medium, and robustness refers to the amount of modification that the stego medium can resist before an adversary can destroy the hidden information [4].

The most widely used steganography technique is concealing of the confidential text or digital image into another digital image. This method exploits the weakness of the human visual system as the human cannot detect the small variation in luminance of the colour vectors at higher frequency side of the visual spectrum. Different schemes of image steganography can be broadly classified into two categories: spatial domain methods and frequency domain methods. The most frequently used image steganography techniques are LSB (least significant bits) substitution method [5] and Haar-DWT (discrete wavelet transform) [6-7]. The basic concept of LSB substitution method is to embed the secret information at the least significant bits of the eight bit sequence representing each pixel value of a gray scale image. Thus, the original pixel values are expected to be less affected during the embedding process if the capacity of the cover image is less. However, when the capacity is increased to a large value, the image quality decreases appreciably and hence a suspected stego image results. The secret information can also be easily stolen as the extraction process is very simple in the LSB substitution method. The wavelet transform offers a multi-resolution decomposition technique in terms of expansion of an image onto a set of wavelet basis function. The DWT divides the signal into high and low frequency components. The high frequency component contains the information about the edge of the image and the low frequency component is further divided into high and low frequency parts. The high frequency components are generally employed for steganography as the human eye is less sensitive to small changes in edges. The first order, two dimensional Haar-DWT splits the image into four sub-bands (coefficients) denoted as LL, HL, LH, and HL. The low frequency portion is represented by LL and looks very similar to the original image.

In this communication, we report a novel technique of image steganography based on the first order Haar-DWT. To begin with, the payload and the cover medium both are considered to be gray scale images. The stego image and the retrieved payload are evaluated in terms of different image assessment parameters. The result is found to be consistent with that obtained in the existing image steganography techniques.

II. PROPOSED METHOD

The entire image steganography operation can be represented by a block diagram as shown in Fig. 1. *M* is the secret image. The size of the cover image (*C*) should be large enough to hold the secret image. The embedding algorithm is represented by the stego function *F*{ } which produces the stego image *S*. The stego image reaches the intended recipient after passing through a communication channel. A key (*K*) or password is used to hide and unhide the payload. The

password keeps the information more secure. The inverse function $F^{-1}\{\ \}$ compares the properties of the cover and stego images and extracts the secret image from the stego image.

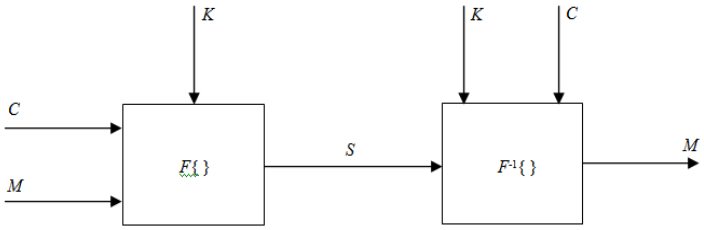

Fig. 1 The image steganography operation

Though the quality of the stego image and recovered payload is generally assessed with the aid of the human eye, different parameters are also used in steganography to assess these images quantitatively. For the present study we use the following image assessment parameters:

Capacity: Capacity can be formulated as

$$\text{Capacity} = \frac{\text{Number of pixels of secret image that hidden}}{\text{Number of pixels of cover image that are used to hide data}}$$

PSNR (peak signal to noise ratio): PSNR is a measure of reconstruction of the transformed image. This parameter is used to study the difference between the stego and cover image and between the retrieved payload and secret image.

$$\text{PSNR} = 10\log_{10} 255^2/\text{MSE},$$

where MSE (mean square error) is represented as follows:

$$\text{MSE} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j) - f'(i,j)]^2$$

Here $f(i,j)$ and $f'(i,j)$ represent the original image and transformed image respectively. A large value of MSE indicates that the image is of poor quality and vice-versa. The unit of PSNR is dB.

The proposed method of image steganography is a two-level process where we perform the first order Haar-DWT twice during the embedding process. The basic difference between the proposed technique and the existing Haar-DWT steganography techniques is that only high frequency components are modified to embed the secret image in the existing techniques whereas in the proposed technique all sub-bands are judiciously modified so as to hide the information and the quality of the stego image with high capacity is still very good as evident from the PSNR value. The embedding and extraction procedures of the proposed technique are as follows:

Embedding procedure:

1. Load password.
2. Read the cover image and payload.
3. Calculate the size of the payload.
4. Insert the pixel values of the payload in the duplicate version of the cover image using an arbitrary formula.
5. Insert the password in the triplicate version of the cover image using the same formula.
6. Take Haar-DWT of the modified duplicate and triplicate versions of the cover image.
7. Take the averages of horizontal, vertical, diagonal, and approximation coefficients of wavelet decompositions.
8. Take Haar-DWT of the cover image.
9. Take the weighted averages of horizontal, vertical, diagonal, and approximation coefficients obtained in steps 7 and 8.
10. Take IDWT.
11. Prepare the stego image to display.
12. Calculate MSE, PSNR (cover to stego image) and capacity of the cover image.

Extraction procedure:

1. Load the password.
2. Read the stego image and cover image.
3. Insert the password in the duplicate version of the cover image using previous formula and obtain modified cover image.
4. Take Haar-DWT of the original cover image, stego image and modified cover image.
5. Obtain horizontal, vertical, diagonal, and approximation coefficients from those of the stego and cover images by doing the reverse operation of step 9 of the embedding procedure.
6. Obtain another new set of coefficients from those obtained in step 5 and of the modified cover image by doing the reverse operation of step 7 of the embedding procedure.
7. Take IDWT.
8. Prepare the recovered payload to display.
9. Calculate MSE and PSNR (original payload to recovered payload).

III. RESULTS AND DISCUSSIONS

The proposed image steganography is simulated with MATLAB 8.1.0.604. An eight bit gray scale image (png) of a tree with size 1024×1024 is shown in Fig. 2. This image is considered to be the cover image for our study. We consider the image of a rose (jpg) as the payload. The corresponding stego image and recovered payload are also shown in Figs. 3, 4, 5, and 6. Different sizes of the payload are considered for comparison between the stego image and the cover image and also between the secret image and the extracted payload. The corresponding capacity, MSE and PSNR values are given in Table 1.

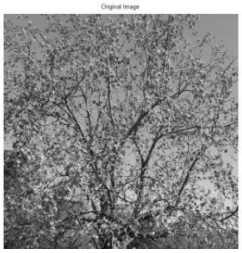

Fig. 2 Cover image (1024×1024)

(a) (b) (c)

Fig. 3 The proposed steganography operation: (a) original payload (256×256), (b) stego image, (c) recovered payload

(a) (b) (c)

Fig. 4 The proposed steganography operation: (a) original payload (512×512), (b) stego image, (c) recovered payload

(a) (b) (c)

Fig. 5 The proposed steganography operation: (a) original payload (768×768), (b) stego image, (c) recovered payload

(a) (b) (c)

Fig. 6 The proposed steganography operation: (a) original payload (1023×1023), (b) stego image, (c) recovered payload

Table I MSE, PSNR and capacity as obtained in the proposed approach

Cover image size (png)	Stego image type	Payload size	Payload type	MSE (cover to stego image)	PSNR (dB) (cover to stego image)	Capacity	MSE (Original payload to extracted payload)	PSNR (dB) (Original payload to extracted payload)
1024×1024	png	256×256	jpg	0.0698	59.6952	0.125	1.1313	47.5951
1024×1024	png	512×512	jpg	0.5017	51.1266	0.25	1.1475	47.5332
1024×1024	png	768×768	jpg	1.2227	47.2578	0.5625	4.5146	41.5846
1024×1024	png	1023×1023	jpg	1.8061	45.5633	0.9980	48.4479	31.2781

As evident from Table 1, the PSNR (cover to stego image) is approximately 60 dB when the capacity is 0.125. As the capacity increases, the MSE also increases as expected and the PSNR decreases. However, even when the capacity is 0.9980 the PSNR (cover to stego image) is still very high and we can extract the secret image from the stego image faithfully using our proposed technique. The corresponding PSNR (original payload to extracted payload) also justifies the fact. The PSNR (cover to stego image) and capacity obtained in the proposed technique are compared with some of the existing approaches given by A. A. Ataby et al. [8] (PSNR: 40.98 dB, capacity: 0.7383), K. B. Shiva Kumar et al. [9] (PSNR: 50.3 dB, capacity: .25), E. Ghasemi et al. [10] (PSNR: 45.2 dB, capacity: 0.5), T. Bhattacharya et al. [11] (PSNR: 27.39 dB, capacity: 0.5), A. Ioannidou et al. [12] (PSNR: 46.88 dB, capacity: 0.2325) and Parul et al. [13] (PSNR: 49.5629 dB, capacity: 0.75). We can conclude that our results are consistent with the results of other analyses and in some cases these are even better.

IV. CONCLUSIONS

In the spatial domain image steganography schemes, the secret message is embedded in the cover image just by modifying the pixel values. The advantage of these methods is that the procedure is easy to implement and computationally fast. The disadvantage is its low ability to bear some signal processing or noises and the secret information can easily be stolen. In the frequency domain methods, the image data are transformed into frequency domain coefficients by some mathematical tools (FFT, DCT, DWT etc.). The confidential data are embedded into the coefficients in frequency domain. Then the modified coefficients are transformed back to spatial domain. Though these methods are computationally complex and slower, the stego images can bear some signal processing or noises and confidential data cannot be stolen easily. In this communication, a novel image steganography technique using first order Haar-DWT has been reported. Unlike existing Haar-DWT image steganography techniques where the secret information is embedded in the high frequency coefficients, the proposed method adopts hiding confidential data within all frequency bands. The proposed technique may be considered to be efficient as evident from the image assessment parameters.

REFERENCES

[1] N. F. Johnson, and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE Computer*, vol. 31, pp. 26-34, Feb. 1998.

[2] D. C. Lou, and J. L. Liu, "Steganography method for secure communications," *Elsevier Science on Computers & Security*, vol. 21, pp. 449-460, 2002.

[3] S. Channalli, and A. Jadav, "Steganography an art of hiding data," *International Journal on Computer Science and Engineering*, vol. 1, pp. 137-141, 2009.

[4] E. T. Lin, and E. J. Delp, "A review of data hiding in digital images," *in Proc. of the Image Processing, Image Quality, and Image Capture Systems Conference* (PICS '99), Georgia, 1999, pp. 274-278.

[5] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," [Online]. Available: http://www.ws.binghamton.edu/fridrich/Research/acm_2001_03.pdf

[6] P. Y. Chen, and E. C. Liao, "A new algorithm for Haar wavelet transform," *IEEE International Symposium on Intelligent Signal Processing and Communication System*, 2002, pp. 453-457.

[7] P. Y. Chen, and H. J. Lin, "A DWT based approach for image steganography," *International Journal of Applied Science and Engineering*, vol. 4, pp. 275-290, 2006.

[8] A. A. Ataby, and F. A. Naima, "A modified high capacity image steganography technique based on wavelet transform," *The International Arab Journal of Information Technology*, vol. 7, pp. 358-364, Oct. 2010.

[9] K. B. Shiva Kumar, K. B. Raja, and S. Pattnaik, "Hybrid domain in LSB steganography," *International Journal of Computer Applications*, vol. 19, pp. 35-40, Apr. 2011.

[10] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi, "High capacity image steganography using wavelet transform and genetic algorithm," *in Proc. of the International Multiconference of Engineering and Computer Scientist* (*IMECS*), 2011, vol. 1, pp. 1-4.

[11] T. Bhattacharya, N. Dey, and S. R. Bhadra Chaudhuri, "A novel session based dual steganographic technique using *DWT* and spread spectrum," *International Journal of Modern Engineering Research*, vol. 1, pp. 157-161, 2011.

[12] A. Ioannidou, S. T. Halkidis, and G. Stephanides, "A novel technique for image steganography based on a high payload method and edge detection," *Expert Systems with Applications*, Elsevier, vol. 39, pp. 11517-11524, 2012.

[13] Parul, Manju, and H. Rohil, "Optimized image steganography using discrete wavelet transform," *International Journal of Recent Development in Engineering and Technology*, vol. 2, pp. 75-81, Feb. 2014.

