Wavelet Steganography: An approach based on 3-level Haar Wavelet Transform

Dhanraj. R. Dhotre

Department of Computer Science and Engineering.
Shri Sant Gajanan Maharaj College of Engineering, Shegaon.
Sant Gadge Baba Amravati University, Amravati.

ABSTRACT

Secret communication over network has captured the imagination of researchers for many years. Steganography and Digital watermarking techniques are used to protect copyright information, address digital rights management, and conceal secrets. Secret data hiding techniques provide an interesting challenge for digital forensic investigations. Research into steganalysis techniques aids in the discovery of such hidden information as well as leads research toward improved methods for hiding information.

This paper presents a new approach of steganography based on Wavelet transform technique on raw images to enhance the security of the secret data.

Steganography is a technique to hide secret information into the image so as unknown to an attacker. The proposed method has ability to hide secret message in a digital color image. In this technique, the bits of secret information are embedded in the coefficients of the Haar Wavelet Transformed cover image. Haar wavelet transform is applied for the separation of different frequency components of image i.e. Low, medium low, medium high and high frequency components of image and these are called sub bands of image. After forming these sub bands we can select high frequency component band from the above four sub bands and embed the bits of secret information into the high frequency coefficient of the selected sub band.

To extract secret information apply wavelet transform on stego image, then select the embedded coefficients and extract the secret information bits from the high frequency coefficient. Without secret key nobody is able to extract the secret information from the stegoed image or even not proves the secret information present in the image. An experimental result shows that this approach perform better and improves the data embedding capacity by 15% approximately than 1-level,2-level haar wavelet methods.

General Terms

Security, Algorithms, Design, Embedding, Extraction, Performance, Experimentation, Verification.

Keywords

Steganography, Haar Wavelet Transform, high frequency coefficients, stego image, Pixel Value Differencing.

1. INTRODUCTION

With the increase of internet users and the growth of high-speed telecommunication secret information sharing such as digital information has been occurring widely by a large number of people [1, 2].

During data transmission, however, attackers will attempt to steal the data or destroy it. Initially cryptography was developed as a technique for secret communication and many different methods have been developed to encrypt, decrypt data in order to keep message or information secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret[1, 3]. Steganography is the technique to implement this. Steganography conceals the existence of a message by embedding it into various types of digital media i.e. text files, digital image audio files, video files etc. Numerous steganographic techniques are developed to hide the secret message into digital media [5, 13]. Encoding secret information in digital images is defining as the art and science of hiding secret information within image without any suspicion on this information and with satisfactory quality [2]. Image steganography is most widely used method in the internet communication, because it can take advantage of the limited power of human visual system [1, 2, 3 and 4]. Any secret message that can be encoded into a bit stream can be hidden in a digital image.

Grayscale images use 8 bits for each pixel and are able to display 256 different colors or shades of gray. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green, blue and each primary color is represented by 8 bits. One given pixel of color image is represented by 256 different quantities of red, green and blue, resulting in more than 16-million color combinations. The drawback of 8 bit images is that only 256 possible colors can be used which can be a potential problem during encoding, the gradual change in color will be harder to detect after the image has been encoded with the secret message. 24 bit images offer much more flexibility when used for Steganography. The large numbers of colors that can be used go well beyond the human visual system, which makes it very hard to detect once a secret message, has been encoded. The other benefit is that a much larger amount of hidden data can be encoded into a 24 bit digital image as opposed to an 8 bit digital image. By considering the flexibility, security and payload capacity of digital image, 24-bit color image are better than of 8-bit image as a cover image for embedding secret information [9, 10, 12, 15, 17 and 18].

In this work 24-bit color images of size 512 × 512 from the USC-SIPI Image database are used [16], in which plaintext as secret information is hidden. Proposed technique of steganography is implemented using 3-level 2-D Haar wavelet transform to hide secret message in gray and color images and results are compared. This method initially identifies the high frequency components in a cover image and embed secret message in it. It can be viewed as the process of combining cover image, secret message and stego key to get stego image. Embedded information is the secret information to be transferred over network together with cover image. Stego key is the shared secret between sender and receiver, additional secret embedded in cover image, which may be required during the extraction process of secret information. Stego

image is the resultant image generated after embedding secret information into cover image The proposed technique can recover the hidden message in lossless manner [4, 7, 8, 14 and 17].

As a performance measurement for image distortion, the well known Peak-Signal-to-Noise ratio (PSNR), which is classified under the difference distortion metrics, can be applied on the stego images. PSNR is often expressed on algorithmic scale in decibels (dB) [4].

2. INTEGER HAAR WAVELET TRANSFORM

Integer Haar Wavelet transform maps integers to integers instead of using the conventional wavelet Transforms. This can overcome the difficulty of floating point conversion that occurs after embedding. The separable 2-D Haar wavelet transform performs 1-D Haar wavelet transform in the horizontal direction, then performs 1-D Haar wavelet transform in the vertical direction to generate Low, medium low, medium high and high frequency components of image [7, 8, 11 and 17] as shown in figure 1 and 3- level haar wavelet decomposition of Lena image is shown in figure 2. Then gather the coefficients of the high frequency components to hide secret data.

2.1 DATA HIDING

For data hiding 3 level of wavelet decomposition is used. The 2-D integer Haar wavelet is applied to decompose the cover image. High-frequency components are used to hide message and higher level of Haar decomposition allows more bits to be embedded. 2-D haar wavelet transform can be performed by averaging and differencing of pixel blocks. Pixel value differencing process is equivalent to high-pass filtering and averaging is equivalent to low-pass filtering [4, 6, and 11].

For a pair of pixels (P_1, P_2), the lossless integer wavelet transform decomposes it into average *a* ie *low-pass* and difference *d* i.e. *high-pass* as given by following equation (1),

$a = \lfloor (P_0+P_1)/2 \rfloor$, $d = P_1-P_0$ with $|d| \in [0, 255]$ (1).

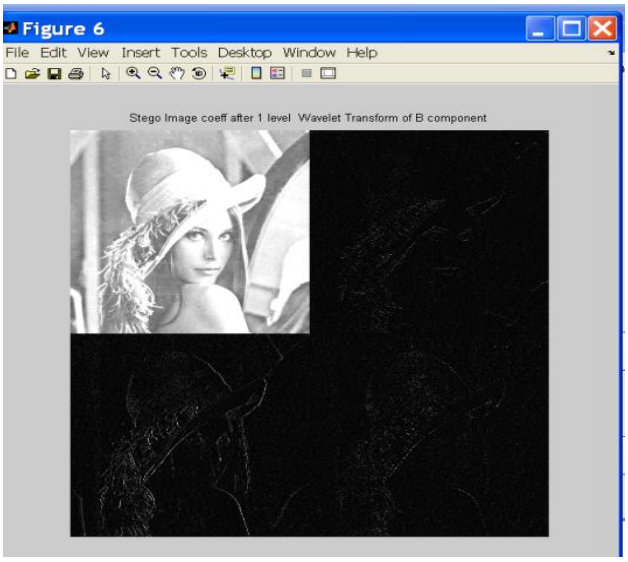

Figure 1. One level Haar wavelet Decomposition

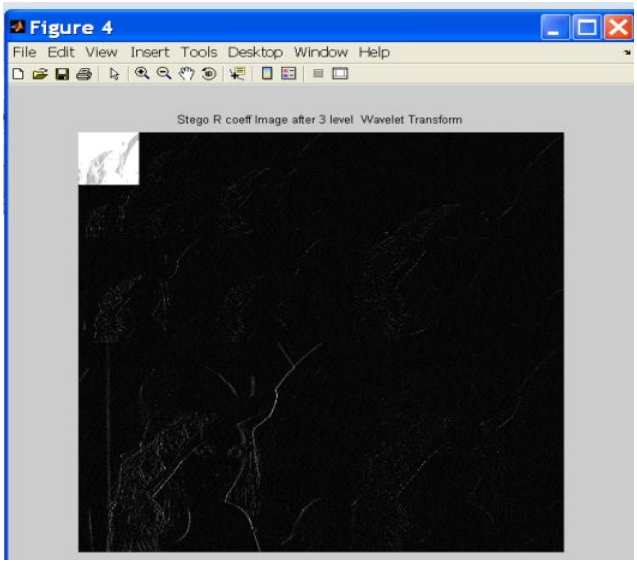

Figure 2. Three level Haar wavelet Decomposition of Lena image.

To hide data *w* secret bits are taken, to decide *w*, |*d*| is classified according to a set of continuous ranges *R*. The choice of R in this work is taken as given below

$$R = \{R_K = [l_k, u_k]\} = \{[0,7],[8,15],[16,31],[32,63],[64,127],[0128,255]\}.$$

The number of secret bits to be embedded in each range is given in the following set,

$$\{w_k = \log_2(u_k - l_k)\} = \{3,3,4,5,6,7\}.$$

If *d* is in R_k, then w_k secret bits are taken and convert to a decimal value *b*, then the new difference value *d'* is calculated by using equation (2) and (3).

$$d' = lk + b \quad \text{if } d \geq 0, \qquad (2).$$

$$d' = -(lk + b) \text{ if } d < 0, \qquad (3).$$

The average value is calculated by using the lifting equation (4)

$$a = a \quad \text{, if } d \text{ is even}$$

$$a = a + 0.5 \quad \text{, if } d \text{ is odd.} \qquad (4)$$

Then the inverse wavelet transform is computed by following equation to generate new pixel values

$$P_0' = a - 0.5d' \quad \text{and} \quad P_1' = a + 0.5d'. \qquad (5)$$

If the new pixel pair (P_0', P_1') is out of the range [0, 255] i.e. the new pixel value is out of the acceptable intensity value, then the block is labeled as unusable and restores its original pixel values (P_0, P_1) [6,4].

By equation 2, 3, 4 and 5 it can be shown that there is a one to one mapping between (P_0, P_1) and (*a*, *d*).

2.1.1 Process of data embedding

Execution steps used for the implementation of Haar Wavelet based embedding method for color images are given as follows.

1. Start.
2. Open cover image file.
3. Open the text message file to hide in cover image.
4. Apply the Haar Wavelet method to hide the message using 3rd level of Wavelet Decomposition to get high frequency bands.
5. Perform embedding process in high frequency coefficients and Inverse Wavelet Transform to display-
   a. cover image,
   b. decomposed image according to the level of wavelet decomposition,
   c. stego-image
   d. number of bits embedded in cover image,
6. Stop.

2.2 DATA EXTRACTION

To extract secret message from the stego image, reverse process of the embedding is to be applied. Apply wavelet transform on stegoed image, select the high frequency coefficient and extract secret information bits by applying the equations given in section 2.1. Extraction process is secure as nobody can be able to extract the secret message without key or even not proves the secret information present in the image.

2.2.1 Process of data Extraction

Steps used for data extraction are given as below.

1. Start.
2. Open cover image file.
3. Decompose the stego image by applying 3rd level Wavelet transform.
4. Perform extraction process in high frequency coefficients and display:
   a. decomposed stego-image according to the level of wavelet decomposition,
   b. extracted message,
   c. PSNR value.
5. Stop

3. EXPERIMENTAL RESULT

The experimental results show that, the data hiding capacities using proposed 3-level Haar Wavelet methods are significantly increased. The stego-image quality was measured using the PSNR. Susceptibility of the implemented methods is approved by examining the histogram. Experimental results are given in the following sections

3.1 Embedding Capacity Estimation

The proposed method is tested on Lena, F-16, Pepper and House images each of the size 512X512, from the USC-SIPI image database [18], and compares the capacity estimates with 1 and 2-level Haar Wavelet methods. Experimental results shows that on applying the proposed method on color images the capacity of data hiding is increased by 15 % approx., than other methods. Results for Lena image as shown in figure 5 are given in table 1 and embedding capacity comparisons for different images is shown in figure 6.

Figure 5. Lena image used to hide data.

Table 1. Results in terms of Capacity and PSNR for Lena image.

Method	Capacity (bits)	PSNR (db)
1-level Haar Wavelet	1816045	38.7357
2-level Haar Wavelet	2229158	35.3927
3-level Haar Wavelet	2416876	35.2241

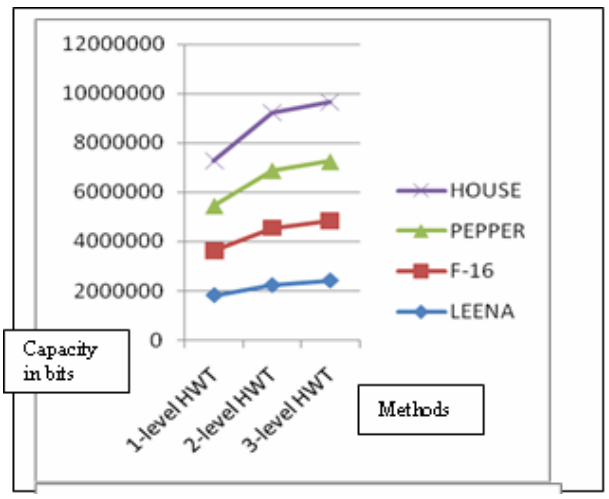

Figure 6. Embedding capacity comparisons for different images

3.2 PSNR

One of the major goals of data embedding is to let the cover image and the stego image be perceptually similar. There are various image quality measures to compare two images. Among them, the most widely used is the Peak Signal-to-

Noise Ratio (PSNR), which is defined by the equation (6) and (7).

$$PSNR = 10 \times \mathrm{Log}_{10} \frac{255^2}{\mathrm{MSE}} \quad (6)$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(x(i,j) - y(i,j)\right)^2 . \quad (7)$$

Where x is the cover image, y is stego image; M and N are the dimensions of the images. Higher PSNR represents better image quality. In general, PSNR above 30 db is considered to be acceptable [4].

4. CONCLUSION

The 3-level 2D haar wavelet transform based method is proposed for embedding secret data in images. In results it is shown that this method increases the embedding capacity of color images than the 1-level and 2-level methods, also it shows that the house image outperforms in embedding capacity as compared to other images.

5. ACKNOWLEDGMENTS

Our sincere thanks to Dr. V. N. Gahokar for supporting this research work and Prof. S. V. Paranjpe for valuable suggestions and getting familiar with haar wavelet transform.

6. REFERENCES

[1] Johnson, N. F. and Jajodia, S. "Exploring steganography: Seeing the unseen", IEEE Computer Journal, vol. 31 no. 2, pp. 26–34, 1998.

[2] Niels Provos, Peter Honeyman, "Hide and Seek: Introduction to Steganography" , IEEE Transaction on Security & privacy, vol. 1, no. 3 pp. 32-44, 2003.

[3] Potdar, V., Chang E., "Grey level modification steganography for secret communication", Proceedings of IEEE Conference on Industrial Informatics, pp. 223-228, 2004.

[4] Jen-Chang Liu , Ming-Hong Shih, "Generalizations of pixel-value differencing steganography for data hiding in images", Elsevier Journal on Pattern Recognition Letters, vol. 83, no. 3, pp. 319-335, 2008.

[5] Bender, W., Gruhl, D.,Morimoto, N., Lu A., "Techniques for data hiding" , IBM System Journal, vol. 35, no. 4, pp. 313-336, 1996.

[6] Colm Mulcahy, "Image compression using the Haar wavelet transform", Spelman Science and Math Journal , vol. 1, no. 4, pp. 22-31, 1995.

[7] Henk Heijmans and Lute Kamstra, " Reversible Data Embedding Based on the Haar Wavelet Decomposition", Proceedings of VII th IEEE conference on Digital Image Computing: Techniques and Applications, pp. 10-12, 2003.

[8] Jianyun Xu, Andrew H. Sung, Peipei Shi, Qingzhong Liu, "JPEG Compression Immune Steganography Using Wavelet Transform", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) pp. 7695-2108, 2004.

[9] Cox, I.J., Miller, M.L., Bloom, J.A., "Digital watermarking", Academic Press, vol. 4, pp. 68-74, 2002.

[10] Wu, M., Liu, B., "Data hiding in image and video: part I – fundamental issues and solutions", IEEE Transaction on Image Processing, vol. 12, no.3, pp. 685-695, 2003.

[11] Dewitte, S., Cornelis, J., "Lossless integer wavelet transform", IEEE Transaction on Signal Processing, vol. 4, no. 6, 1997.

[12] Masry, M., Ramos, M., Hemami, S.S., "Robust data hiding using psychovisual thresholding" , Processing IEEE International Conference Image Processing, vol. 1, pp. 593-596, 2000.

[13] Norishige Morimoto, "Digital Watermarking Technology with Practical Applications" Information science special issue of Journal on Multimedia Informing Technologies part1, vol. 2, no. 4 pp. 107-111, 1999.

[14] Kessler, G., "An Overview of Steganography for the Computer Forensics Examiner", Computer & Digital Forensics Program, Champlain College, Burlington, Vermont, February 2004.

[15] Fridrich, J., Goljan, M., Du, R., "Detecting LSB steganography in color, and gray scale images", IEEE Transaction on Multimedia, vol. 8, no. 4, pp. 22-28,2001.

[16] Standard Test Images from USC-SIPI Image Database, available on http:\\www.usc-sipi.com.

[17] M. F. Tolba, M. A. Ghonemy, I. A. Taha, and A. S. Khalifa , "Steganography using Integer wavelet Transform in Colored Image Steganography" IJICIS vol. 4, no. 2, pp. 75-85, 2004.

[18] C.K. Chan. L.M. Cheng, "Hiding data in images by simple LSB substitution", Elsevier Journal on Pattern Recognition, vol. 37, no.3, pp. 469-474, 2004.