

(An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 12, December 2015

Stationary Wavelet Transform Based Steganography for Transmitting Images

Mrunalini Madhavrao Chaudhari¹, Prof.K.N. Pawar²

P.G. Student, Department of Electronics Engineering, S.V.P.S.B.S.D College of Engineering, Dhule, India¹

Head of Department of Electronics Engineering, S.V.P.S.B.S.D College of Engineering, Dhule, India²

ABSTRACT: Steganography gained importance in the past few years due to the increasing need for providing secrecy in an open environment like the internet. With almost anyone can observe the communicated data all around, steganography attempts to hide the very existence of the message and make communication undetectable. Many techniques are used to secure information such as cryptography that aims to scramble the information sent and make it unreadable while steganography is used to conceal the information so that no one can sense its existence. In most algorithms used to secure information both steganography and cryptography are used together to secure a part of information. Steganography has many technical challenges such as high hiding capacity and imperceptibility. In this paper a novel Steganographic technique using Stationary Wavelet Transform (SWT) for transmitting pictures is proposed. Two different techniques are proposed, single level and three level wavelet decomposition taking a single plane of the cover image for embedding and processing the image as 4 x 4 blocks with swapping and using single level wavelet decomposition. Experiments show that Peak Signal Noise Ratio (PSNR) generated by the proposed method is better than those generated by the existing schemes.

KEYWORDS: Pre-processing, Stationary Wavelet Transform, Embedding, Extraction, Parameter analysis (PNSR, MSE).

I. INTRODUCTION

Steganography is the art and science of hiding data in a cover. The cover can be text, audio, image, video, etc. We can divide the data hiding techniques into two groups: spatial and frequency domain [1-3]. The first group is based on embedding message in the Least Significant Bits (LSB) of image pixels. The basic LSB method has a simple implementation and high capacity [4]. However, it has low robustness versus some attacks such as low-pass filtering and compression [5]. A variant of LSB method can be found in [6] that propose an Optimal Pixel Adjustment Process (OPAP) in which image quality of the stego-image can be improved with low computational complexity. The group finds the frequency coefficients of images and then embeds the messages with them. These hiding methods overcome the robustness and imperceptibility problem found in the spatial domain.

JPEG, a standard image compression technique, employs Discrete Cosine Transfonn (DCT). Several steganography techniques for data hiding in JPEG have been proposed; such as JSteg [7], JP Hide&Seek [7] and OutGuess [8]. Most recent researches utilize Discrete Wavelet Transfonn (DWn because of its wide application in the new image compression standard, JPEG2000. An example is the employment of an adaptive data embedding technique with the use of OPAP to hide data in Integer Wavelet coefficients of the cover image [9].

The application of Genetic Algorithm in steganography can increase the capacity or imperceptibility [10-12]. Fard, Akbarzadeh and Varasteh [11] proposed a GA evolutionary process to make secure steganography encoding on the JPEG images. Rongrong et al [12] introduced an optimal block mapping LSB method based on Genetic Algorithm.



(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

II. LITERATURE SURVEY

1. A new Image Steganography scheme is proposed in this paper. Based on different requirements of applications, two operation modes and 5 cases are provided for selection. According to the simulation results, the PSNR is still a satisfactory value even the highest capacity case is applied. This is due to the different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the original image).

2. In this paper, we observe the effect of embedding the secret messages into different bands of cover image. Experimental results show that error block replacement in diagonal detail coefficients (CD) gives better Peak Signal to Noise Ratio (PSNR) as compared to PSNR obtained when using the replacement with other coefficients (CV and CD).

3. Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The methods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of the computer era. Although the techniques are still not used very often, the possibilities are endless. Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly. Since detection can never give a guarantee of finding all hidden information, it can be used together with methods of defeating steganography, to minimize the chances of hidden communication taking place. Even then, perfect steganography, where the secret key will merely point out parts of a cover source which form the message, will pass undetected, because the cover source contains no information about the secret message at all. In the near future, the most important use of Steganographic techniques will probably lie in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down.

4. The color quantization algorithm proposed here is quasipreserving of luminance information. In general, most color quantization algorithms are based on multidimensional data processing, which ignores the meaning of the color axis. On the other hand, the color quantization algorithm presented here uses the characteristics of the human visual system as much as possible. This is a difference between our color quantization and conventional methods.

III. IMAGE TYPES

There are three type of image, which is described below.

3.1 Binary image

Logical array containing only 0s and 1s, interpreted as black and white, respectively.

3.2 Grayscale image

It is also known as an intensity, gray scale, or gray level image. Array of class uint8, uint16, int16, single, or double whose pixel values specify intensity values. For single or double arrays, values range from [0,1]. For uint8, values range from [0,255]. For uint16, values range from [0,65535]. For int16, values range from [-32768, 32767].

3.3 True color image

It is also known as an RGB image. A true color image is an image in which each pixel is specified by three values one each for the red, blue, and green components of the pixel scalar. M by -n-by-3 array of class uint8, uint16, single, or



(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

double whose pixel values specify intensity values. For single or double arrays, values range from [0, 1]. For uint8, values range from [0, 255]. For uint16, values range from [0, 65535]

RGB to Gray conversion

To convert a (RGB) color image in to Gray scale we have to use the following formula.

Intensity = 0.2989*red + 0.5870*green + 0.1140*blue (1)

IV. PROPOSED METHOD

In this paper a novel Steganographic technique using Stationary Wavelet Transform for transmitting pictures is proposed .Two different techniques are proposed one using three level wavelet decomposition and another using single level wavelet decomposition. Take the secret image and turn it into black and white. Then apply embedding process as well as inverse transform for getting stego image.

Block diagram:



Fig1. Block diagram of proposed method

4.1 Median Filtering Technique

Median Filter [1] is an image filter that is more effective in situations where white spots and black spots appear on the image. For this technique the middle value of the m×n window is considered to replace the black and white pixels.

When white spots and black spots appear on the image, it becomes very difficult to guess which pixel is the affected one. Replacing those disturbing pixels with AMF, GMF and HMF are not sufficient because those pixels are replaced by a value which is not appropriate to the original one. We have seen over the distorted images that Median Filter has better influence than that of AMF, GMF and HMF, where AMF is the best among all the mean filtering techniques and HMF has the worst performance.

4.2.1 Algorithm of Embedding using Three Level Wavelet Decomposition

1. Perform three level 2D-Haar SWT decomposition as follows:

a) Take the cover image (JPEG) (512 x512) and its green plane alone and perform first level 2D-SWT on the image to obtain approximation 1 coefficient (LL 1), horizontal 1 coefficient (HL 1), vertical 1 coefficient (LH 1), diagonal 1 coefficient (HH1) respectively.



(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

b) Take the approximation 1 coefficient (LLl) and perform second level 2D-SWT on the image to obtain approximation 2 coefficient (LL2), horizontal 2 coefficient (HL2), vertical 2 coefficient (LH2), diagonal 2 coefficient (HH2) respectively.

c) Take the approximation 2 coefficient (LL2) and perform third level 2D-SWT on the image to obtain approximation 3 coefficient (LL3), horizontal 3 coefficient (HL3), vertical 3 coefficient (LH3), diagonal 3 coefficient (HH3) respectively.

2. Take the secret image and turn it into black and white.

- 3. Perform Embedding as follows:
- a) Assume an embedding coefficient of value of 0.05.
- b) Process LL3 block by block (4x4).
- c) Process the secret image block by block (4X4).

d) The following formula is used to obtain the secret image block (4x4) which is basically swapping, Secret image block «(1-Embedding Coefficient) x LL3 intensity value) + (Embedding coefficient x secret image intensity value).

4. Perform three level 2D-Haar inverse SWT for reconstruction which is the inverse process of three level 2D-Haar SWT decomposition in order to obtain the stego image.

5. Calculate the PSNR value in order to check for the visual quality of the stego image.

4.2.2 Algorithm of Embedding using Single Level Wavelet Decomposition

1. Take the original image and the secret image and take the Red (R) plane separately and perform single level 2D-Daubechies SWT decomposition on the original image as well as the secret image.

2. Assume a embedding co-efficient a of value ranging from 0 to 1, coefficient of a, large increase in robustness, small increase in transparency.

3. To find the approximation co-efficient, horizontal co-efficient, vertical co-efficient and diagonal coefficient of the embedded image use the formula:

Approximation co-efficient of the embedded image = $(1-a)^*$ Approximation coefficient of the original image $+a^*$ Approximation coefficient of the secret image.

Similarly the same is used to find the horizontal co-efficient, vertical co-efficient and diagonal co-efficient of the embedded image.

4. Perform single level 2D- Daubechies inverse SWT decomposition on the calculated approximation, horizontal, vertical and diagonal coefficients to get the approximation, horizontal, vertical and diagonal coefficients of the R plane of the embedded image.

5. The above mentioned procedure is done for the Green(G) plane and Blue(B) plane separately

6. Concatenate Red (R), Green (G) plane and Blue (B) plane to get the embedded image.

V. METRICS MEASUREMENT

The discussed algorithms are tested with different variety of images. The performance of the algorithm is evaluated quantitatively using the measures viz. mean square error (MSE), peak signal to noise ratio (PSNR in dB). MATLAB 7.0 (R14) on a PC equipped with 2.13-GHz CPU and 2 GB of RAM memory has been employed for the evaluation of computation time of all algorithms. The values are tabulated.



(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \{x(i,j) - y(i,j)\}^{2}$$
(2)

 $PSNR=20 \times \log_{10}(255/\sqrt{MSE})$

S. no	Cover image	Logo image	Logo size	MSE	PSNR
1	1.jpg	Logo2.jpg	512 x 512	5.796	32.8678
2	Lena.png	Logo2.jpg	512 x 512	4.816	34.4759
3	3.jpg	Logo2.jpg	512 x 512	8.705	29.3350

S. no	Cover image	Logo image	Logo size	MSE	PSNR
1	4.jpg	12.bmp	256 x 256	2.3934	84.3406
2	1.jpg	12.bmp	256 x 256	1.8475	85.4650
3	3.jpg	12.bmp	256 x 256	0	100

(3)

Table1. Embedding using Three Level Wavelet Decomposition

		8	
S.no	Cover image	Logo image	Correlation
			coefficient
1	1.jpg	Logo2.jpg	0.9897
2	Lena.png	Logo2.jpg	0.9498
3	3.jpg	Logo2.jpg	0.9903

Table2.Embedding using Single Level Wavelet Decomposition

S.no	Cover image	Logo image	Correlation coefficient
1	4.jpg	12.bmp	1
2	1.jpg	12.bmp	1
3	3.jpg	12.bmp	1

Table3. Extraction using Three Level Wavelet Decomposition

Table4. Extraction using Single Level Wavelet Decomposition

VI. EXPERIMENTAL RESULTS

Below figures shows the results of steganography using three level and single level wavelet transform. Fig.2 & 3 Shows three level wavelet decomposition. Fig.4 Shows single level wavelet decomposition.



Fig2. Embedding using Three Level Wavelet Decomposition



Fig3. Extraction using Three Level Wavelet Decomposition



(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015



Fig4. Embedding Extraction using Single Level Wavelet Decomposition

VII. CONCLUSION

In this paper, a new image data hiding technique based on stationary wavelet transform has been proposed. The stegoimage is looking perfectly intact and has high peak signal to noise ratio value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image is perceptually similar to the original secret image.

In this paper two different techniques namely

1. Using three level stationary wavelet transform.

2. Using single level stationary wavelet transform for hiding images has been proposed and implemented. The relative analysis between the proposed technique and the other existing techniques has shown the pre-eminence of the proposed technique.

REFERENCES

- [1] A. Z. Tirket, R.G. Van Schyndel, C. F. Osborne, "A digital watermark," Proceedings ofiCIP, Austin Texas, Vol. II, 1994, pp. 86-90,1994
- [2] W. Bender, N. Morimoto, "Techniques for data hiding," IBM Sys. J. 35(3/4) (1996) 313-336.
- [3] K. L. Chung, C.H. Shen, L. C. Chang, "A novel SVD and VQ- based image hiding schem," Pattern Recognition Let. 22(9) 1051-1058 July 2001.
- [4] N. Wu and M. Hwang, "Data hiding: current status and key issues," International Journal of Network Security, vol4, No.1, pp. 1-9, Jan. 2007.
- [5] W. Chen, "A comparative study of information hiding schemes using amplitude, frequency and phase embedding," PhD thesis, National Cheng Kung University, Taiwan, May 2003
- [6] C. K. Chan and L. M. Chang, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.
- [7] N. Provos, P. Honeyman, "Hide and Seek: an introduction to steganography," IEEE Computer Society, pp. 32-44, May-June 2003.
- [8] Banoci, V.; Bugar, G.; Levicky, D. A novel method of image steganography in DWT domain, Radioelektronika, 20 II 21 st International Conference
- [9] Kumar, V., Kumar, D,Performance evaluation of DWT based image steganography, Advance Computing Conference (IACC), 2010 IEEE 2nd International
- [10] Po-Yueh Chen, Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290
- [11] Wang, H, Wang, S, "Cyber warfare: steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004
- [12] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002
- [13] Nan-I Wu, Min-Shiang Hwang Data Hiding: Current Status and Key Issues, International Journal of Network Security, Vol.4, No.1, PP.I-9, Jan. 2007
- [14] Foley, J., et al., Computer Graphics, Principles and Practice, Reading, MA: Addison Wesley, 1990. Bender, W., D. Gruhl, N. Morimoto, "Techniques for data hiding," iBM Systems Journal, vol. 35, no. 3/4, 1996, pp. 131-336.