VOL. 10, NO. 14, AUGUST 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ROBUST IMAGE STEGANOGRAPHY BY EMBEDDING SELECTIVE INTRINSIC MODE FUNCTIONS WITH DISCRETE WAVELET TRANSFORM

S. Senthil Kumar[1] and K. Palani Thanaraj[2]
[1]Department of Electronics and Communication Engineering, Agni College of Technology, Chennai, India
[2]Department of Electronics and Instrumentation Engineering, St. Joseph's College of Engineering, Chennai, India
E-Mail: sskpuliyur@gmail.com

ABSTRACT

Steganography is the method of embedding information in a carrier medium for secure transmission. Steganography enables protection of confidential data that arise in many military and communications systems, online retail and banking systems, medical data transmission etc. This paper focuses on medical image steganography that involves hiding a secret medical image into a cover image thereby preserving patient privacy. In this work improvements to discrete wavelet transform (DWT) based steganography is attempted in different clinical settings. Here we propose to combine DWT with empirical mode decomposition (EMD) at different frequency scales for robust and secure image steganography. Initial step involves decomposing the cover and secret image to predefined approximation level using DWT. Then the approximate secret image is decomposed to intrinsic oscillating modes that contain details at different frequency scales. A selection procedure is initiated in this stage where the user can embed the secret image at different detail level based on the application requirements. The predefined intrinsic modes of secret image are embedded in the cover image by a linear mixing model. Then inverse DWT is applied to reconstruct the stegano image. Performance assessment of the proposed method is carried out (6.5% of payload) with image quality metrics such as peak signal to noise ratio (PSNR), mean Square Error (MSE), maximum absolute error (MAXERR) and ratio of squared norms (L2RAT) are tabulated and compared with DWT based steganography. Our study shows that proposed method can be a robust tool in secure transmission of secret images.

Keywords: image steganography, discrete wavelet transform, empirical mode decomposition, intrinsic mode functions.

INTRODUCTION

Steganography is the science of transmitting confidential data by embedding in a carrier image. The idea behind this is to mainly counter the blind attacks that are on the rise due to recent developments in communication media. Since most of the data transmitted through internet are digital, there are high chances for it to be illegally used or copied. To avoid such illegal incidents, it is necessary to have a secure communication through the internet. Steganography provides secrecy by hiding the secret data into another medium before transmitting it to the end user (Cheddad *et al.* 2010). This method has been proved to provide a secure communication through the internet. There are various types of Steganography that is currently used for carrying a wide variety of payloads such as text data, image data, voice and video data. Based on the nature of carrier medium steganography can be classified as text steganography, image steganography, video steganography and audio steganography (Bachrach and Shih, 2011).

The type of steganography depends on the type of secret data need to be transmitted to the end user. Most of the existing steganography methods rely on two factors: a) the secrecy of the key and b) the robustness of the steganography algorithm (Li *et al.* 2011) . Robustness is defined as the ability of the hidden data to withstand against intentional and unintentional attacks in noisy transmission environment. In this paper the usage of image steganography for medical applications is investigated. Confidential patient data are stored in Picture Archival and Communication Systems (PACS). This medical data is an electronic media that is transmitted to physician for patient analysis. This is accessible by the patient and physicians anywhere (Ibaida and Khalil, 2013). This added facility comes with a bottleneck of privacy issues. So secrecy of patient data has to be maintained. In this perspective we have taken the studies on hiding a patient anatomical Magnetic Resonance Imaging (MRI) into another cover image thereby blocking unwanted attacks that questions the privacy of patients. For a secure communication, the quality of the stego-image must be high so that the attackers would not find any difference between the stego-image and the cover image. This shows the need for robustness of the steganographic method for a secure communication. There are many techniques used in steganography that can be found in current literature.

Information hiding schemes in carrier images can be broadly classified as 1) pixel based methods 2) transform based methods. Least significant bit (LSB) substitution is a common pixel based steganography that hides information in the LSB of the carrier data (Chan and Cheng 2004). It provides high payload capacity with

minimal computation complexity *(Xia et al*. 2011). LSB method is modified for wide range of carrier medium such as text, voice and video (Kessler and Hosmer 2011). Another widely used method is transform based steganography that embeds the secret data in the transform coefficients. These methods provide high security by performing encryption operation in the transform domain. Discrete cosine transform (DCT) and Discrete wavelet transform (DWT) are predominantly used methods for image steganography (Chandramouli, Kharrazi, and Memon, 2003). In this paper a novel attempt is made to improve DWT based image hiding scheme by combining with Bidimensional Empirical mode decomposition (BEMD). The secret image is transformed to intrinsic mode functions (IMFs) that contain important features at different scales. This approach provides flexibility in transmitting the required information content of the secret image.

METHODOLOGY

Image decomposition

The Discrete Wavelet Transform (DWT) is used to decompose the image data to predefined approximation level (Zhiweil *et al.* 2007). DWT decomposes the image into various spectral bands (low pass and high pass components) of details. Initially, the cover and secret image is transformed from spatial domain to frequency domain in this method. It uses different types of mother wavelet that is scaled and shifted to capture the details of the image at different time and frequency scales.

$$W(n,m) = \frac{1}{\sqrt{a}} \sum f(x,y) \Psi \left[\left(\frac{k}{a} - m \right) T \right] \quad (1)$$

here, $\Psi(x)$ represents the mother wavelet and *'n','m'* are wavelet parameters. There are various types of mother wavelet functions that are commonly used such as Haar wavelet, Daubechies, Legendre and Symlet. In our proposed method Haar-wavelet as shown in Figure-1 is used.

$$\psi(x) = \begin{cases} 1 & 0 \le x < \frac{1}{2} \\ -1 & \frac{1}{2} < x \le 1 \\ 0 & otherwise \end{cases} \quad (2)$$

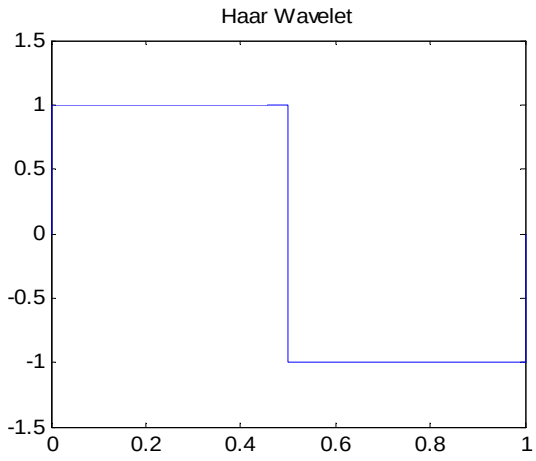

Figure-1. Haar wavelet.

In 2D-DWT the decomposition process is a two stage process. Initially 1D-DWT is first applied to columns and then to rows. The first one is the vertical decomposition operation and the second one is the horizontal decomposition operation (Rekik et al. 2012). Each pixel in each row is first added and subtracted with its neighboring pixels and the added sum is denoted as 'L' and the subtracted sum is denotes as 'H'. It represents Low and High frequency components of the image respectively. In the same way the pixels in each column is added and subtracted with its neighboring pixels. Dyadic low pass and high pass filters are used for this operation. Since each filter is half band the frequency is down sampled by a factor of two at every stage. The above mentioned process is illustrated in Figure-2.

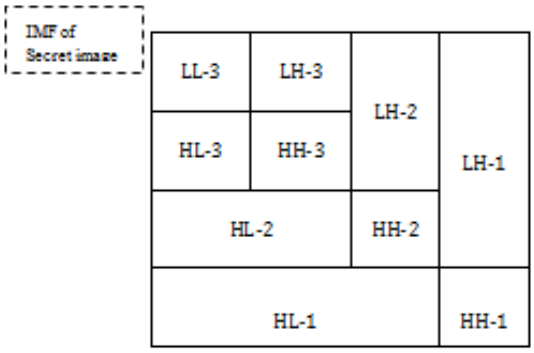

Figure-2. DWT image decomposition.

The output of DWT at first decomposition level consist of first level approximate image coefficients and detailed image coefficients. As noises are high frequency components the original data that lies on the low frequency part is used to carry the secret image without any visual degradation in the cover image statistics.

Embedding process

a) The process flow of the image encryption step is shown in Figure-3. Two-dimensional separable dyadic DWT is first applied to predefined level of decomposition for the cover and secret images. Level of decomposition is selected to be 3 in this work.

b) The 3rd level approximate coefficients of secret image are then transformed to intrinsic mode functions (IMF) by using Bidimensional EMD (Damerval, Meignen, and Perrier, 2005; Nunes, 2003).

c) IMFs contain details of the input data at different frequency scales (Flandrin, Rilling, and Goncalves, 2004; Huang, 2001). Lower order IMFs contain high frequency features such as edges and higher order IMFs contain smoothened texture features. The procedure for BEMD is given in the section below (Rehman and Mandic, 2009).

Bidimensional EMD procedure

1. Compute local extrema (minima and maxima) of the input image $f_{(x,y)}$
2. Perform 2 dimensional spline interpolations to form the lower $f^{l}_{(x,y)}$ and upper $f^{u}_{(x,y)}$ envelopes.
3. Compute the local mean of the input image
$$m_{(x,y)} = \frac{f^{l}_{(x,y)} + f^{u}_{(x,y)}}{2}$$
4. Subtract the local mean from $f_{(x,y)}$ to get
$$d_{(x,y)} = f_{(x,y)} - m_{(x,y)}$$
5. If $d_{(x,y)}$ is less than the stopping criteria σ such that $\sum_{i \in k} \frac{\left[d^{i}_{(x,y)} - d^{i-1}_{(x,y)}\right]^2}{d^{i-1\ 2}_{(x,y)}} < \sigma$ then $d_{(x,y)}$ is the first intrinsic mode function and the first residue is $r_{(x,y)} = f_{(x,y)} - d_{(x,y)}$
6. Repeat the procedure by iterating on the residue till it ends in a monotonic function.

d) The obtained IMFs are analyzed and few modes that carry vital information are embedded in the cover image. Figure-4 shows different IMFs of the secret image (MRI). The selected IMFs are linearly mixed with the cover image for the next step. Here inverse DWT is applied to obtain the stegano cover Image.

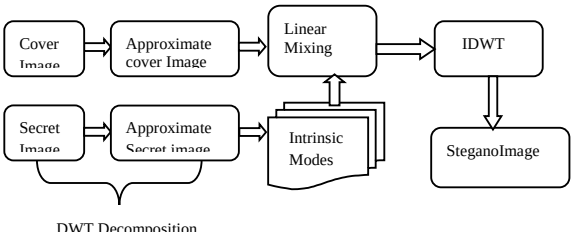

Figure-3. Embedding operation.

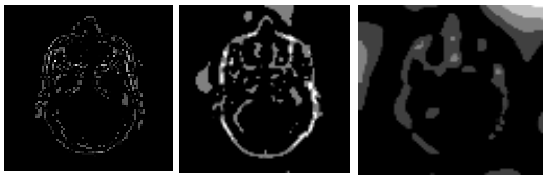

Figure-4. IMFs of secret image.

Extraction process

a) The steps involved in the extraction process are illustrated in Figure-5.

b) The received stegano image (possibly attacked) is decomposed using two-dimensional separable dyadic DWT similar to the embedding process.

c) The approximate image of the transmitted stegano image after 3 levels of decomposition is obtained.

d) Then the recovered stegano image is subtracted with the cover image key to get the secret image.

$$Secret = LL3_{Stegano} - LL3_{cover} \quad (3)$$

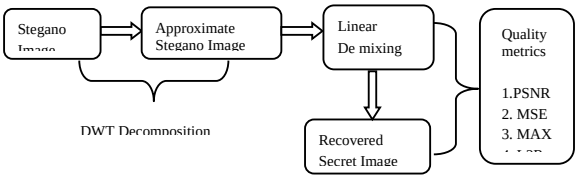

Figure-5. Extraction process.

PERFORMANCE MEASURES

Steganography methods used in the encryption of secret images are required to maintain original cover image statistics so that visual degradation is kept minimal low. Many performance measures are reported in the

literature that quantifies the image quality (Wang and Wang 2004; Kumar and Kumar 2010). The following section explains the performance metrics used in this work.

Mean Square Error (MSE)

MSE quantifies the difference between the cover image and the stego image. The formulation of MSE is given as follows:

$$MSE = \frac{\sum_{m,n}[I_C(m,n) - I_{Steg}(m,n)]^2}{m*n} \quad (4)$$

Here *'Ic'* represents the cover image and 'I_{steg}' is the stego image and *'m,n'* are the number of rows and columns in the input images respectively.

Peak Signal -To-Noise Ratio (PSNR)

PSNR is another widely used image quality metric that is expressed as the ratio of maximum gray scale intensity to MSE. It is expressed as shown in the equation below.

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad (5)$$

Peak Signal-to-Noise Ratio (PSNR) assess the quality of stego-image with respect to the cover image. PSNR is measured in decibels (dB).

Maximum absolute error (MAXERR)

Maximum Absolute Error (MAXERR) is the maximum absolute squared deviance of the data (original image) from approximation image (steganoimage).

$$MAXERR = \left\| I_C - I_{steg} \right\|^2 \quad (6)$$

Ratio of squared norms (L2RAT)

L2RAT is the ratio of the squared norms (energy) of the cover image to the steganoimage. It is defined by the following equation.

$$L2RAT = \frac{\left\| I_{steg} \right\|^2}{\left\| I_{cover} \right\|^2} \quad (7)$$

RESULTS AND DISCUSSIONS

The secret image used in our work is a medical magnetic resonance image (MRI) of an anonymous patient and the cover images are standard test images. The images are of dimension 256X256. The cover and secret images are scaled to dimension of 2048x2048 as DWT down samples the data by factor of 2. The information hiding is done in the approximate level-3 of the decomposed cover image as it is immune to high frequency noises. In the proposed method only important features of the secret image is embedded into the cover image for data transmission. This improves the performance of the steganographic method.

2D-EMD method is used to select the prominent texture features of the secret image. EMD is a fully data driven method that decomposes the data to orthogonal intrinsic mode functions. Here low order IMFs namely 1, 2 and 3 levels are selected for the embedding process. The cover image and IMFs of the secret image are linearly mixed. Then inverse DWT is performed to obtain the final steganographic image. Figure-6 shows the stegano images that are embedded with the secret image (MRI).

Figure-7 shows the stegano images using conventional DWT. Visual comparison between the methods reveal that DWT shows some form of image degradation with a payload of 6.5% of secret data. Table-1 shows the performance metrics of proposed algorithm (DWT-BEMD). Combination of DWT with Bidimensional EMD proves to be robust to hide images for effective data transmission. Thus the proposed algorithm uses the benefits of DWT and EMD in efficient transmission of medical images that can overcome unwanted intrusion.

CONCLUSIONS

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient suspects the existence of the message. In this paper, MRI Image (secret image) is hidden into cover image using discrete Wavelet transform and 2D-EMD. Performance parameters such as Mean Square Error (MSE), Maximum Absolute Error (MAXERR), L2RAT (Ratio of Squared Norms) and Peak-To-Signal Noise Ratio (PSNR) are tabulated for various carrier medium (Huynh-Thu and Ghanbari, 2008; Thung and Raveendran, 2009).

Figure-6. Stegano images using proposed DWT-BEMD.

Figure-7. Stegano images using DWT.

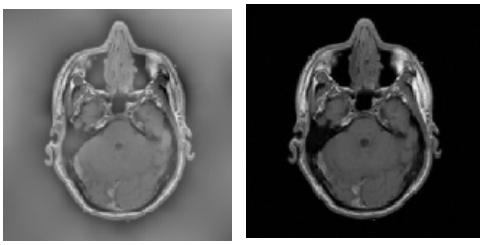

Figure-8. Recovered secret image a) DWT-BEMD b) DWT.

Table-1. Performance analysis of the DWT-BEMD with DWT.

Cover image	Secret image	PSNR (dB)		MSE		MAXERR		L2RAT	
		DWT BEMD	DWT	DWT BEMD	DWT	DWT BEMD	DWT	DWT BEMD	DWT
Lena	MRI	99.8094	85.5764	6.7913e-06	1.8007e-04	0.0151	0.0619	1.0006	1.0281
Cameraman		99.8091	85.5766	6.7924e-06	1.8002e-04	0.0153	0.0621	1.0009	1.0228
House		99.8093	85.5761	6.7976e-06	1.8010e-04	0.0151	0.0615	1.0010	1.0223
Airplane		99.8093	85.5764	6.7911e-06	1.8001e-04	0.0157	0.0612	1.0004	1.0196
Vegetables		99.8096	85.5770	6.7933e-06	1.8006e-04	0.0152	0.0619	1.0011	1.0292

The study shows that DWT and EMD can be combined to improve the robustness and security of the image steganography. The idea behind the proposed method is selective embedding of secret image features (IMFs) can improve the payload capacity of DWT based steganography. As only few IMFs are used for image hiding there is a loss of image contrast in the recovered images as shown in Figure-8. Further improvements to the proposed method are needed to improve the image contrast and to reduce the impact of stegano-analysis such

as detection of secret images and destruction of stegano images by adding Gaussian random noises.

REFERENCES

Bachrach Mayra and Frank Y. Shih. 2011. Image Steganography and Steganalysis." Wiley Interdisciplinary Reviews: Computational Statistics. doi:10.1002/wics.152.

Chan Chi Kwong and L. M. Cheng. 2004. Hiding Data in Images by Simple LSB Substitution. Pattern Recognition 37: 469-74. doi:10.1016/j.patcog.2003.08.007.

Chandramouli R., M. Kharrazi and N. Memon. 2003. Image Steganography and Steganalysis: Concepts and Practice. Lecture Notes in Computer Science. 35-49. doi:10.1007/978-3-540-24624-4_3.

Cheddad Abbas, Joan Condell, Kevin Curran and Paul Mc Kevitt. 2010. Digital Image Steganography: Survey and Analysis of Current Methods. Signal Processing. doi:10.1016/j.sigpro.2009.08.010.

Damerval Christophe, Sylvain Meignen and Valérie Perrier. 2005. A Fast Algorithm for Bidimensional EMD. IEEE Signal Processing Letters. 12(10): 701-4. doi:10.1109/LSP.2005.855548.

Flandrin P., G. Rilling and P. Goncalves. 2004. Empirical Mode Decomposition as a Filter Bank. IEEE Signal Processing Letters 11(2). doi:10.1109/LSP.2003.821662.

Huang Norden E. 2001. Review of Empirical Mode Decomposition. In Proceedings of SPIE. 4391: 71-80. doi:10.1117/12.421232.

Huynh-Thu Q. and M. Ghanbari. 2008. Scope of Validity of PSNR in Image/video Quality Assessment. Electronics Letters. doi:10.1049/el:20080522.

Ibaida Ayman and Ibrahim Khalil. 2013. Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems. IEEE Transactions on Biomedical Engineering 60: 3322-30. doi:10.1109/TBME.2013.2264539.

Kessler Gary C. and Chet Hosmer. 2011. An Overview of Steganography. Advances in Computers. Vol. 83. doi:10.1016/B978-0-12-385510-7.00002-3.

Kumar V. and D. Kumar. 2010. Performance Evaluation of DWT Based Image Steganography. Advance Computing Conference (IACC), 2010 IEEE 2nd International. doi:10.1109/IADCC.2010.5423005.

Li Bin, Junhui He, Jiwu Huang and Yun Qing Shi. 2011. A Survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing. 2: 142-72.

Nunes J. 2003. Image Analysis by Bidimensional Empirical Mode Decomposition. Image and Vision Computing 21(12): 1019-26. doi:10.1016/S0262-8856(03)00094-5.

Rehman N. and D. P. Mandic. 2009. Multivariate Empirical Mode Decomposition. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 466(2117): 1291-1302. doi:10.1098/rspa.2009.0502.

Rekik Siwar, Driss Guerchi, Sid-Ahmed Selouani and Habib Hamam. 2012. Speech Steganography Using Wavelet and Fourier Transforms. EURASIP Journal on Audio, Speech, and Music Processing. doi:10.1186/1687-4722-2012-20.

Thung Kim-Han and Paramesran Raveendran. 2009. A Survey of Image Quality Measures. 2009 International Conference for Technical Postgraduates (TECHPOS), 1–4. doi:10.1109/TECHPOS.2009.5412098.

Wang HuaiQing and ShuoZhong Wang. 2004. Cyber Warfare: Steganography vs. Steganalysis. Communications of the ACM 47(10): 76-82. doi:10.1145/1022594.1022597.

Xia Zhihua, Lincong Yang, Xingming Sun, Wei Liang, Decai Sun and Zhiqiang Ruan. 2011. A Learning-Based Steganalytic Method against LSB Matching Steganography. Radio Engineering. 20: 102-9.

Zhiweil Kang, Liu Jing, He Yigang and Kang Zhiwei. 2007. Steganography Based on Wavelet Transform and Modulus Function. Systems Engineering and Electronics, Journal of 18(3): 628-32. doi:10.1016/S1004-4132(07)60139-X.