International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-10, Jan 2019

Covert Communication Based on Symlet and Daubechies Wavelets

Laxmi Gulappagol, Research Scholar, VTU, Belgaum, Karanataka, India,
laxmigulappagol@gmail.com
K. B. ShivaKumar, Dept. of Telecommunication Engineering, SSIT, Tumkur, Karnataka, India.
kbsssit@gmail.com

Abstract **Rapid technological growth in digital communication is responsible for the development of newer techniques to communicate secret data. Covert communication is the advanced method of concealing the secret data into a cover media. This article presents image steganography in which the secret image is concealed in the cover image by two different techniques: Symlet and Daubechies wavelets. The performance analysis for Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and processing time is evaluated. It is evident from the experimental results that the proposed techniques are suitable for secured communication in which embedded data is out of reach for human visual system**

Keywords — Covert communication, Symlet, Daubechies wavelets, PSNR, Embedding Cost, Distortion function

I. Introduction

Information hiding is a new and multidisciplinary field that encompasses cryptography, coding theory, information theory and theory of human perception. Data hiding using steganography is applicable in various fields which includes business and corporate companies. Covert communication is the process of hiding a data within another data. This data can be a file, message, image or video. Steganography is a combination of the two Greek words steganos and grapheia, where steganos means covered, concealed or protected [1-4]. Image steganography is based on stegno-key, where images are altered in unique ways thus enabling the detection of embedded data using proper steganalysis method. [5, 6, 7]

Another classification for image steganalysis is Specific and Generic. The specific approach depends on the underlying steganographic algorithm used whereas the generic approach does not depend on underlying steganographic algorithm. The high success rate for detecting the presence of the secret message is hidden with the algorithm is possible by specific approach. The accuracy of the prediction heavily depends on the choice of the right features, which should not vary across images of different varieties in generic approach [4,9] The wavelets are classified into Orthogonal and Biorthogonal of which Daubechies, Coiflet and Symlet come under Orthogonal family. The Daubechies wavelets, based on the work of Ingrid. Daubechies are a family of orthogonal wavelets defining a discrete wavelet transform and characterized by a maximal number of vanishing moments for some given support whereas Symlet Wavelet is a family of wavelets. They are a modified version of Daubechies wavelet with increased symmetry [10-13].

II. Literature Survey

Youseef et al., [1] have proposed a steganographic method to embed data in gray scale and RGB images. Wavelet domain communication has been adopted. Mayra Bachrach et al., [2] have adopted a image steganography to embed secret messages in files, texts and images. DCT and DWT have been implemented for experimental analysis. Chang Wang et al., [3] have presented JPEG covert communication based on Discrete Wavelet Transform coefficients and syndrome trellis coding. The flipping and rounding errors have caused block complexity and distortion effects. S. Kumari et al., [4] have experimented the effect of Symlet filter order on denoising of still images. Compression Ratio and Peak signal to noise ratio have been analyzed. Vojtech Holub et al., [5] have proposed a universal wavelet relative distortion to embed secret data in arbitrary domain. Distortion during embedding is calculated to measure the degree of security. Ashwani Kumar Yadav et al., [8] have proposed a Discrete wavelet transform with Symlet wavelet with wiener and median filters to denoise ultra sound image. J K Mandal et al., [12] have proposed a new scheme of hiding information in images using four-point Daubechies wavelet in which horizontal, vertical and diagonal coefficients of the transformed array is used for embedding. DFT and DCT algorithm are adopted. Vijay Kumar Sharma et al., [13] have proposed a method of hiding the secret image Daubechies discrete wavelet transform operation followed by mixing operation further decryption using inverse

DOI : 10.18231/2454-9150.2018.1322

Daubechies discrete wavelet transform.

This article present a new algorithm and its working details is shown in next section. Section IV shows the experimental results and analysis. The paper is summarized in Section V.

III. PROPOSED WORK

This article presents the steganographic strategy based on the frame work of minimizing the distortion. The proposed technique involves the calculation of embedding cost, distortion function using two different types of wavelets: Symlet and Daubechies wavelets. The low pass and high pass decomposition filters are used to form three filter banks LL, LH and HH and the embedding is displayed in the Fig. 1.

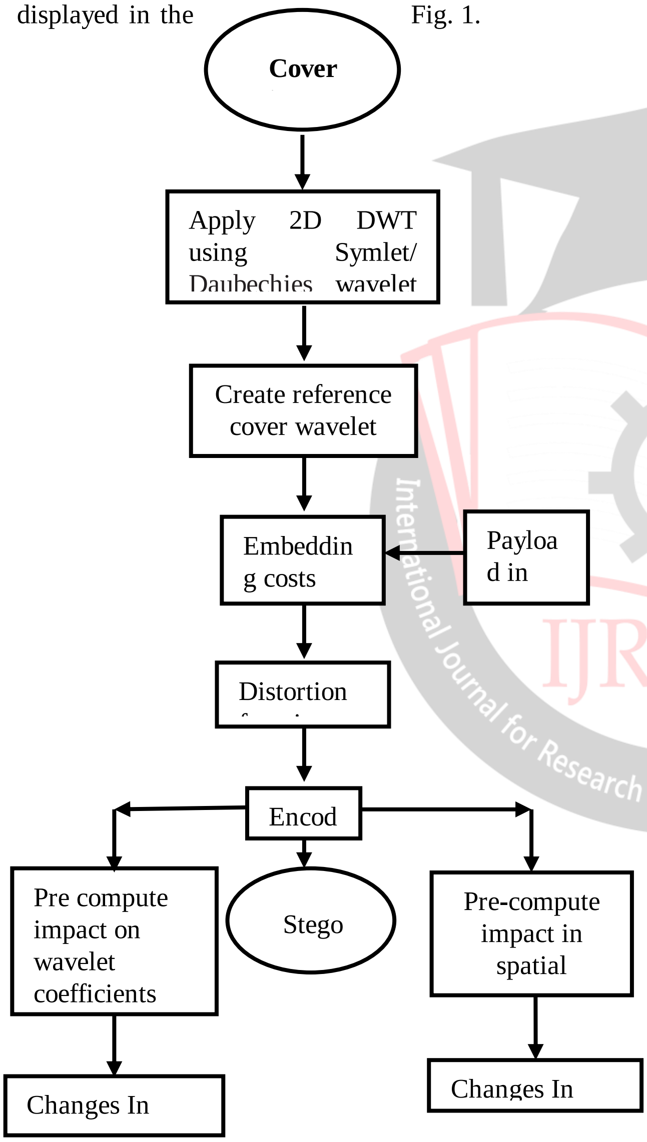

Cover
Apply 2D DWT using Symlet/ Daubechies wavelet
Create reference cover wavelet
Embedding costs
Payload in
Distortion f...
Encod
Stego
Pre compute impact on wavelet coefficients
Pre-compute impact in spatial
Changes In
Changes In

Figure 1. Proposed algorithm of JPEG image steganography

A. Algorithm

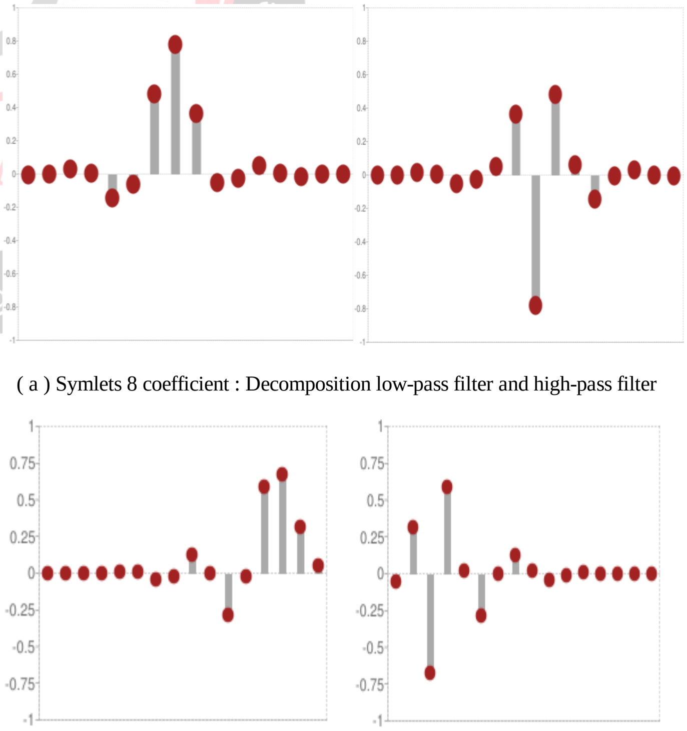
Inputs: Cover Image and secret Image; Output: Stego Image

The algorithm for JPEG image steganography is proposed below:

1. Load the image from the user.
2. Apply 2D DWT using Symlet and Daubechies wavelet over the image, a block of 8×8 DCT coefficients is computed
3. Create reference cover wavelet coefficients (LH, HL, HH) and embedding should minimize their relative change. Computation uses mirror-padding.
4. Computation of costs and residual that is to get differences between cover and Stego image.
5. Pre-compute impact in spatial domain when a jpeg coefficient is changed by 1
6. Pre-compute impact in spatial domain when a jpeg coefficient is changed by 1
7. Change rate is obtained

B. Symlet and Daubechies Wavelet

Symlet Wavelet is a family of wavelets. They are a modified version of Daubechies wavelet with increased symmetry. The properties of the Daubechies and Symlet wavelet families are similar [4, 12]. There are 7 different Symlet functions from sym2 to sym8. In *sym N*, *N* is the order. Symlets are symmetrical wavelets. They are designed so that they have the least asymmetry and maximum number of vanishing moments for a given compact support. The Wavelet Symlets 8 (sym8) and Daubechies 89 (db8) filter coefficient are shown in Fig. 2.



(a) Symlets 8 coefficient : Decomposition low-pass filter and high-pass filter

(b) Daubechies 8 coefficient: : Decomposition low-pass filter and high-pass filter

Fig. 2 Wavelets: (a) Symlets 8 Coefficient [4] and (b) Daubechies 8 Coefficient [12]

DOI : 10.18231/2454-9150.2018.1322

C. Result conceptualization

The embedding changes in the DCT domain by ±1 ,to measure the distortion it is natural to use some measure of the statistical spread, such as the expected value of the square of the residual distortion or its absolute value. The quantized DCT coefficients in the $(a,\ b)^{th}$ block of the cover and stego image by ckl(a,b) and skl(a,b) = ckl(a,b) kl + wkl(a,b) , respectively, where wkl(a,b) are the embedding changes, which are independent realizations of random variables Wkl(a,b) attaining the values in {−1, 0, 1} with probabilities $\{\beta_{kl}^{(a,b)}, 1-2\beta_{kl}^{(a,b)}, \beta_{kl}^{(a,b)}\}$ determined by the steganographic scheme and the payload size. The cover and stego images $x_{ij}^{(a,b)}$ and $y_{ij}^{(a,b)}$ are given equation (1) and equation (2), respectively [1].

$$x_{ij}^{(a,b)} = \Sigma_{k,l=0}^{7} f_{kl}^{(i,j)} q_{kl} c_{kl}^{(a,b)} \qquad (1)$$

$$y_{ij}^{(a,b)} = \Sigma_{k,l=0}^{7} f_{kl}^{(i,j)} q_{kl} s_{kl}^{(a,b)} \qquad (2)$$

The difference between the non-rounded pixel values is given by equation (3)

$$z_{ij}^{(a,b)} = y_{ij}^{(a,b)} - x_{ij}^{(a,b)} = \Sigma_{k,l=0}^{(i,j)} f_{kl}^{(i,j)} q_{kl} w_{kl}^{(a,b)} \qquad (3)$$

The embedding changes are mutually independent, we have

$$E[Z_{ij}^{(a,b)}] = 0 \qquad (4)$$

$$Var[Z_{ij}^{(a,b)}] = 2\Sigma_{k,l=0}^{7} (f_{kl}^{(i,j)})^2 q_{kl}^2 \beta_{kl}^{(a,b)} \qquad (5)$$

IV. SIMULATION RESULT AND ANALYSIS

The algorithm proposed is tested using MATLAB 2014 on different set of images. The results are displayed in Fig. 3 and Fig. 4 by considering P_E as a function of payload and DCT coefficients in both spatial domain and DCT domain.

Two different cover images are considered for experimentation such as Crocodile (Fig. 3. (a)) and Penguin (Fig. 3. (d)) and the respective stego images are shown in Fig. 3. (b) and (e). The resultant difference between cover image and stego image with respect to the colour coefficients is considerable identified in Fig. 3(c) and (f) respectively. The exact position of the changes is spotted by using DCT in frequency domain and also in spatial domain as displayed in Fig. 4. (a) (b) and (c) (d) respectively for both the cover images. These colour differences are considerably minimised using histogram analysis which is shown in Fig. 5. (a) and (b). The change in pixel difference reveals the data hidden in a spatial domain of the image.

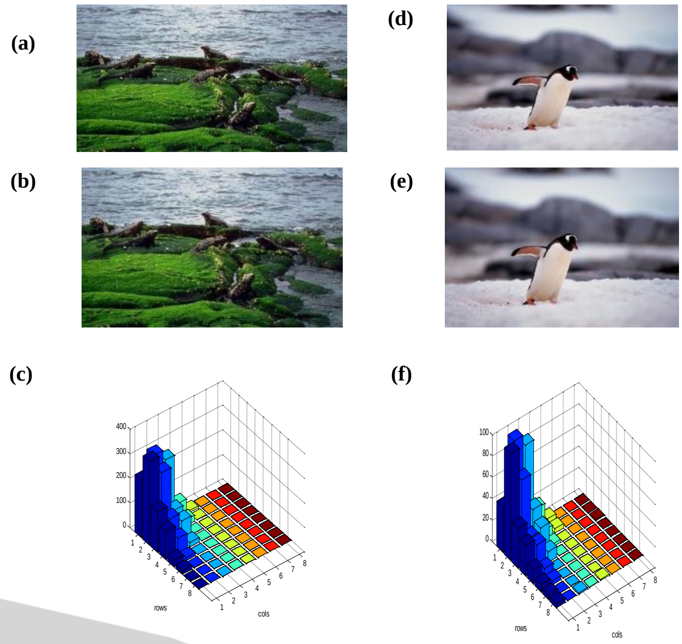


Figure 3. Illustrates the steganography : (a) and (d) Cover Image; (b) and (e) Stego image ; (c) and (f) Difference in coefficient with color map

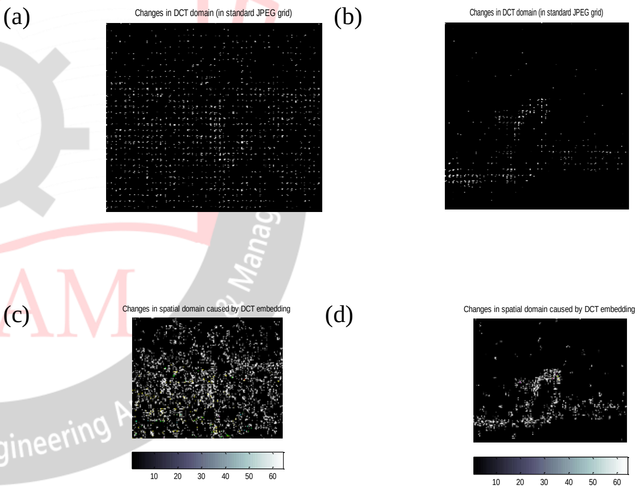


Figure. 4 (a) and (c) Change in DCT (b) and (d) Change in Spatial domain

Embedding cost and distortion function are used to reduce the distortion to gain robustness and security.

For the spatial jitter and the additive noise, the detection errors would increase with increasing the strength of noise, especially when the embedding rate is low, *e.g.*, 0.1 bpp. However, for high embedding rates, such as 0.2 bpp and 0.3 bpp, the increases of detection errors are relatively smaller compared to the corresponding case of 0.1 bpp, as illustrated in Table 1.

DOI : 10.18231/2454-9150.2018.1322

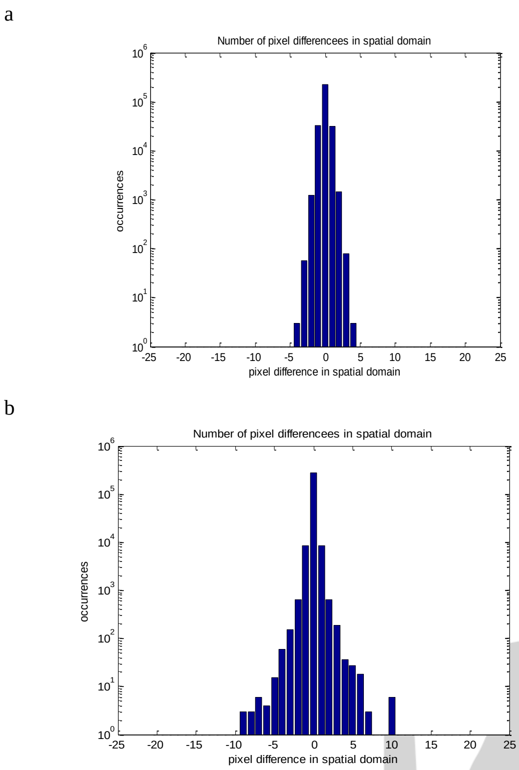


Fig.5 (a) and (b)Histogram of pixel difference in spatial domain for cover image and stego image respectively

TABLE 1. TABULATES THE CHANGE RATE FOR DIFFERENT PAYLOAD IN BPP

Cover Image	Cover Image size	Change rate per nzAC		
		payload=0.1	payload=0.2	payload=0.3
1.jpg	680x512	0.0167	0.0361	0.0555
2.jpg	384x256	0.0200	0.0421	0.0694
3.jpg	256x384	0.0200	0.0442	0.0739

The PSNR, MSE and processing time in seconds is tabulated in Table 2 and Table 3 for Symlet and Daubechies wavelts respectively.

Table 2. Performance analysis for Symlet wavelet

Sl.No	Cover Images	Secret Image	Time To Embedded in Sec	Chang e Rate	PSNR
1	W.Jpg	Lena.jpg	0.11	0.7736	58.27
2	E1.Bmp	7.jpg	1.08	0.5800	59.52
3	M1.Bmp	b.jpg	0.5	0.8128	58.06
4	Grayscal.Bmp	barbara.jpg	3.75	0.5352	59.88
5	Barbara.Tif	Dog.jpg	0.41	0.6272	59.18
6	Dog.Jpg	Lena.jpg	0.77	0.6384	59.10
7	B.Jpg	7.jpg	1.83	0.6152	59.2
8	7.Jpg	b.jpg	1.32	0.6273	58.74
9	Flower.Jpg	barbara.jpg	0.45	0.6112	59.29
10	Goldhill.Tif	Dog.jpg	1.85	0.6944	59.76

Table 3. Performance analysis for Daubechies wavelet

Sl.N o	Cover Images	Secret Image	Time To Embedded in Sec	Chang e Rate	PSNR
1	W.Jpg	Lena.jpg	0.1	0.5634	53.11
2	E1.Bmp	7.jpg	0.09	0.4474	55.12
3	M1.Bmp	b.jpg	0.1	0.5608	53.15
4	Grayscal2.Bmp	barbara.jpg	0.08	0.4539	54.99
5	Barbara.Tif	Dog.jpg	0.1	0.6187	52.30
6	Dog.Jpg	Lena.jpg	1.81	0.4341	55.33
7	B.Jpg	7.jpg	1.12	0.5308	53.63
8	7.Jpg	b.jpg	1.83	0.3011	58.55
9	Flower_Yellow	barbara.jpg	1.14	0.5309	53.63
10	Goldhill.Tif	Dog.jpg	1.84	0.2033	61.97

V. CONCLUSION

Covert Communication based on Symlet and Daubechies Wavelets for image steganography is presented. The differences in the colour coefficients in frequency domain and spatial domain are computed and embedding cost and distortion function are used to reduce the distortion to gain robustness and security. The performance analysis for Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and processing time is evaluated. The average PSNR for Daubechies wavelet is 55 dB and 58 dB for Symlet wavelet. Thus, it is evident from the result that Symlet wavelet is combatively better for image steganography with processing time of less than one second to embed payload.

REFERENCES

[1] Sherin Youssef, Ahmed Ab Elfarag, and Reta Raouf, " A Robust Steganography model using Wavelet-based Block-partition Modification," *International Journal of Computer Science & Information Technology (IJCSIT)*, pp. 15-28, 2011.

[2] Bachrach, Mayra, and Frank Y. Shih, "Image steganography and steganalysis," *Wiley Interdisciplinary Reviews: Computational Statistic* vol. 3, 2011, pp. 251-259, 2011.

[3] Wang, Chang, and Jiangqun Ni. "An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients." *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference*, pp. 1785-1788. IEEE, 2012.

[4] Kumari, Sarita, and R. Vijay, "Effect of symlet filter order on denoising of still images," Advanced Computing: An International Journal (ACIJ), Vol.3, No.1, January 2012.

DOI : 10.18231/2454-9150.2018.1322

[5] Holub, Vojtěch, Jessica Fridrich, and Tomáš Denemark. "Universal distortion function for steganography in an arbitrary domain." EURASIP Journal on Information Security 2014, vol.1, pp. 2-13, 2014.

[6] Nimje, Swati, Amruta Belkhede, G. Chaudari, Akanksha Pawar, and Kunali Kharbikar, "Hiding existence of communication using image steganography," *International Journal of Computer Science and Engineering*, vol. 2, pp. 163-166, 2014.

[7] Sezal Khera and Sheenam Malhotra, "Survey on Medical Image De noising Using various Filters and Wavelet Transform," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, Issue 4, pp. 230-234, April 2014.

[8] Yadav, Ashwani Kumar, R. Roy, Archek Parveen Kumar, Ch Sandesh Kumar, and Shailendra Kr Dhakad, "De-noising of ultrasound image using discrete wavelet transform by symlet wavelet and filters," Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference, IEEE, pp. 1204-12082015.

[9] Panda, Susmita Subhadarshini, and R. Saravanan, "A Secure Approach to Spatial Image Steganography" available Online through Research Article www. ijptonline. Com, *IJPT*, vol. 8, Issue No.2, pp. 13384-13400, June-2016

[10] Denemark, Tomáš Denemark, Mehdi Boroumand, and Jessica Fridrich. "Steganalysis features for content-adaptive JPEG steganography," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1736-1746, 2016.

[11] Tang, Weixuan, Haodong Li, Weiqi Luo, "Adaptive steganalysis based on embedding probabilities of pixels," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 734-745, 2016.

[12] Mandal, J. K., and S. Das. "An Information Hiding Scheme in Wavelet Domain using Chaos Dynamics," Journal of Scientific and Industrial Research, vol. 77, pp. 264-267, May 2018.

[13] Sharma, Vijay Kumar, Pratistha Mathur, and Devesh Kumar Srivastava. "Highly Secure DWT Steganography Scheme for Encrypted Data Hiding," *in Information and Communication Technology for Intelligent Systems*, pp. 665-673. Springer, Singapore, 2019.

DOI : 10.18231/2454-9150.2018.1322