IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 6, Issue 2, Ver. I (Mar. -Apr. 2016), PP 01-06
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Efficient Security for Data Transmission Using CDF-5/3 Lift-DWT and LSB Technique

Mamtha Mohan[1], B.K.Sujatha[2]
[1](ECE, MSRIT/Autonomous,Idia)
[2](TCE, MSRIT/Autonomous,India)

Abstract : *Stegnography hides the message information inside a specific digital media. In this paper we propose image steganography using CDF-5/3 lift-DWT and Least Significant Bit (LSB) technique. First CDF-5/3 lift-DWT is applied to cover image to generate LL, LH, HL and HH sub-bands. The message information is converted into corresponding ASCII code simultaneously. This code is embedded onto the LL band co-efficients of cover image whose positions are derived from shared key and perform inverse DWT to get stegano image which increase the security of message without degrading the quality of cover image.*

Keywords: *Discrete Wavelet Transform, Image Hiding, LSB Technique and Stegnography.*

I. Introduction

The popularity of internet and digital media are increasing rapidly day by day. Similarly the amount of data transmitted and received through internet increases proportionally. This increase the risk of the transmitted information can be viewed or modified by un-authorized persons. To make the transmission secure many techniques are invented. Most commonly used methods are various cryptographic methods [1]. In this method the information in terms of text is changed to cipher-text by using some algorithms and pre-shares key. But the text can be viewed by un-authorized persons and can be decrypted. To overcome this problem image stenography came into picture. Here the secret data or image is hidden into another image (cover image) in such way that only cover image is visible to the viewer. But with the proper pre-shared key it is possible to decrypt the hidden data or image from cover image. The fast developments in resource sharing through network essentially require security. Secured communication is possible by using different techniques such as watermarking, cryptography, steganography etc. Digital watermark is a perceptually transparent system which is inserted in digital data using an embedding algorithm and key. Digital watermarking is mainly used in copy right protection. Cryptography is the class of information security and associated with scrambling text into cipher text. Steganography is a technique of hiding confidential information in the cover media. In image steganography the cover media used is an image and confidential information may be an image, text audio and video. Image is preferred compare to other media because it has more redundant information. The important aspects of steganography are security, capacity and imperceptibility. The common image steganography techniques are (i) Least Significant Bit (LSB) insertion: The LSB of the cover image are replaced with the confidential information. (ii) Masking and filtering method: The specific masking algorithms or a mathematical formula is used to select specific pixels to embed the secret information. The secret information looks as an integral part of the cover image after embedding. (iii) Transform techniques: The cover image is converted into transform domain by applying transformation such as Discrete Cosine Transform (DCT) [2], Discrete Wavelet Transform (DWT) [3], Integer Wavelet Transform (IWT) [4], Discrete Fourier Transform (DFT) [5], Fast Fourier Transform (FFT), Dual Tree Complex Wavelet Transform (DTCWT) [6, 7] etc., and confidential information is embedded into the transformed coefficients of the cover image.

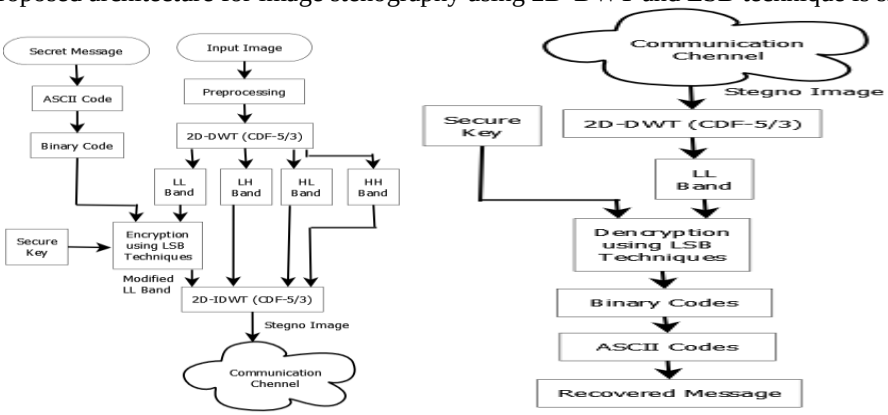
Related Works

Rigdas and ThemrichonTuithung [8] proposed a Huffman encoding based steganography. The secret image is encoded using Huffman encoding which is embedded into the cover image. The embedding is done by altering the LSB of each cover image pixel. Ran-zanwang and Yeh-shun chen [9] presented a steganography technique based on two way block matching procedure. The block matching procedure generates a series of blocks and searches the highest similar blocks from cover image. The secret information is embedded into imperceptible areas of the cover image by using hop embedding schemes which gives high quality of stegno image and extracted image. This method exhibits high payload embedding. Vojtechholub and Jessica Fridrich [10] developed an adaptive stenographic distortion function a bank of directional high pass filters which is ued to obtain the directional residuals. The embedding is done on smooth areas along edges and noisy areas. The directional residual is measured of embedded image. RongJian Chen et al., [11] presented a multi bit and multi-image steganography system using adaptive embedding algorithms with minimum error. The algorithm

evaluates the most similar value to replace the original value. The adaptive method is divided into three steps as i) embed logo data into cover data ii) adaptively adjust LSB's of the cover data. iii) Adaptively adjust the MSB of the cover data. Ajitdanti and Manjula [12] proposed an image steganography using DWT and hybrid wavelet transform. The cover and secret images are normalized and then the wavelet coefficients are obtained by applying DWT onto the image. The wavelet coefficients of both the cover and secret images are fused into single image to get stegno image. Manojkumar et al., [13] proposed image steganography based on the Data Encryption Standard (DES) which uses the S box mapping and secret key. The secret image is preprocessed by embedding function and the stego image is formed by replacing the embedding function values into the cover image. Prabhakaran and Bhavani [14] developed a modified digital image steganography technique using DWT. The secret image is scrambled using a class of cropping transformation called Arnold transformation with key then, DWT is applied to both cover image and payload followed by alpha bending operation. This alpha bending matrix is obtained by addition of wavelet coefficient of respective sub bands of cover image and scrambled secret image. Payload is hidden in the DWT coefficient of cover image. Premkumar and Narayanan [15] have proposed a new scheme for secure banking application based on visual cryptography. The work integrates both steganography and cryptography. The scheme considers maximum number of surrounding pixels to achieve capacity of every target pixel. Rong –Jian Chen and shi-Jinn Horng [16] proposed an anti-forensic steganography system using multi bit adaptive embedding algorithm with flexible bit location to overcome the problem of forensics and to achieve high performance including both large embedding capacity and high image quality. Chao wang et al.,[17] proposed a method of fast matrix embedding by matrix extending to reduce the computational complexity of random linear code based matrix embedding. The fast algorithm is developed by appending some referential columns to the parity check matrix. The parameters considered for improvement are computational complexity and embedding efficiency which is more suitable for real time stenographic systems. VladimarBanoci et al., [18] proposed a secure steganography system in JPEG file based on modulus function which is secure against histogram attacks. The modulo histogram fitting with dead zone method embeds the secret data in JPEG file format. JPEG image is used as cover image and embedding is performed in DCT domain in JPEG file, the data hiding is done by changing the selected quantized DCT transform coefficients according to modulus function. Before embedding, the secret message is encrypted by AES-128 bit cipher to increase security level of steganography system. H S Manjunatha Reddy and K B Raja [19] developed wavelet based secure steganography with scrambled payload which is a hybrid domain technique. Daubechies Lifting Wavelet Transform (LWT) is applied on the cover image to produce sub-band co-efficients. For payload embedding the LL band co-efficients are decomposed into upper and lower bands. The payload is segmented into four blocks and Haar LWT is applied on alternate blocks of payload to generate F1 and F2 wavelet transform bands. The remaining blocks of payload are retained in spatial domain say S1 and S2. Then, bit reversal is applied on each coefficient of payload blocks to scramble payload and cube root is applied on these scrambled values to scale down the number of coefficient bits. The payload is embedded into XD band of cover image to obtain stego image.

Proposed Method

The proposed architecture for image stenography using 2D-DWT and LSB technique is shown in Fig.1.



Pre-Processing

In this section different sizes of images are converted into uniform size (256x256). To reduce the design complexity colour image is converted into gray image is converted into gray image. Also Gaussian filter is used in this section to remove noises present in input images. The Gaussian mask filter of 3x3 is derived from equation (1) to obtain mask [20] given in equation (1).

$$Mask\ Matrix = \frac{1}{16}\begin{bmatrix}1 & 2 & 1\\ 2 & 4 & 2\\ 1 & 2 & 1\end{bmatrix} \quad (1)$$

Discrete Wavelet Transform

The Cohen, Daubechies and Feauveau (CDF-5/3) [21] wavelet is used to generate LL, LH, HL and HH sub-band co-efficients. The basic equations for CDF-5/3 Lifting-Schemes are given in equation (2) and (3).

$$y_{2i+1} = -0.5(x_{2i} + x_{2+2i}) + x_{2i+1} \quad (2)$$

$$y_{2i} = 0.25(y_{2i+1} + y_{2i+3}) + x_{2i} \quad (3)$$

Where x is the input signal value and y is the output transformed signal values. The odd output samples are calculated from even input and even outputs are calculated from updated odd output samples along with even input samples.

In lifting scheme, the decomposition is done via three lifting steps [22] in the forward transform

i. Splitting: where the input samples are divided into even and odd samples.
ii. Prediction: where the odd samples are multiplied by the time domain equivalent of odd samples and are added to the even samples.
iii. Update: where updated even samples are multiplied by the time domain equivalent of even samples and are added to the odd samples.

The basic block diagram of forward lifting scheme is shown in Fig.2

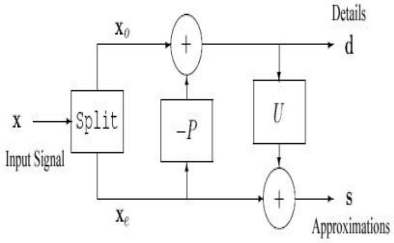


Fig.2: Basic forward 1D-DWT lifting scheme

Similarly block diagram of forward and inverse 2D-DWT lifting scheme is shown in Fig. 3

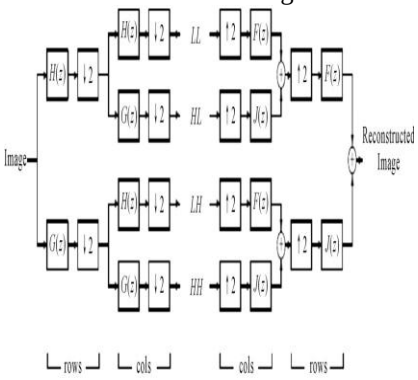


Fig. 3: Forward and Inverse 2D-DWT

The wavelet decomposition and reconstruction of Lena image is shown in Fig.4.

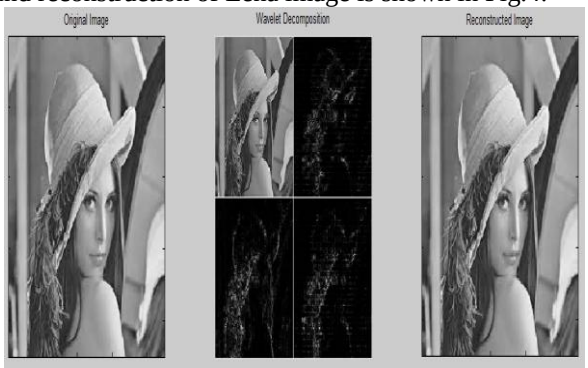


Fig. 4: Forward and Inverse 2D-DWT

LSB Substitution

In this method, the data to be hidden is inserted into the least significant bits [23] of the pixel information. Increase or decrease of value by changing the least significant bit doesn't change the appearance of the image, such that the resulted stegno-image looks exactly same as the cover image.
The algorithm for embedding process is given below:

Embedding Algorithm

On the sender side, the pixel positions for embedding the information are calculated using secure key. Then the bit stream generated from the message is replaced using LSB technique. The embedding algorithm is given below
Input: cover image, key, secret message
Procedure:
Step1: Convert the secret message into bit stream (Length L)
Step2: Generate L number of ASCII number using seed key
Step3: Calculate the non-collide L pixel positions in the cover image
Step4: while complete bit stream not embedded
{ Replace LSB of pixel denoted by ith pixel position, with secret bit
Insert pixel into cover image
}
End
Output: Watermarked-image

Extracting Algorithm

On the receiver side, first of all the pixel positions are calculated in the same way with the use of the secure key. Then secret bit-stream is formed by the LSBs of these pixels. The Extraction algorithm is as below:
Input: stegano-image, key
Procedure:
Step1: Convert the secret message into bit stream (Length L)
Step2: Generate L number of ASCII number using seed key
Step3: Calculate the non-collide L pixel positions in the cover image
Step4: for i=1 to L
{ Get LSB of pixel denoted by ith pixel position
Append this LSB into secret bit stream
}
Step5: Convert secret bit stream into secret message
End
Output: secret message

Simulation Results And Performance Analysis

In this section the proposed design is simulated using MATLAB R2012a (7.14.0.739) version.

Performance Parameters

In this section, the performance parameters are evaluated using PSNR values between original image and stegno image by using the formula [24] as

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad (4)$$

Where, MSE = $\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[P_I(i,j) - P_O(i,j)]^2$
PI(i,j) is input image pixel values.
PO(i,j) is stegno image pixel values.
MN is the image dimensions (256x256).

Image Output

The original and stegno image is shown in Fig.5.

Fig. 5: Original and Stegno Image

Performance Analysis

To analyse the performance of proposed architecture we take different test images and encrypt same information into the image and check PSNR values using equation (4). Those values are tabulated into Table 1.

TABLE I: PSNR Values for different input images

Image	PSNR(dB)
Lena	96.2956
Mandrill	86.7532
Boy	96.2956
Bridge	96.2956
Building	82.3162
Girlface	90.2750

Performance Comparisons With Existing Techniques

Table 2 shows the comparison of PSNR of proposed technique and the existing techniques. The PSNR varies between 35.79 and 96.29 based on cover images. The proposed technique is compared with existing techniques presented by HodaMotamedi and AyyoobJafari [25], TasnuvaMahajabinet. al., [26] and AshishSoniet. al.,[27]. It is observed that the PSNR values values are higher in the case of proposed algorithm compare to existing algorithms for the following reasons since, the PSNR values do not vary significantly though the capacity is varied, because of the high frequency sub bands which have negligible randomness

TABLE II: Comparison of PSNR values of Proposed Method with the Existing Methods.

Authors	Techniques	Cover Image	PSNR (dB)
HodaMotamedi and AyyoobJafari [24]	Wavelet transform and image denoising techniques.	Barbara	39.65
		Boat	36.34
TasnuvaMahajabin et. al.,[25]	Pixel value differencing and LSB substitution Method	Mandrill	32.67
AshishSoni et.al.,[26]	Discrete Fractional fourier Transform.	Rice	32.46
Proposed Method	CDF-5/3 and LSB	Barbara	68.05
		Boat	80.49
		Mandrill	86.75
		Rice	76.79

II. Conclusion

In this work, an algorithm for embedding LL sub band coefficients of secret information into LSB coefficients of cover image using CDF 5/3 transformation method based on Lifting scheme is proposed. The new coefficient replacement technique improves the security, PSNR and hiding capacity. The transformation in the proposed technique shows better results compared to the existing techniques. In future, the proposed technique is used in spatial domain.

References

[1] Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill, 2007.
[2] AnirbanGoswami, Dipankar Pal and NabinGhoshal, "Authentication Technique for Gray Images using DCT," Third International Conference on Emerging Applications of Information Technology, pp. 421 - 424, 2012.
[3] T Narasimmalou and Allen Joseph R, "Optimized Discrete Wavelet Transform based Steganography," IEEE International Conference on Advanced Communication Control and Computing Technologies, pp. 88 – 91, 2012.
[4] NedaRaftari and Amir MasoudEftekhariMoghadam, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm," Sixth Asia Modeling Symposium, pp. 87 – 92, 2012.
[5] SudhirKeshari and ShriGopalModani, "Weighted Fractional Fourier Transform based Image Steganography," International Conference on Recent Trends in Information Systems pp. 214 – 217, 2011.
[6] G Prabhakaran, R Bharani and K Kanimozhi, "Dual Transform based Steganography using Wavelet Families and Statistical Methods," International Conference on Pattern Recognition, Informatics and Medical Engineering, pp. 287 – 293, 2013.
[7] Ivan.W.Selesnick, Richard.G. Baraniuk and Nick G. Kingsbury, "The Dual-Tree Complex Wavelet Transform," Signal Processing Magazine IEEE, Vol. 22, issue 6, pp. 123-151, 2005,

[8] Rig Das and ThemirchonTuithung, "A Novel Steganography Method for Image Processing Based on Huffman Encoding," Third National Conference on Emerging Trends and Applications in Computer Science, pp. 14-18, March 2012.
[9] Ran-Zan Wang and Yeh-Shun Chen, "High-payload Image Steganography using Two-way block matching," IEEE Signal Processing Letters, Vol. 13, Issue 3, pp. 161 – 164, 2006.
[10] VojtechHolub and Jessica Fridrich, "Designing Steganographic Distortion using Directional filters," IEEE International Workshop on Information Forensics and Security, pp. 234 – 239, 2012.
[11] Rong-Jian Chen, Jui-Lin Lai and Shi-Jinn Horng, "Novel Multi-bit and Multi-image Steganography Using Adaptive Embedding Algorithms with Minimum Error," Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 221 – 228, 2011.
[12] AjitDanti and G R Manjula, "Secured Data Hiding of Invariant Sized Secrete Image based on Discrete and Hybrid Wavelet transform," IEEE International Conference on Computational Intelligence & Computing Research, pp. 1 – 6, 2012.
[13] Manoj Kumar Ramaiya, Naveen Hemrajani and Anil Kishore Saxena, "Security Improvisation in Image Steganography using DES," Third International Advance Computing Conference, pp. 1094 – 1099. 2013.
[14] Prabakaran G and Bhavani R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform," International Conference on Computing Electronics and Electrical Technologies, pp .1096 - 1100, 2012.
[15] S Prem Kumar and A E Narayanan, "New Visual Steganography Scheme for Secure Banking Application," IEEE International Conference on Computing Electronics and Electrical Technologies, pp.1013-1016, 2012.
[16] Rong - Jian Chen and Shi-Jinn Horng, "Multi-Bit Adaptive Embedding Algorithm for Anti Forensic Steganography," IEEE International Symposium on Biometrics and Security Technologies, pp.82-89, 2012.
[17] Chao Wang, Welming Zhang, Jiufen Liu and Nenghai Yu, "Fast Matrix Embedding By Matrix Extending," IEEE Transactions on Information Forensics and Security, Vol 7, No 1, pp.346-350, February 2012 .
[18] Vladimir Banoci, Gabriel Bugar, DusanLevicky and ZitaKlenovicova, "Histogram Secure Steganography System in JPEG File Based on Modulus Function," Twenty Second International conference Radioelectronika, pp. 1 – 4, 2012.
[19] H S Manjunatha Reddy and K B Raja, "Wavelet Based Secure Steganography with Scrambled Payload," International Journal of Innovative Technology and Exploring Engineering, vol. 1, issue 2, pp.121 - 129, July 2012.
[20] R. A. Haddad and A. N. Akansu, "A Class of Fast Gaussian Binomial Filters for Speech and Image Processing", IEEE Transactions on Acoustics, Speech and Signal Processing, Vol. 39, pp. 723-727,1991.
[21] AmitPande and Joseph Zambreno, "Design and Analysis of Efficient Reconfigurable Wavelet Filters", IEEE International Conference on Electro/Information Technology, pp. 327-333, May 2008, America.
[22] Geert Uytterhoeven, Dirk Roose and AdhemarBultheel, "Integer Wavelet Transforms using the Lifting Scheme", Proceedings of the CSCC, World Scientific Journal, Vol.2, pp. 6251-6253, 1999.
[23] Neil F. Johnson and SushilJajodia, "Steganalysis of Image Created Using Current Steganography Software", Workshop of Information Hiding Proceedings, Portland Oregon, USA,15-17 April,1998. Lecture Notes in Computer Science, Vol.1525, Springer-Verlag (1998).
[24] [Online]https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.
[25] HodaMotamedi and AyyoobJafari, "A New Image Steganography based on Denoising Methods in Wavelet Domain," Ninth International Conference on Information Security and Cryptology, pp. 18 – 25, 2012.
[26] TasnuvaMahjabin, Syed MonowarHossain, and Md. SharifulHaque, "A Block Based Data Hiding Method in Images using Pixel Value Differencing and LSB Substitution Method," Fifteenth International Conference on Computers and Information Technology, pp. 168 – 172. 2012.
[27] AshishSoni, Jitendrajain and RakeshRoshan, "Image Steganography using Discrete Fractional Fourier Transform," International Conference on Intelligent Systems and Signal Processing, pp. 97 – 100. 2013.