ISSN 2320-9984

Volume 2 Issue 2 | June 2014

ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Twice Steganography Method Along with DWT for Highly Secure Data Transmission

Jyoti Viswakarma
M. Tech. Scholar,
Shri Ram Institute of Technology
Jabalpur, (M.P) [India]

Prof. Ravi Mohan
Head of the Department
Department of Electronics & Communication Engg,
Shri Ram Institute of Technology,
Jabalpur, (M.P.) [INDIA]
Email: ravimohan7677@yahoo.co.in

Abstract— *Proposed paper is a unique DWT based method for steganography. The Covering image is divided into four sub bands using transform technique DWT. Two different privet images set fixed in the HL and HH sub-bands respectively. When inserted privet images are spread within each band and use a semi random succession and only one Session key. Privet images are retrieved using the session key along with size of the images. In this approach the stego image produce is of acceptable level with good imperceptibility and less distortion as compared to other cover image with different methods and enhance the overall security.*

Keywords:—*Discrete Wave Transform, Discrete Cosine Transform, steganography, cryptography.*

1. INTRODUCTION

Steganography [1,2,3] is the method of hiding any privet message in an ordinary message and retrieve it at its destination. Anyone other viewing the message cannot know that it contains encrypted (privet) data. The particular word originate from the Greek word "*steganos*" and "*graphei*" meaning "covered" &"writing". LSB [4] insertion is a not tough and very common method to placing information in an image binary domain. The drawback of this method is quite common and small image manipulation. Stego-images can be simply interpreted by histogram analysis. In frequency domain information can be design secure by using Discrete Cosine Transformation method [5,8]. Main problem with this method is blocking artefact. In the DCT it made chunks of pixels into 8x8 blocks and then after transforming the pixels into total 64 DCT coefficient each. A small modification of a any DCT co-efficient will affect complete 64 image pixels in that particular block. One new method of Steganography is Discrete Wavelet Transformation approach [6,7]. In this technique the distortion & imperceptibility of the Stego image is up to the mark and it is reliable in many attacks.

2. DISCRETE WAVELET TRANSFORMATION

The wavelet transform is a multi-resolution decomposition method in form of spreading an image into some set of wavelet function. Discrete Wavelet Transformation has excellent space frequency resolution properly. Using DWT in 2D images likes applying a 2D filter image processing in every dimension, the input image can be divided into 4 non-overlapped multiple resolution sub-bands by 2D filters, namely LL1, HL1, LH1 and HH1.

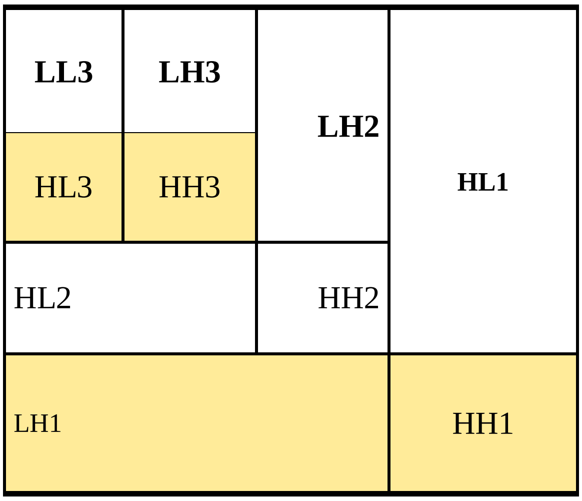

Figure1: Three phase decomposition using DWT.

The sub-band LL1 can be processed further to find the next scale of wavelet coefficients; it keeps does that till final scale N is reached. At that total have 3N+1 sub-band containing multi-resolution sub-bands (LLN), (LHX), (HLX) and (HHX) here X ranges from 1 to N. normally lots of the energy gets stored in these sub-bands. The Forward type Discrete Wavelet Transform is very good to find the areas in the covering image that where can be privet image hidden successfully because of its efficient space & frequency resolution properties. With only, this property let the masking affect of the human visual system, as that if a DWT co-efficient is changes, it changes only the region respective of that coefficient. The hiding privet image in the less frequency sub-bands like in LLX it can cause degrade the image in more amount, as normally lots of the energy is consumed by these sub-bands. Hiding in the lower frequency bands, but, could increase robustness somewhat. On the other hand, the textures and edges of the image and human eye generally not sensitive to small changes in the higher frequencies sub-bands e.g. HHX. So it allows the stego image to be hide without being observation by the human eye. Same compromise used by lots of DWT based algorithms, to have required performance of robustness & imperceptibility both one should hide the privet image in somewhere middle of frequency sub-bands LHX or HHX.

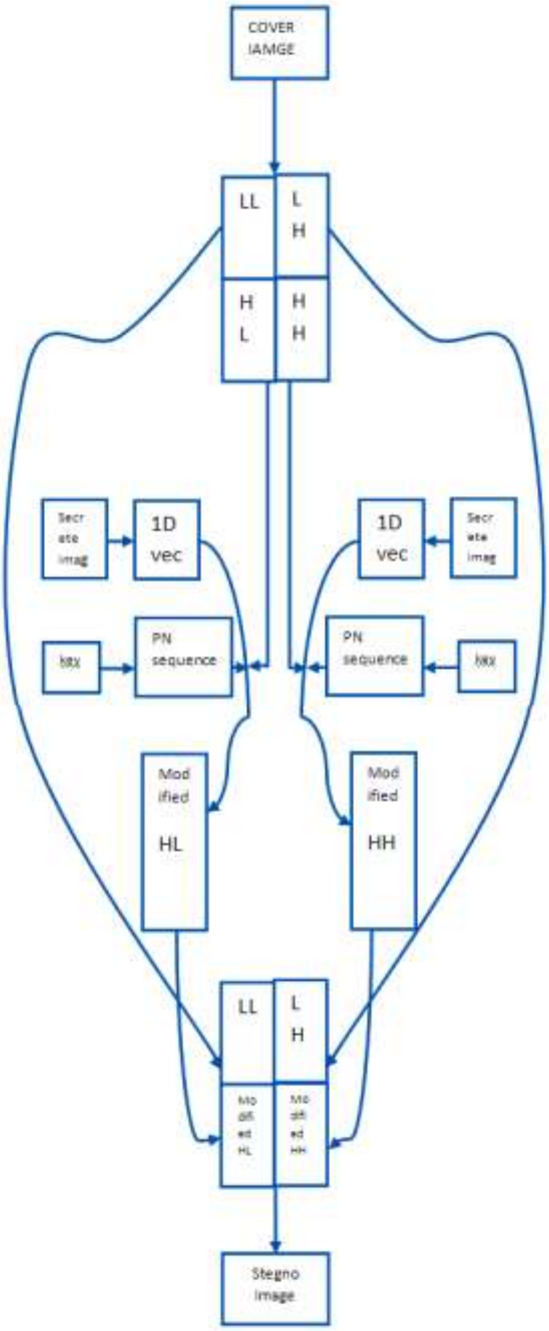

Figure 2: Image Hiding Process Privet Image Extraction

3. PROPOSED ALGORITHM

Privet Image Hiding:

1. First Cover image decomposed by DWT into four sub-bands (LL, HL, LH and HH).
2. Second Two isolated privet images taken & then converted into two isolated 1D Vectors.
3. Third Two pseudo random 2D patterns are designed by the based key.

4. Fourth Each HL and HH bands of the covering image modified individually as the content of the respective privet 1D image vector.
5. Finally four sub bands along with two modified sub bands are mixed and develop the stego image using IDWT.

Recovering of the privet Image:

1. Session key and Sizes of the privet images are sent to the intended receiver via a privet communication channel.
2. Privet images can recovered from the stego image using Correlation function and knowing the size of the privet image.
3. Extracted Privet Images are filtered to remove the unwanted signal.

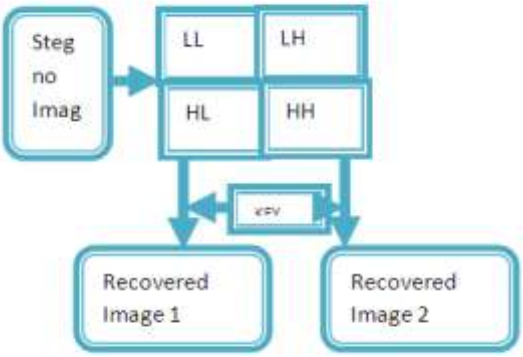

Figure 3: Image Extraction Process

4. RESULTS

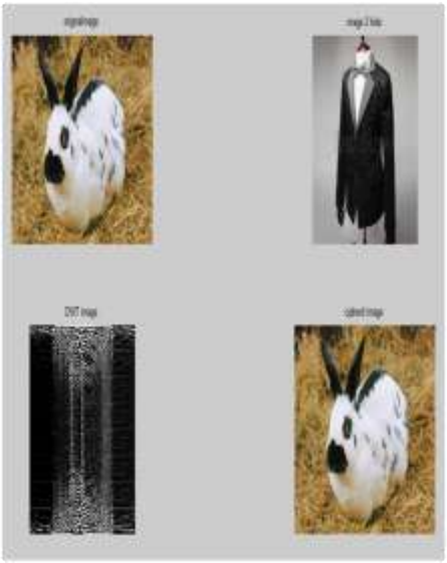

Figure 4: Results generated on MATLAB as Observed after developing stegno Image

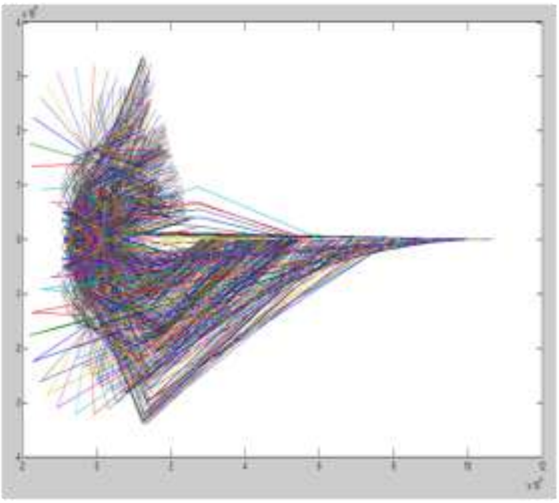

Figure 5 The DWT of The cover Image

Figure 4 and 5 shown above are the results observed for the proposed approach and it can be easily observed that the stegno image the rabbit (i.e cipher image) is as same as the original image and though it has complete data image (i.e. the image of a suit), their image is the DWT of object image (data image) and as per proposed approach that DWT is been hidden into the cover image.

Table 1: the Analysed Results of the Proposed work

Results Observed			
Data Image size	**Cover image size**	**MSE**	**SNR**
8kb	200 kb	0.089	85.2
14kb	200 kb	0.098	84.8
22 kb	200 kb	0.102	83.1
25kb	200 kb	0.154	82.9
8kb	500 kb	0.036	98.2
14kb	500 kb	0.051	97.3
22 kb	500 kb	0.067	96.9
25kb	500 kb	0.088	96.1

Table 1 shows the Mean square error observed for the different size of Data and cover image and it also shows the Signal to Noise ratio (SNR) for different scenario, it can be easilt seen that observed results that

Maximum SNR is 98.2 which is quite good but it gets reduces when size if covering image increases after deeply analysing the results it can be said that results are as was expected and it is very clearly hiding the data image into the covering–stegno-image.

5. CONCLUSION

Steganography is an approach to hide the data (image in our case) efficiently into any covering object (image in our case) and it should do that any intruder cannot interpret it by any means, as from the proposed method that is been achieved and one can say that our generated stegno image cannot be interpreted easily by any intruder, also the total SNR observed for any scenario where the data image and cover image has ration of 1:8 or less is more than 82.9, and it is a good results for that ration better than previous work on the area.

REFERENCES:

[1] Sandra Bazebo Matondo, Guoyuan Qi, Two-Level Image Encryption Algorithm Based on Qi Hyper-Chaos, 2012 Fifth International Workshop on Chaos-fractals Theories and Applications, 978-0-7695-4835-7/12 $26.00 © 2012 IEEE, DOI 10.1109/ IWCFTA.2012.47

[2] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum, International Journal of Modern Engineering Research (IJMER), Vol.1, Issue1, pp-157-161 ISSN: 2249-6645

[3] Belmeguenaï Aïssa, Derouiche Nadir, Redjimi Mohamed, Image Encryption Using Stream Cipher Algorithm with Nonlinear Filtering Function, 978-1-61284-383-4/11/$26.00 ©2011 IEEE

[4] S. Sasidharan and R. Jithin, "selective encryption using DCT stream cypher " International Journal of Computer Science and Information Security, 2010.

[5] H. Jiang and C. Fu, "An image encryption scheme based on Lorenz chaos system," Natural computation, ICNC’08, vol. 4, pp. 600-604, 2008.

[6] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 3998-4006, 2010.

[7] G. Qi, M. A. van Wyk, B. J. van Wyk, and G. Chen, "A new hyperchaotic system and its circuit implementation," Chaos, Solitons & Fractals, vol. 40, pp. 2544-2549, 2009.

[8] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos -based cryptosystems," International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, vol. 16, p. 2129, 2006.