Twice Steganography method along with DWT for highly secure data transmission

Shanu Suryawanshi[1], Prof Mukesh Tiwari[2]

[1]Mtech student, LNCT Jabalpur,
Shanus1c@rediffmail.com

[2]Asst. Professor, LNCT Jabalpur ,
Mukesh_tiwari836@yahoo.co.in

Abstract *: There is much possible type of stenographic methods already been developed. Steganography is getting more popular then cryptography because of its advantages over cryptography. But the techniques that are been developed in the area are based of complex and pattern based data hinging in pixels of images, later on key based approaches are also been developed, later on many combination (two different approaches cryptography and steganography working together) based method been developed. the proposed work is new theory for steganography that is analytical cum pattern based Image steganography the proposed method is been developed for achieving very high SNR and low MSE even if the size of original is less, actually the only problem with steganography is that it requires lots of data (a full image) for transmitting few original data, so proposed work aims to reduce the size of image while maintaining the size of original data same.*

Keywords : Peak Signal to Noise Ratio (PSNR) Discrete Wave Transform, Mean Square Error (MSE), Discrete Cosine Transform, cryptography, steganography**.**

1. Introduction

The way of protecting information by *encrypting* it into an unpredictable format, called cipher text. Only one who possesses a *key* can *decrypt* the message into original text. Encrypted messages can seldom be broken by *code-breakers*, but modern cryptography methods are virtually unbreakable. The Internet and different forms of data communication become more important, electronic security is becoming important. Cryptography is also used to protect e-mail and messages, mostly credit card information, and industry data. Many famous cryptography systems used on the Internet Cryptography methods can be classified as symmetric-key systems which use a single key in which both the sender and recipient have, and key known as public-key systems which use two isolated keys, one public key known to all and one private key that only the recipient have to extract the messages.

The science of hiding data by embedding messages inside other, harmless messages. Steganography works by changing bits of useless data in regular computer files say graphics, text, sound or HTML with bits of invisible information. This hidden data can be plain text, image or even cipher text. Steganography few times is used when encryption is not allowed. Or commonly, steganography is work as supplement for encryption. An encrypted file can still hide data using steganography; hence if the encrypted file gets deciphered, the hidden data is not seen.

A discrete wavelet transform (DWT) is any transform in which the wavelets are discretely sampled. As compare to other wavelet transforms, a main advantage in it that it captures both location information (location in time) and frequency.

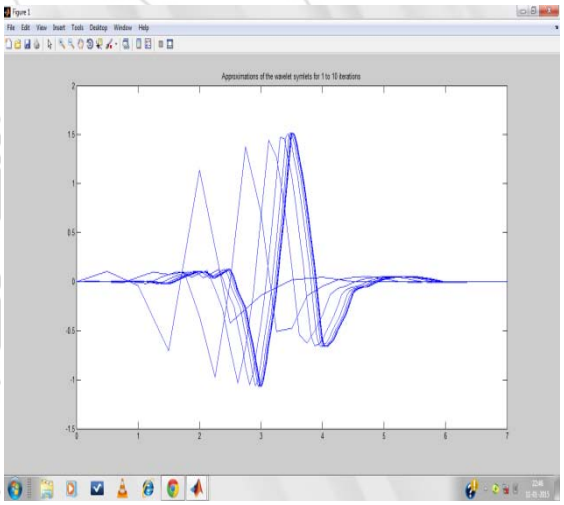

Figure 1: Symlet's of order1 to 10

It is observed that discrete wavelet transform (it is discrete in scale and shifted, and also continuous in time) is successfully used as analog filter bank in biomedical or other signal processing for design of less-power pacemakers and also in ultra-wideband wireless communications.

2. Literature Survey

Sandra Bazebo Matondo1 and Guoyuan Qi2 presents 'Two-Level Image Encryption Algorithm Based on Qi, Hyper-Chaos', Their work introduces a two-level encryption algorithm which was based on the high level of randomness of the Qi hyper-chaos and its sensitivity to its initial condition, Their analysis show that the Qi hyper-chaos has bigger key space and faster encryption speed because of its

faster pseudo random sequence generation rate as compared with existing chaotic systems[1].

Tanmay Bhattacharya , Nilanjan Dey and S. R. Bhadra Chaudhuri presents 'A Novel Session Based Dual Steganography Technique Using DWT and Spread Spectrum' In their proposed method second image is embedded inside the HL sub band of cover image. So there was a small visual change in between cover image and their stegno image. But because of strong security aspects that small amount of imperceptibility was acceptable. Their approach can be applied for color image and also for audio Steganography because DWT is applicable for any digital signal[2].

Belmeguenaï Aïssa, Derouiche Nadir, and Redjimi Mohamed presents 'Image Encryption Using Stream Cipher Algorithm with Nonlinear Filtering Function', In their Work, a new algorithm based encryption scheme for image data was introduced, their simulations were carried out with different images. Their visual test indicates that their encrypted image was very different and has no visual information which can be deduced about the original image for all images. In addition, their method was very simple to implement, the encryption and decryption of an image. Their proposed algorithm can to resists the additive noises [3].

3. Methodology

Figure 1 shown next shows the proposed method. At first step the image is been taken through MATLAB and then in the MATLAB environment it gets converted into pixels form (integer numbers) for the data hiding as it is an analytical approach we required to convert it into frequency cum time domain which is possible with Wavelet transform only there are many transform techniques are available so it was our decision to made that up to what we required time or frequency resolution if we choose 'db1' then very good frequency resolution and if we choose 'db10' then time resolution gets better so we have chosen 'db5' wavelet which give adequate time and frequency resolution. After transform comes to new method to find out the area where one can hide pixels in image and it affects the original image negligibly for that we have chosen correlation of pair of three continuous pixels to search the required area where one hide the data.

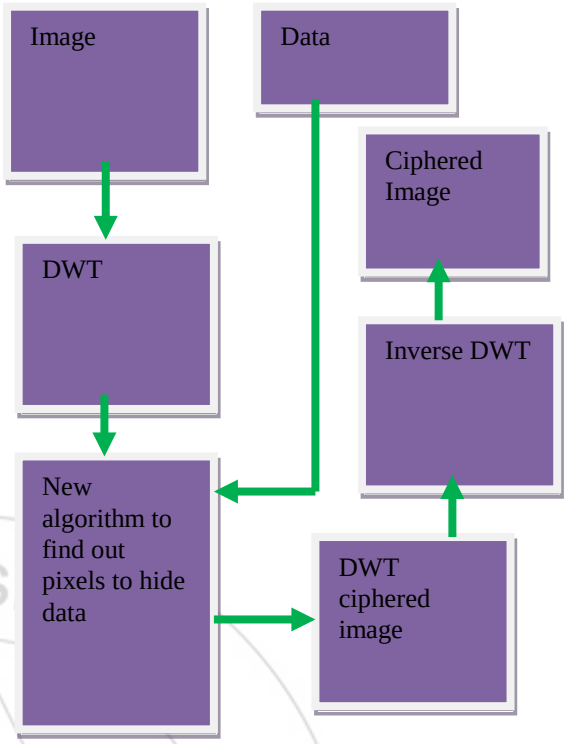

Figure 2: The proposed data hiding method

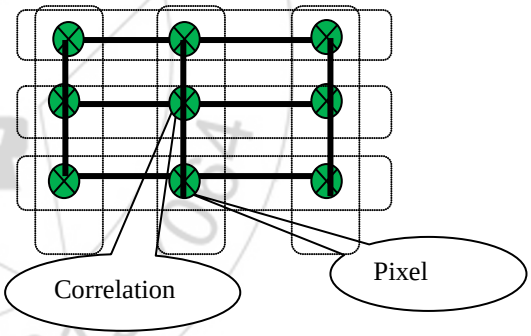

Figure 2: The correlation approach

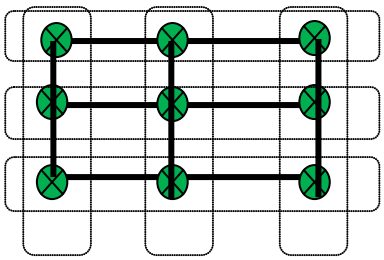

Table 1: Observed Results

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

After finding out the appropriate area in the image the data can be hide as LSB replacement and then inverse DWT taken to have pixels back after having pixels the ciphered image been constructed.

Figure 3 shows the decryption process for as can be observed it exact reverse order than the encryption process and our aim is to extract data not construct the original image so we did the process to have original data only.

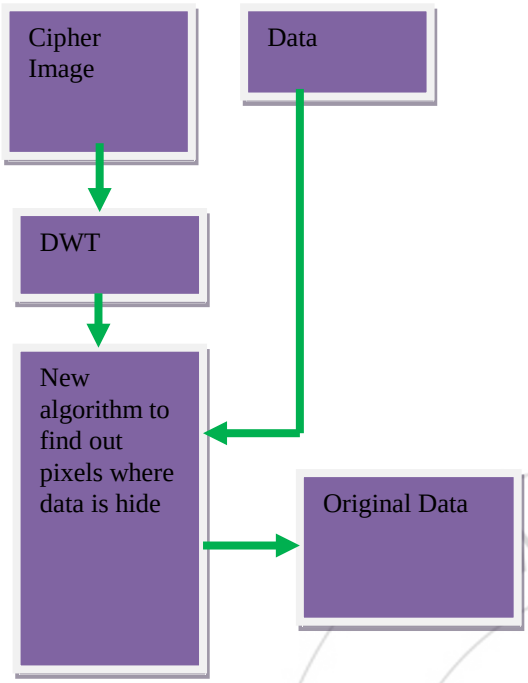

Figure 3: The decryption method

4. Results

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 easily 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

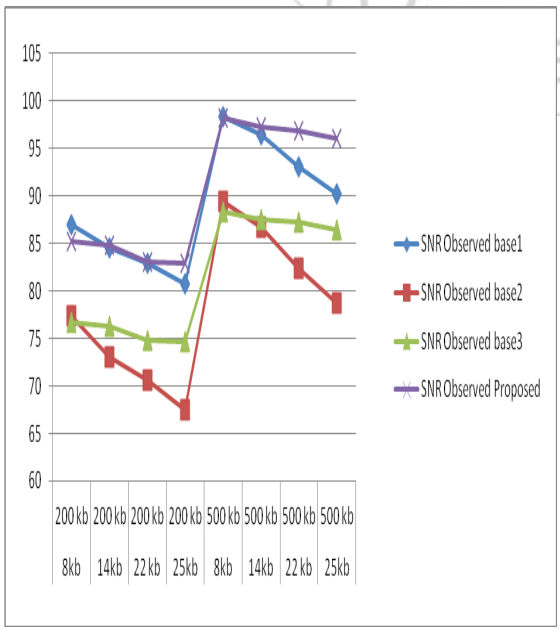

Figure 4: SNR generated on MATLAB as Observed after developing stegno Image

Table 2: Comparative Results

	Correlation	SNR
Proposed	**0.9887**	**90.5**
Paper by Sandra Bazebo Matondo in IEEE 2012	**0.9830**	
Tanmay Bhattacharya, IJMER in 2013	**0.9381 and 0.8870**	**27.3850**
Derouiche Nadir in IEEE 2012	**0.975**	

Table 2 shown above are the results observed for the proposed approach and it can be easily observed that the correlation factor between the original and cipher image is been best observed in proposed design also the value of SNR is very impressive in proposed work and better than other works.

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 easily 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.

3. 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 hyper-chaotic system and its circuit implementation," Chaos, Solutions & Fractals, vol. 40, pp. 2544-2549, 2009.

[8] G. Alvarez, 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.

Author Profile

Shanu Suryawanshi[1]received the B.E.degree in Electronics and communication from RGPV Bhopal in 2013 and Pursuning Mtech in Digital Electronics from RGPV Bhopal from 2013 to 2015.Her area of interest is Stenography using Discrete wavelet transform.