Steganography Methods with unique DWT and SVD for Secure Communication

1Shanu Suryawanshi, 2Prof Mukesh Tiwari

1M. tech. student, LNCT, Jabalpur
2Asst Prof., LNCT, Jabalpur

Abstract: **As known there are many possible type for stenographic methods already been developed. Steganography is getting much popular then cryptography due to its advantages over cryptography. however techniques that are been developed in area are based for complex & pattern based data hinging in pixels for images, later on key based approaches are also been developed, later on many combination (two various approaches cryptography & steganography working together) based procedure been developed. proposed work is new theory for steganography that is analytical cum pattern based Image steganography proposed procedure is been developed for achieving very high SNR & low MSE even if size for original is less, actually only problem with steganography is that it nessesory many for data (a full image) for transmitting few original data, so proposed work aims to increase size of data while maintaining size for image same. In proposed approach stego image produce is for acceptable level with good PSNR & less BER as compared to other cover image with various methods & enhance overall security.**

Keywords: **Peak Signal to Noise Ratio (PSNR), Discrete Wavelet Transform (DWT),Discrete Cosine Transform (DCT) MSE: Mean Square Error, Bit Error Rate (BER), Discrete Fourier Transform (DFT)**

I-INTRODUCTION

The science for hiding data by embedding messages inside other, harmless messages. Steganography works by changing bits for useless data in regular computer files say graphics, text, sound or HTML with bits for invisible information [3]. This hidden data may 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 may still hide data using steganography; hence if encrypted file gets deciphered, hidden data is not seen.

Steganography relies on hiding covert message in unsuspected multimedia data & is generally used in secret communication between acknowledged parties. Steganography is a procedure for encryption that hides data among bits for a cover file, such as a graphic or an audio file. Technique replaces unused or insignificant bits with secret data. Steganography is not as robust to attacks since embedded data is vulnerable to destruction[5].
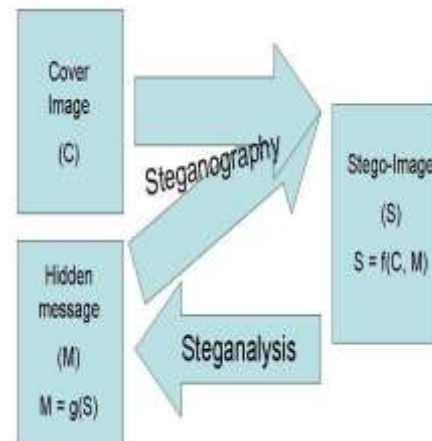

Figure 1: Data hiding scenario

DWT: A discrete wavelet transform is a transform in which wavelets are discretely sampled. As compare to other wavelet transforms, a main advantage in it that it captures both location information (location in time) & frequency[7].

Till now, information hiding methods have much less attention from researchers & also from industrialist as compare with cryptography. however it has been a fast growth for interest in steganography for two main causes:

1.-The broadcasting & publishing industries are interested in methods for hiding encrypted massages marks & also serial numbers in audio recordings, digital films, books & various multimedia products[6].

2.-Along with various governments to stop availability for resources that they use for Encryption, It inspired people to study methods which may be use for private messages to embed in seemingly unobjectionable cover messages[6].

As stenography is depends upon data cover a cover may be any image, audio or video however it is been seen that generally size for cover is very large as compare to actual data which means if we want to secure data transfer using steganography we will need to transmit much much data as compare to actual data it is a big drawback with all available steganography methods. Peoples tries many things like changing approach for data hiding in cover image or hiding data first then compress stenograph cover or compress data then stenograph it into cover many tried multilevel steganography & combination & achieved good level for data hiding however still size for cover is around 70 to 200 times for size for actual data.

Figure 2: LSB substitution procedure for various substitution positions

In essence, image steganography is about exploiting limited powers for human visual system. Inside reason, any plain text, cipher-text, other images, or anything that may be embedded in a bit stream may be hidden in an image. Common methods followed for hiding data in images are 'Least Significant Bit (LSB) Insertion' technique shown in figure 2 in which LSB for pixel values are replaced with data to be encoded in binary form

Drawbacks in substitution method
1.-Extremely liable to attacks like Image Manipulation techniques where pixels will be scanned for a possible relation which will be used to trace out actual characters.
2.-Only 24 bit messages are suitable & 8 bit images are to be used at great risk.
3.-Extreme Care needs to be taken in selection for cover image, so that changes to data will not be visible in stego-image.
4.-Commonly known images, such as famous paintings must be avoided.

II-LITERATURE WORK
After going through & deep study total 12 research papers, few articles, books & Google on internet it is been observed that available work in related work is itself is good enough however as nothing may be best so there are still possibilities for improvement in various parameters in steganography.

Krishna Rao et al.	Block Based Robust Blind Image Watermarking Using Discrete Wavelet Transform, Proposed a blind image watermarking technique which embeds watermark into image in frequency domain using discrete wavelet transform, singular value decomposition & torus automorphism techniques. This technique extracts watermark without cover image & also proved that this procedure is robust against various signal & non signal processing attacks. They hide watermark in Image with BER for 0.29 in JPG images.
Tanmay Bhattacharya et al	A Novel Session Based Dual Steganographic Technique Using DWT & Spread Spectrum, Their approach may be applied for colour image & also for audio Steganography because DWT is applicable for any digital signal, they observed PSNR for 27.3850
Mr. Sandra Bazebo et al	Qi, Two-Level Image Encryption Algorithm Based on Qi Hyper-Chaos, Their observed result was they took an image size for 512x512 & encrypt it to test their algorithm. Using their selective encryption, only 4096 DC coefficients gets encrypted to change values for total 262144 pixels, correlation found in cipher is images is 0.9830
Belmegu enaï Aïssa et al	Image Encryption Using Stream Cipher Algorithm with Nonlinear Filtering Function, Their procedure was very easy to implement, encryption & decryption for an image. Their proposed algorithm may to resists additive noises, correlation found in cipher is images is 0.0975

Table 2.1 various literature base work

Image hiding method by **Krishna Rao et al.***:*
1. First Cover image decomposed by DWT into four sub-bands (LL, HL, LH & HH).
2. Second take SVD of LL part of original Image
3. Third take data image and convert it into binary.
4. Fourth modify S part as per the data image modification process is as per equation below:-
$S(2,2) = S(2,2) = \alpha1 * S(3,3) + \alpha2\ wmbit.$
5. Finally perform ISVD and Then IDWT and develop a Stegno Image.
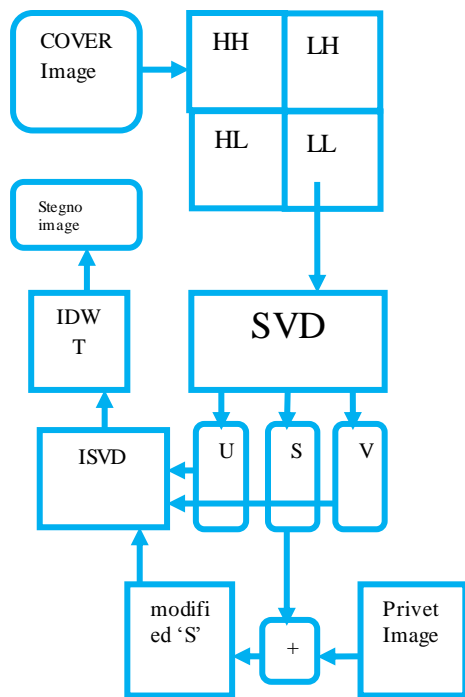
Figure 3: Flow of work by Krishna Rao et al.

III-PROBLEM STATEMENT

[1] Has used frequency domain information may be design secure by using Discrete Cosine Transformation method. Main problem with this procedure is blocking artefact. In DCT it made chunks for pixels into 8x8 blocks & then after transforming pixels into total 64 DCT coefficient each. A small modification for a any DCT co-efficient will affect complete 64 image pixels in that particular block. One new procedure for Steganography is Discrete Wavelet Transformation approach. In this technique distortion & imperceptibility for Stego image is up to mark & it is reliable in many attacks. BER they observed is 0.29 for Image for lady. [2] Work is extremely liable to attacks like Image Manipulation techniques where pixels will be scanned for a possible relation which will be used to trace out actual characters. In [3] Only 24 bit messages are suitable & 8 bit images are to be used at great risk.[4] Extreme Care needs to be taken in selection for cover image, so that changes to data will not be visible in stego-image. Not good with commonly known images, such as famous paintings.

IV-PROPOSED WORK

Because for drawbacks in currently followed techniques, proposed work is a new technique for hiding data in images using DWT and SVD. Here, we replace only in that area where it affect very less changes in original picture. that area where can be detected with help for DWT

Proposed work aims to increase size of data while maintaining same size of image. Proposed work will reduce MSE, BER & increase SNR and Correlation factor.

Proposed DWT will by symlet-6 type for image analysis and finding out higher frequencies. SVD isolate Eigen values and as known Eigen values does not change during data communication hence we hide our data after taking SVD hence our hidden data along with image does not change during communication.

V-RESULTS

Result will be measure on behalf of results parameters MSE, BER, PSNR and Correlation Coefficient

Mean Squared Error (MSE) Definition: mean squared error MSE for an estimator is one from many types to quantify & difference between values used by an estimator & actual values for quantity being estimated. MSE measures averages for squares for errors. MSE should be less in order to better performance. let X is transmitted signal & Y is Received N is length for signal, MSE: Mean Square Error , SNR: Signal to Noise ratio

$$MSE = \frac{(X-Y)^2}{N}$$

Signal-to-noise ratio (SNR) Definition: SNR is a measurement that compares level for a required signal to level for background noise. It is defined as ratio for actual signal power to noise power, often expressed in decibels. SR should be high in order to better performance for design system

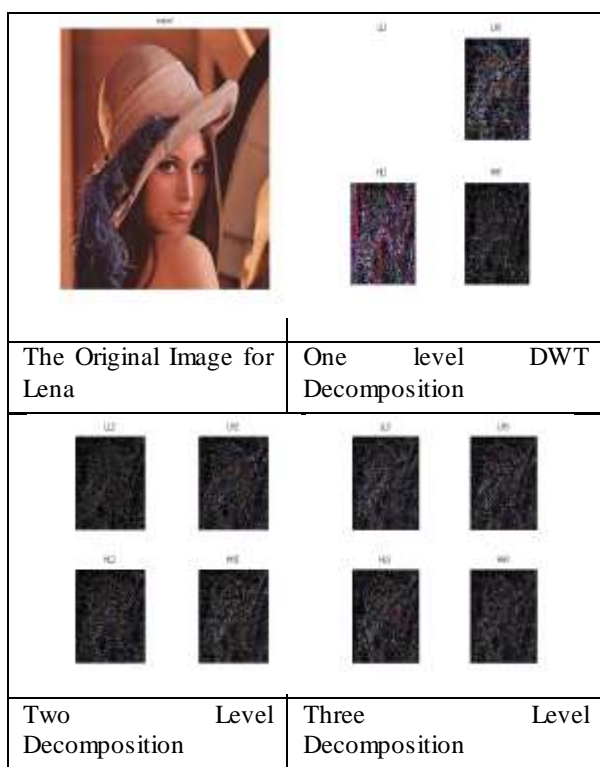$$SNR = 10log_{10}\frac{256^2}{MSE}$$

Correlation: Similarity in received signal bits as compare to input signal. Let discrete samples for transmitted signal is X with & discrete samples for received signal is Y with size for *len* than

$$Corr = \frac{X * Y}{len}$$

BER: Bit error rate is shows number of bit change. let 'X' is the original image and 'Y' is the Cipher image and 'r' is number of roe and 'c' is number of column then

$$BER = \frac{X \; xor \; Y}{r * c * 8}$$

Simulation Results: proposed technique for data inside image hiding is processed with MATLAB standard Image of 'Lena'

The Original Image for Lena	One level DWT Decomposition
Two Level Decomposition	Three Level Decomposition

Figure 4: Analyzed Results for proposed work

Figure 4 above shows the original Image of lena and its decomposition after applying DWT on it.

V-CONCLUSION

Many research papers are been studied and compared. The original objective for paper work was to develop an optimised technique for hiding data inside cover image also to reduce amount for data on channel while stenograph data transmission. Steganography is that it necessary many for data means image for sending few small amount for data, so our work will be a good solution for this problem.

REFERENCES

[1] Krishna Rao Kakkirala & Srinivasa Rao Chalamala, Block Based Robust Blind Image Watermarking Using Discrete Wavelet Transform, TCS Innovation Labs,TATA Consultancy Services, HiTec City, Madhapur, Hyderabad, India, 2014 IEEE 10th International Colloquium on Signal Processing & its Applications (CSPA2014), 7 - 9 Mac. 2014, Kuala Lumpur, Malaysia

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

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

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

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

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

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

[9] Iwata, M., Miyake, K., & Shiozaki, A. 2004. *"Digital Steganography Utilizing Features for JPEG Images",* IEICE Transfusion Fundamentals, E87-A, 4:929-936.

[10] Po-Yueh Chen & Hung-Ju Lin, *"A DWT Based Approach for Image Steganography",* International Journal for Applied Science & Engineering 2006. 4, 3: 275-290