# Secret Key Steganography technique based on three-layered DWT and SVD algorithm

Priyanka Chouksey[1], Dr. Prabhat Patel[2]

[1]Research Scholar , Department of Electronics & Telecommunication, JEC Jabalpur, India
[2]Associate Professor , Department of Electronics & Telecommunication, JEC Jabalpur, India

***Abstract*—** *Steganography is a technique of hiding secret messages in another data (which can be a video, an audio, an image or a text) to protect unauthorized access. Regardless of years of research in the area of data hiding, it is still a very challenging task. A combination of DWT decomposition and singular value decomposition (SVD) is proposed to achieve effective hiding of secret information into an image. The proposed technique finds out the pixels to hide secret data (Text) by performing two approaches successively. The first approach (DWT) decomposes the cover image iteratively to find the high frequency components of it, since human eyes are less sensitive to high frequency. The second approach (SVD) again decomposes the high frequency components of cover image to find singular value matrix where secret data can be hide securely. The BER has been used as a comparison parameter for proposed work and previous work. In addition to this, noise is also added before transmitting the data hided image called 'Stego' image. The BER between retrieve data and original data is simulated.*

**Keywords**--*Steganography, DWT, Singular Value Decomposition, BER and SNR, Stego image.*

## I. INTRODUCTION

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security of information does not matter. This has led to a heightened awareness of the need to protect the data transmitted. Thus the field of cryptography has got more attention nowadays. More and more complex techniques for encrypting the information are proposed every now and then. Some advanced encryption algorithms like RSA, DES, AES etc. which are extremely hard to crack have been developed. But, as usual, when a small step is made to improve the security, more work is done in the opposite direction by the hackers to break it. Thus they are able to attack most of these algorithms and that too, successfully. Even complex algorithms like RSA are no exception to this.

So, to deceive the hackers, people have started to follow a technique called 'Steganography'. It is not an entirely new technique and has been in the practice from ancient times. In this method, the data is hidden behind unsuspecting objects like images, audio, video etc. so that people cannot even recognize that there is a second message behind the primary object. Images are commonly used in this technique.

### *A. Types of Steganography*

The steganography can be classified according to its importance and goals [1].Steganography Techniques are broadly classified into two categories; spatial domain techniques and transform domain techniques. Spatial domain methods, which are more popular, take the advantage of human visual system and directly embed data by manipulating the pixel intensities. In transform domain procedures, the image is first transformed into frequency domain and then the message is embedded. Depending upon the embedding and extraction procedures used, Steganographic systems can again be classified into the following three different categories [2]:

***1) Pure Steganography (No Key Steganography - NKS):*** This is the simplest and weakest form of Steganography in which the secret message is directly embedded into the cover image without any encryption. The success of this hidden communication depends upon the assumption that parties other than the intended receivers (attackers) are not aware of the existence of the secret message within.

***2) Secret Key Steganography (SKS):*** In this form of Steganography, both the receiver and transmitter have commonly agreed upon secret keys. The secret message is embedded into and extracted out of the stego image using these keys. The keys can be separately shared between both parties using some confidential channel prior to the actual transmission starts. The robustness of this system, of course, lies with the secrecy of the keys and the difficult part in this method is how to share the keys between the transmitting and receiving parties maintaining their secrecies.

***3) Public Key Steganography (PKS):*** This method uses a pair of public and private keys to hide the secret information. The key benefits of this system are its robustness as well as easy key management. The method is robust because the parties other than the intended receivers need to know both the private and public keys used for embedding and the

encryption algorithms used, in order to be able to extract the hidden information.

The transform domain enables operation on the frequency content of the image, and therefore high frequency content such as edges and other subtle information can easily be enhanced. The principle behind the frequency domain methods of image enhancement consists of computing a 2-D discrete unitary transform of the image, for instance the 2-D DFT, manipulating the transform coefficients by an operator M, and then performing the inverse transform. The orthogonal transform of the image has two components magnitude and phase. The magnitude consists of the frequency content of the image. The phase is used to restore the image back to the spatial domain [3].

## II. LITERATURE REVIEW AND PROBLEM IDENTIFICATION

Belmeguenai Aissa [4] introduced a technique which is based on stream cipher with nonlinear filtering function. The Boolean function used in this algorithm is resilient function, satisfying all the cryptographic criteria, carrying out the best possible compromises. The visual test indicates that the encrypted image was very different and no visual information can be deduced about the original image for all images. In addition, this method is very simple to implement the encryption and decryption of an image. This algorithm can be used to resists the additive noises.

Sandra Bazebo Matondo [5] proposed a new image encryption algorithm based on Qi hyper-chaotic system. Pseudo random sequences generated from Qi hyper-chaotic system have used to hide the image visual information and to change the image characteristics in the frequency and spatial domains. In this method, a two-level encryption is employed. The first level consists of a selective encryption of Discrete Cosine Transform coefficients at the frequency domain using exclusive-or operation. In the second level, the pseudo random sequences' sorting is used to shuffle the image pixels in the spatial domain. The experimental results and analysis of the algorithm suggest that this scheme provides not only effective encryption but also a large key space and a resistance to different types of attacks.

Tanmay Bhattacharya [6] discussed that the Forward type Discrete Wavelet Transform is very good to find the areas in the covering image where private data can be hide successfully because of its efficient space & frequency resolution properties. The paper proposed a DWT based Steganographic technique. In this technique the cover image is decomposed into four sub bands using DWT. Two secret images are embedded within the HL and HH sub bands respectively. During embedding, secret images are dispersed within each band using a pseudo random sequence and a Session key. Secret images are extracted using the session key and the size of the images. In this approach the stego image generated is of acceptable level of imperceptibility and distortion compared to the cover image and the overall security is high.

Krishna Rao Kakkirala [7] proposed a block based blind image watermarking using DWT, SVD and Torus automorphism. The technique extracts watermark without cover image. They also proved that this method is robust against different kinds of geometric and signal processing attacks. We can still further make this method more robust against different filtering attacks by applying same embedding method to other sub bands of the host image in DWT domain.

The proposed algorithm makes steganography more robust as follows: The algorithms involved in this literature although provide a better security of private message as compare to the old steganography techniques, but all of it works on low frequency components of cover image. Since human eyes are very sensitive to low frequency components, a small distortion in the cover image due to private data can be easily predicated. The proposed algorithm uses high frequency components for data hiding as our eyes are less sensitive to it. Also, Singular Value Decomposition allow us to distribute every bit of private message over a block of 8×8 i.e. 64 pixels so that in case of any loss during transmission, private data or message can be recovered. In addition to above, the algorithm works with a confidential key (known to sender and intended receiver only) which prevent an unauthorized extraction of private message.

## III. STEGANOGRAPHY USING THREE LAYERED DWT & SVD

In this section, the three layered DWT and SVD based steganography algorithm is introduced with the explanation how effectively it facilitates the process of data hiding in an image. The basis of the proposed method, DWT is introduced below.

### *A. Discrete Wavelet Transform*

The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. For 1-D DWT the input data is passed through a set of low pass and high pass filters. The output of high pass and low pass filters are down sampled by 2. The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient. Human eyes are less sensitive to the high frequency signals. Our eyes will average fine details within the small area and record only the overall intensity of that area.

Since images are two dimensional data, so to transform images, either two dimensional wavelets can be used or one dimensional transform can be applied to the rows and columns of the image successively. For the latter case, the input data (image) is passed through a set of both low pass and high pass filter in two directions, rows and columns of that image. The outputs are then down sampled by 2 in each direction as in case of 1- D DWT [8]. As shown in Figure: 1, output is obtained in set of four coefficients LL, HL, LH and HH. The first alphabet represents the transform in row whereas the second alphabet represents transform in column.

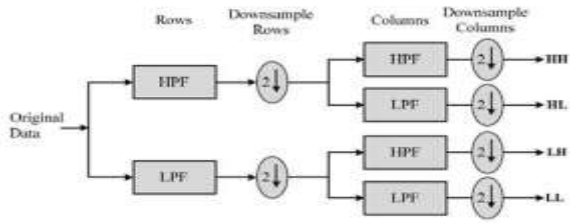


Fig 1: Block Diagram of 2-D DWT [9]

The alphabet L and H specifies low pass signal and high pass signal respectively. LH signal is a low pass signal in row and a high pass in column. Hence, LH signal contain horizontal elements. Similarly, HL and HH contains vertical and diagonal elements, respectively. Figure: 2 represent the decomposition of an image after three iterations of DWT.

<table>
<tr><td rowspan="2">LL1</td><td colspan="3">LH1</td></tr>
<tr><td>LL2</td><td colspan="2">LH2</td></tr>
<tr><td rowspan="2">HL1</td><td rowspan="2">HL2</td><td>LL3</td><td>LH3</td></tr>
<tr><td>HL3</td><td>HH3</td></tr>
</table>

Fig 2: Three level DWT decomposition of an image

### *B. Singular Value Decomposition*

SVD is a matrix factorization technique commonly used for producing low-rank approximations. Given an m × n matrix A with rank r, the singular value decomposition SVD(A), is given by [10]

$$SVD(A) = U \times S \times V \quad (1)$$

where U,S and V are of dimensions m × m, m × n, and n × n respectively. U and V are two orthogonal matrices called the left and the right singular vectors, respectively and S is a diagonal matrix, called the singular matrix.

Matrix S has only r nonzero entries, which makes the effective dimensions of these three matrices m × r, r × r and r × n respectively. The diagonal entries ($s_1, s_2 \ldots, s_r$) of S have the property that $s_i > 0$ and $s_1 \geq s_2 \geq \ldots \geq s_r$. The first r columns of U and V represent the orthogonal eigenvectors associated with the r nonzero Eigen values of $AA^T$ and $A^TA$ respectively. In other words, the r columns of U corresponding to the nonzero singular values span the column space, and the r columns of V span the row space of the matrix A. SVD has an important property that makes it particularly interesting for our application. SVD provides the best low-rank linear approximation of the original matrix A. It is possible to retain only k << r singular values by discarding other entries. We term this reduced matrix $S_k$. Since the entries in S are sorted i.e. $s_1 \geq s_2 \geq \ldots \geq s_r$, the reduction process is performed by retaining the first k singular values. The matrices U and V are also reduced to produce matrices $U_k$ and $V_k$ respectively. The matrix $U_k$ is produced by removing $(r - k)$ columns from the matrix U and matrix $V_k$ is produced by removing $(r - k)$ rows from the matrix V. When we multiply these three reduced matrices, we obtain a matrix $A_k$. The reconstructed matrix (Inverse SVD)

$$A_k = U_k \times S_k \times V^T \quad (2)$$

$A_k$ is a rank-k matrix that is the closest approximation to the original matrix A. It has been pointed out[11][12] that the low-rank approximation of the original space is better than the original space itself due to the filtering out of the small singular values that introduce "noise" in the customer-product relationship.

### *C. Proposed Algorithm*

Figure 3(a) and 3(b) shows the flowchart of the proposed algorithm. It starts with decomposition of cover image into its frequency components. For this we transform the cover image into frequency domain with the help of 2-dimensional Discrete Wavelet Transform. Following are the steps of our algorithm at transmitter and receiver side respectively.

Secret data hiding at transmitter:

1. Cover image is decomposed into blocks of 8×8 pixels. Each block is then transformed in four sub bands (LL1, LH1, HL1 and HH1) using 2-D DWT. The HH1 component is again decomposed into four sub bands (LL2, LH2, HL2 and HH2). Likewise HH3 is obtained with HH2.
2. The secret message is converted into 1-D binary bit string.
3. A confidential key provided by user is also converted into binary string.
4. Every 8×8 block of HH3 is decomposed by SVD.
5. Every binary bit of Secret message is distributed over one block each by modifying all the singular values of that block.
6. After inverse SVD, four sub bands including modified sub band HH3 are combined iteratively to generate the modified image using IDWT.
7. Secret key is hided in modified image to get 'Stego Image'.

Secret message Extraction at receiver:
1. Confidential key is sent to the intended receiver via a secret communication channel.
2. The received stego image is decomposed into blocks of 8×8 pixels.
3. The key known to recipient is XORed with the hided key to check the authorization of recipient.
4. After successful match of key, three iterations of DWT are performed to obtain HH3.
5. SVD is performed on HH3 to get the singular value coefficients.
6. Binary bits of secret message are extracted from singular value coefficients of every block.
7. Extracted binary bits are finally converted into characters.

Mean Square Error (MSE) - The mean square error is defined as the square of the difference between the pixel values of the original image and the stego image and then dividing it by size of the image. The mathematical formula for computing Mean square error between x and y images of sizes $M \times N$ is given below

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} [x(m,n) - y(m,n)]^2 \quad (3)$$

Peak Signal to Noise Ratio (PSNR) - The Peak Signal to Noise Ratio (PSNR) measures the estimates of the quality of stego image compared with an original image and is a very commonly used metric way to measure image reliability or conformity. The mathematical formula to calculate the PSNR value is as follows:

$$PSNR = 20 log_{10} [\frac{MAXPIX}{MSE}] \quad (4)$$

where MAXPIX is the maximum pixel value and MSE is the Mean Square Error.

Bit Error Rate (BER) – In telecommunication transmission, the bit error rate (BER) is the percentage of bits that have errors relative to the total number of bits received in a transmission, usually expressed as ten to a negative power.

$$BER = \frac{\text{number of bits recieved in error}}{\text{Total number of bits transmitted}} \quad (5)$$

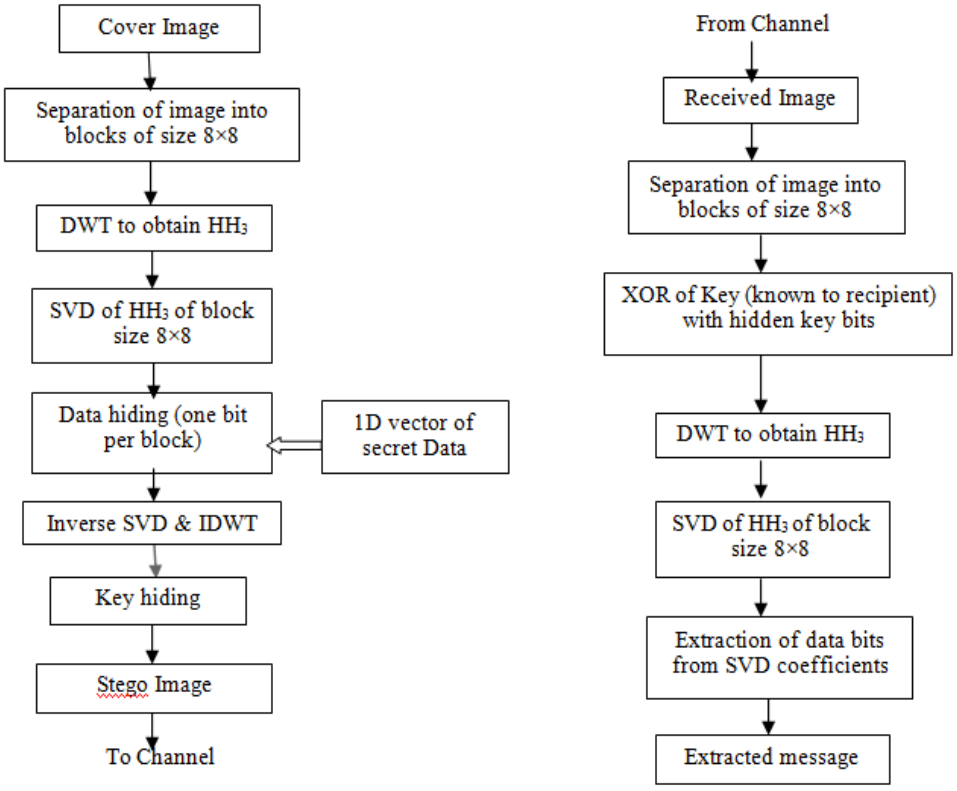


Fig 3(a) & 3(b): Flow Chart of proposed algorithm at transmitter and receiving end respectively

## VI. RESULT ANALYSIS

In this section, the proposed three layered DWT and SVD based algorithm has evaluated with the help of two case studies. Image for the case studies is collected from the web data.

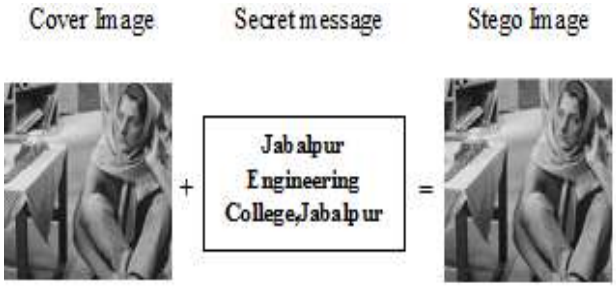


Fig 4: Formation of stego

Case study 1:-

In this case study, the BER between cover image and stego image is calculated and compared with the result of existing steganography algorithm.

Table I: BER comparison

| Parameter | Existing algorithm | Proposed algorithm |
|---|---|---|
| BER between cover image and stego image | 0.29 | 0.1041 |

The lower value of Bit Error Rate (BER) signifies lesser error in the stego image with respect to cover image. Figure: 4 show the stego image formed by hiding secret message into the cover image. Table I provides the comparative BER analysis between previous and proposed steganography algorithm.

Case study 2:-

This case study extends the application of proposed algorithm under the consideration of noise. Here BER is calculated (eq.5) for the measurement of degree of deviation produced in extracted message and original secret message in the presence of noise. Figure: 5 shows Cover image, Secret message and stego image formed for Gaussian noise with SNR = 55dB.

Figure: 6 show the Bit Error Rates between original message and extracted message for different SNRs.

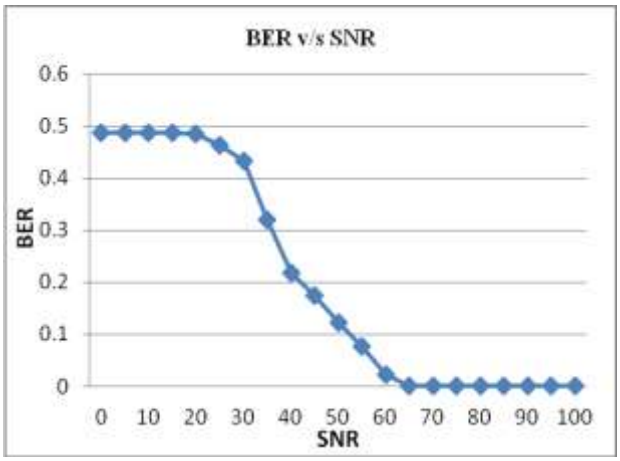


Fig 6: BER analysis with respect to noise

## V. CONCLUSION

The goal of this work is to overcome the drawbacks, which is an essential step to maintain the security of secret message and to allow the intended receiver to extract the hidden message even if any transmission loss occurs. In this paper, the 'three layer DWT and SVD algorithm' as a steganography scheme is proposed and implemented. Experimental results conclude that combined proposed algorithm is quite efficient and can be applied practically.


Fig 5: Formation of stego image for SNR = 55dB

## REFERENCES


[1] Navneet Kaur, Sunny Behal, A Survey on various types of Steganography and Analysis of Hiding Techniques, Volume 11, Number 8, PP 388-392 ISSN 2231-5381

[2] Neil F. Johnson: "Exploring Steganography: Seeing the Unseen", George Mason University, IEEE Computer, pp. 26-34, Feb 1998.

[3] Raman Maini and Himanshu Aggarwal, "A Comprehensive Review of Image Enhancement Techniques", Journal of Computing, Vol. 2, Issue 3, March 2010, ISSN 2151-9617.

[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] 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

[6] 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

[7] Krishna Rao Kakkirala and Srinivasa Rao Chalamala, Block Based Robust Blind Image Watermarking Using Discrete Wavelet Transform, 2014 IEEE 10th International Colloquium on Signal Processing & its Applications (CSPA2014), 7 - 9 Mac. 2014, Kuala Lumpur, Malaysia.

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

[9] Image Steganography using DWT and Blowfish Algorithms IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 8, Issue 6 (Jan. - Feb. 2013), PP 15-19

[10] Incremental Singular Value Decomposition Algorithms for Highly Scalable Recommender Systems University of Minnesota, Minneapolis, MN 55455, USA

[11] Berry, M. W., Dumais, S. T., and O'Brian, G. W. (1995). Using Linear Algebra for Intelligent Information Retrieval. SIAM Review, 37(4).

[12] [Deerwester, S., Dumais, S. T., Furnas, G. W., Landauer, T. K., and Harshman, R. (1990). Indexing by Latent Semantic Analysis. Journal of the American Society for Information Science, 41(6)