Comparative Analysis of Discrete Wavelet Transform and Stationary Wavelet Transform Techniques in Data Hiding

[1]Akhil Mathew, [2]Angel Kurien, [3]Carmel Mary Jose, [4]Cyril Wilson, [5]Anu Abraham Mathew
[1-4]UG Scholars,[5]Assistant Professor
Department of Electronics and Communication Engineering
Amal Jyothi College of Engineering
Kanjirappally, Kerala
[1]akhilmathew80@gmail.com, [2]angelkurien94@gmail.com, [3]carmelmaryjose94@gmail.com, [4]cyrilwilson2794@gmail.com,
[5]anuabrahammathew@amaljyothi.ac.in

***Abstract*— Digital image being one of the best media to store data, provides large capacity for hiding secret information imperceptible to human vision. Hence data hiding finds its application in covert communications, copy control, traitor tracing, authentication of digital images, etc. This paper presents a comparative analysis of data hiding using the techniques: Discrete Wavelet Transform (DWT) and Stationary Wavelet Transform (SWT). The basic data hiding technique consists of the following steps:**

- **Choose a cover image**
- **Encrypt the image to be hidden**
- **Perform DWT/SWT and hide the encrypted image into the cover image**
- **Retrieve the hidden image**

An analysis is performed on the retrieved image and parameters such as Peak Signal to Noise Ratio and Mean Square Error are calculated. On the basis of this analysis, the most efficient technique is proposed.

***Index Terms*—Image encryption, Discrete Wavelet Transform, Stationary Wavelet Transform, Image hiding, Image decryption.**

I. INTRODUCTION

In this rapid technically developing world, sharing multimedia like audio, video and images over the internet has become a trend. Hence providing security and integrity to the confidential data which is passed on internet becomes a major concern. In order to improve the security features, many techniques like cryptography, steganography and watermarking has been developed. Cryptography is the technique used for securing secrecy in communication. Many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, it is sometimes not sufficient to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. This disadvantage is overcome through steganography. Steganography is the art and science of invisible communication. This is accomplished by hiding information in another information, thus hiding the existence of the communicated information. Watermarking is mainly concerned with the protection of intellectual property. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection.

All data hiding techniques are divided into two classes which are:

1. Spatial domain**:** This technique directly hides data into the cover image pixel itself. Here, the pixel value changes with respect to the intensity of image.
2. Transform domain: Here, the image is transformed from time domain to frequency domain using mathematical operators called transforms. There are many transforms like Discrete Wavelet transform, Fourier transform, Discrete Cosine transform, Z-transform and so on. Transform domain enables operation on the frequency content of an image, and therefore high frequency content such as edges and other subtle information can easily be modified. Low frequency band consists of smooth region of an image and hence it contains more information of an image as compared to high frequency band.

II. METHODOLOGY

Most of the strong steganographic systems today operate within the transform domain. Transforms have been effectively used as a powerful tool in many fields like signal processing, physics, astronomy and image processing. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. The use of such transforms will mainly address the capacity and robustness of the steganographic system.

A. Discrete Wavelet Transform

DWT is the transform in which the wavelets are discretely sampled. The main idea involves obtaining a time scale representation of the digital signal through digital filtering techniques. Here, filters of different cutoff frequencies are used to analyze the signal at various scales. The signal is passed through a series of high pass filters to analyze the higher frequencies and is passed through a series of low pass filters to analyze the lower frequencies. The resolution of the signal, which gives the measure of the amount of detail information in the signal, is changed by the filtering operations, and the scale is changed by up-sampling and down-sampling operations. The key advantage of DWT over other transforms is that it captures both frequency and location information. DWT is applied to the entire image to get the HH, HL, LH and LL sub-bands. For the message to be imperceptible, a high frequency component (HH) is chosen for embedding the secret message. DWT provides an appropriate basis for separating the noise from an image. As the wavelet transform is good at energy compaction, the small coefficients more likely represent noise, and large coefficients represent important image features.

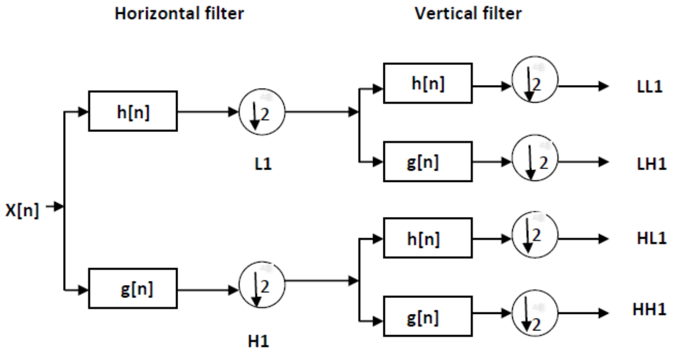

Fig.1 Two dimensional sub-band coding algorithm for DWT

B. Stationary Wavelet Transform

The Stationary Wavelet Transform (SWT) is a wavelet transform algorithm designed to overcome the lack of translation-invariance of the Discrete Wavelet Transform (DWT). The way to restore the translation invariance is to average some slightly different DWT, called un-decimated DWT, to define the stationary wavelet transform (SWT). It does so by removing the down-samplers in the DWT and up-sampling the filter coefficients by a factor of $2^{(j-1)}$ in the j^{th} level of the algorithm. The SWT is therefore an inherently redundant scheme in which the output of each level of SWT contains the same number of samples as the input. So for a decomposition of N levels, there is a redundancy of N in the wavelet coefficients. As with the decimated algorithm, the filters are first applied to the rows and then to the columns. Although four images are produced (one approximation and three detail images) at half the resolution of the original, they are of the same size as the original image. The approximation images from the un-decimated algorithm are therefore represented as levels in a parallelpiped, with the spatial resolution becoming coarser at each higher level with the size remaining the same.

The 2D SWT is based on the idea of no decimation. SWT omits both down-sampling in the forward and up-sampling in the inverse transform. More precisely, it applies the transform at each point of the image and saves the detail coefficients.

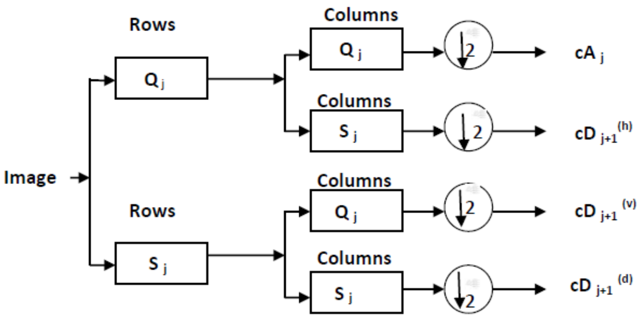

Fig.2 SWT decomposition scheme

III. PROPOSED METHOD

The proposed scheme consists of three main phases: image encryption, data embedding and data extraction. The cover image is first selected from the database. Discrete Wavelet Transform and Stationary Wavelet Transform is performed before embedding the secret image to get the stego image. A key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the cover image in order to view the secret image. The stego image should look identical to the cover image.

A. Embedding Algorithm

Step 1: Select cover image and perform DWT/SWT transform to get LL, LH, HL and HH components
Step 2: Find size of HH component
Step 3: Select secret image and convert to grayscale
Step 4: Resize the secret image to the size of HH component
Step 5: Generate random number which serves as key and create key array
Step 6: Encrypt the secret image by performing bitwise XOR operation with the key array
Step 7: Place the encrypted image on the HH component
Step 8: Perform IDWT/ISWT with the renewed HH component to get the intermediate image
Step 9: This intermediate image is again put into the HH component of another cover image to get the stego image

B. Extraction Algorithm

Step 1: Perform DWT over the received image and original cover image
Step 2: Subtract the HH portions of the cover image with from the received image
Step 3: Perform DWT on this subtracted data
Step 4: Remove normal HH from the HH received from step 3
Step 5: Generate key array
Step 6: Perform bitwise XOR operation of the key array and the result of step 4 to get the secret image

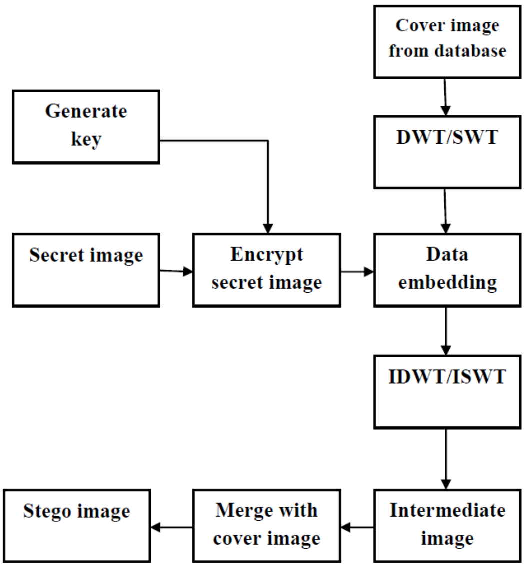

Fig.3 Block diagram of embedding process

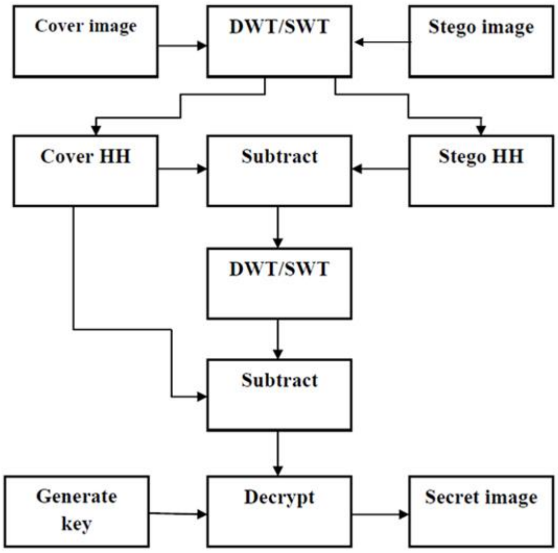

Fig.4 Block diagram of extraction process

C. Performance Parameters

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image quality. The MSE represents the cumulative squared error between the extracted hidden image and the original secret image. PSNR represents a measure of the peak signal to noise. Peak Signal to Noise Ratio (PSNR) is calculated to analyze quality of image. Here, a comparison of the PSNR results of the two techniques DWT and SWT is done by this algorithm. The PSNR calculation of two images, one original secret image and extracted image, describes how far two images are equal. PSNR in dB given as

$$PSNR(dB) = 10log_{10}(\frac{R^2}{MSE})$$

where R= maximum pixel dimension

The mean square error is calculated by the equation

$$\frac{1}{MSE} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I(i,j) - K(i,j)]^2$$

where M represents the number of rows and N represents the number of columns. I and K are the matrix of the extracted image and the original secret image at (i,j)th pixel respectively.

D. Advantages of proposed method

1. Hiding data only in certain regions of the cover data increases the security level.
2. No one can extract the data until and unless they get the value of the key.
3. Data is hidden in the higher frequency band rather than the lower frequency band. Hence a good stego image quality is obtained.

IV. SIMULATION RESULTS

Simulation is carried by using MATLAB software. The simulation results are shown below.

Fig.5 Cover image

Fig.6 Secret image "flower.jpg"

Table 1. Comparison of PSNR and MSE values

Secret image	PSNR value	MSE value	Method
Baboon	42.84 40.81	3.41 5.44	DWT SWT
Football	51.25 46.86	0.49 1.35	DWT SWT
Lena	55.48 68.59	0.05 0.01	DWT SWT
Flower	35.7 39.86	4.48 6.77	DWT SWT

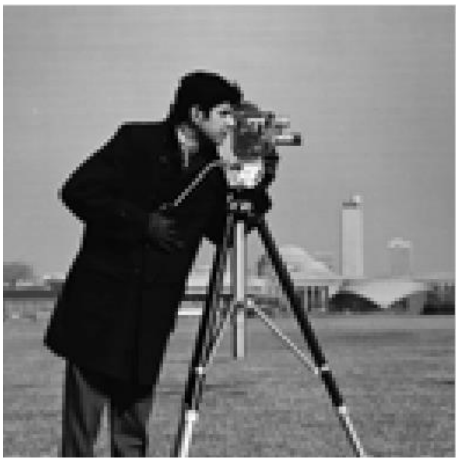

Fig.7 Image after embedding using DWT technique

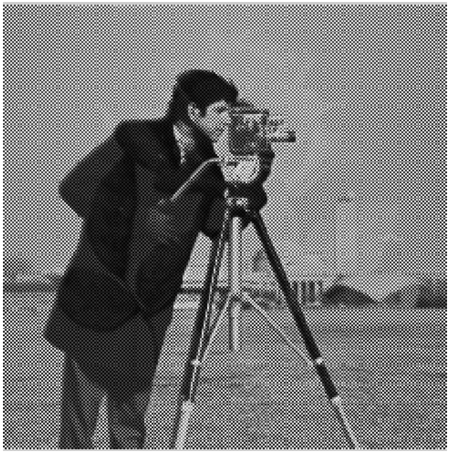

Fig.8 Image after embedding using SWT technique

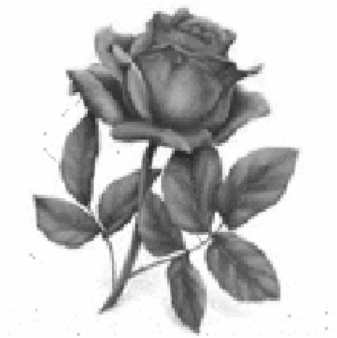

Fig.9 Secret image after extraction using DWT technique

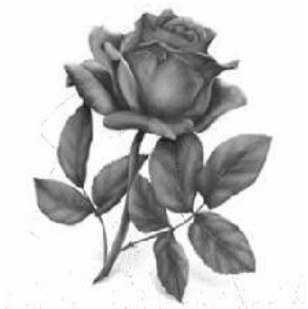

Fig.9 Secret image after extraction using SWT technique

V. CONCLUSION

This work is a comparison of data hiding using the transform based techniques – Discrete Wavelet Transform and Stationary Wavelet Transform. The proposed technique uses DWT/SWT to decompose an image into various sub-bands, and then the encrypted secret image is hidden in the high frequency sub-band of the image. Afterwards, by performing IDWT with the altered frequency sub-bands, the image is reconstructed. The proposed technique has been tested on various images and image quality is assessed by using performance parameters like PSNR and MSE. The embedded image should be absolutely invisible to human eye to achieve a good stego image quality. It is observed that for Baboon and Football, the PSNR values are higher for DWT than for SWT but is the reverse for Lena and Flower. Thus we reach the conclusion that SWT performs better for lesser variation between cover image and secret image whereas DWT performs better for higher variation conditions.

REFERENCES

[1] Shilparani Noubade and Hemavathi.N.V, “Private Confidential Data Hiding by Using Wavelet Approach”, International Journal of Electronics & Communication Technology, Vol. 5, Issue 4, 2014

[2] Patel Roshni, Aslam Durvesh and Patel Urvisha, “Lossless Method for Data Hiding In Encrypted Image”, International Conference on Innovations in Information Embedded and Communication Systems, 2015

[3] Swapnali Zagade and Smita Bhosale, “Secret data hiding by using DWT”, International Journal of Engineering and Advanced Technology, 2014.

[4] Suchi Sharma and Uma kumara,”High capacity data hiding technique using steganography”, International journal of emerging trends and technology in computer science, 2013.

[5] Komal Hirachandani, Gaurav Soni and Rajesh Nigam, “New Approach of Information Security through Steganography by using Wavelet Transformation and Symmetric Encryption”, International Journal of Computer Science and Information Technologies, Vol. 5 , 2014

[6] Kanzariya Nitin K., Nimavat Ashish V., “Comparison of Various Images Steganography Techniques”, International Journal of Computer Science and Management Research Vol 2, 2013