Implementation of Stegnographic Image using Symmetric Framelets

Shashidhara H. R.

Department of Electronics and Communication, The National Institute of Engineering, Mysuru-570008

Abstract: Common ways to conceal the existence of concealed data within a cover object is using steganography. Steganography can be applied to images as one of the appropriate cover objects. It displays the private data that can be transformed into image, video, and audio formats. This paper provides a Lifting scheme based Symmetric framelets for implementation of Steganographic Image using Discrete wavelet Transform. The optical cover picture is absent. The Stego pictures yield very good numbers for the Peak Signal to Noise Ratio.

Keywords: *Steganography, DWT, Lifting scheme, Symmetric Framelets.*

1. Introduction

Nowadays, internet users usually need to send, receive, or save confidential information. The most popular method for doing this is to convert data into a different format. Only those who know how to restore the data to its original state can comprehend the altered data. Thus, encryption is the process of securing the data in this way. A major disadvantage of encryption is that existence of the data is not secured. A solution to this problem is Steganography. The Greek words "stegano," which means "covered" or "secret," and "graphic," which means "writing" or "drawing," are the main roots of the word "steganography." Steganography is the art and science of concealing confidential data [1].

Steganography is a pre-security invention where a cover contains the hidden data. Steganography's primary goal is to conceal the communication process under a secure cover medium. The cover medium can be audio, text, video or computer files. The three very important characteristics of Steganography are capacity, security and robust [2].

Capacity refers to the amount of information that can be embedded into cover medium. Security is the inability to detect the secret information. Robustness is the amount of modification that can be made to the Stego medium without destroying the secret information. The fundamental requirements of Steganography are imperceptibility of embedding, exact recovery of secret data and large payload. he two primary categories of steganography concealment techniques are spatial domain techniques and frequency domain approaches. The hidden information is directly incorporated into the cover object when using spatial domain approaches. The Spatial domain techniques are attractive because of simpler implementation, high payload and easy control on quality of Stego image. The drawback of this approach higher chances of Steganalysis methods. In frequency domain techniques, cover image which is used to hide the secret image is converted into frequency domain co-efficient. Discrete Wavelet (DWT), Discrete Cosine (DCT), and Fast Fourier (FFT) transforms are the most used transforms. The advantage of the Frequency domain technique over Spatial domain are high resistance against Stegano-analysis methods and signal processing manipulation but transformation into frequency domain is bit complex. The wavelet-based techniques are more robust when compared to other techniques and through this technique good quality Stegoimages are obtained [3].

2. Related Work

Seyyed Amin Seyyedi at al [4] in this method image partitioned into 8x8 block and then for each block IWT through lifting scheme is performed. In order to provide secured Steganographric method we use frequency domain partition approach. Therefore, the secret message is encrypted using the symmetric RC4 method for high security and authentication, and a tree scan order is carried out in the frequency domain to choose the appropriate location for the confidential message. The suggested approach offers enough security and stability against statistical attacks, as well as two layers of protection to preserve the embedded message, so the secret information can be in a lossy channel. E. Prakash and G. Kanaganvalli at al [5] use to prevent noise and attacks, the secret information is embedded in the lowest plane and the random noise is replaced by hidden pieces of information. The embedded data which is retrieved from Steganography process leads to very less image distortion. However, capacity constraints have prompted us to consider a better approach. In LSB embedding, always some information is lost from cover image.

Mehdi Safarpor and Mostafa Charmi at al [6] in most of the technique, increasing in the capacity leads to decrease in the quality of the Stego image. So in this paper we combine two technique PVD and GLM technique to emerge up with a hybrid Steganography scheme to hide information without affecting quality of stego image. This proposed method has two phases, in first phase by using PVD method secret data are embedded within the image and in second phase the remaining data are mapped by GLM technique. The proposed method improves capacity by 25 while the PSNR valve is declined by 2.

Komal Hirachandani at al [7] in this paper to enhance the security of information cryptography technique is used. Wavelet transformation is a compression method that is used for big amounts of data that shrinks the size of the data. With wavelet transformation, the original information's size can be decreased and its efficiency raised. Using the encryption technique, secret data is separated into its binary value, and 128 bits are chosen at a time to carry out operations. In the Decryption technique chipper information is divided into its binary value and 128 bits are selected at a time to perform operation during the whole process. In this paper, picture compression is achieved by the application of wavelet transform with lossless approach. This technique reduces a big quantity of image and inserts it using the LSB technique.

Sachin Mungmode, and et. Al.[8] attempted to improve the quality and the modification rate of a Stego Image. From the threshold value, the high frequency pixels from the cover image are chosen. The Sobel Edge Detector algorithm makes use of Sobel's operator to extract the edges. It is the gradient operator, or Sobel operator. A Gaussian operator is used by the clever edge detector method to extract an image's edges. The Least Significant Bit matching revisited algorithm employs two pixels from the cover image to conceal the secret message. By using the LSBMR algorithm, the asymmetry property that the standard LSB approach created is removed. Pixel pairs and message bits are fed into LSBMR for data encoding. The parameters PSNR and MSE are used to measure an image's quality and modification rate, respectively. Comparing the suggested Threshold Value approach to the Sobel and Canny-based strategy, the results show an improvement in image quality of roughly 0.2% to 0.6%.

Mamta Junja and Parvinder SinghSandhu at al [10] Used a hybrid feature detection technique, this research study attempts to suggest an extra information security measure. There are two methods for data hiding: the adaptive LSB substitution approach and the component based Least Significant Bit Substitution methodology. Moreover. The two-tier security provided by an Advanced Encryption Standard is enhanced by Random Pixel Embedding, which makes it more resilient to visual and statistical attacks, and Hybrid Filtering, which increases its resistance to different disturbances like noise.

3. Implementation

Encoding: Embedding of data requires two files. The first image called cover image holds hidden information. The second image that holds information to be hidden is called Stego image. The hiding of Stego image inside the cover image is called Steganographic image. An image is an array of numerical values that represent light intensities at various points. These pixels make up the image raster data [9]. A common image consists of 640x480 pixels and 256 colors. Hence, such images can contain 300kilobits of data. This image is converted into bit map file using wavelet transformation.

Decoding: The Steganographic image contains both cover image and Stego image. At receiver side, the secret message is extracted from cover image by using inverse LDWT.

A. Discrete Wavelet Transform

The small oscillating wave in time domain is called wavelets. The simultaneous frequency and time analysis is performed because of the oscillating wavelet characteristics.

A wavelet function Ψ(t) as two prosperities.

$$\int_{-\infty}^{0} \Psi(t)dt = 0 \quad (1)$$

That is, the function has oscillatory or wavy appearance [10].

$$\int_{-\infty}^{0} \Psi(t)dt < \infty \quad (2)$$

Wavelet transforms are based on small waves called wavelets of limited time and variable frequency band. Wavelets are used in the picture steganography model for transformation because they can distinguish between high-frequency and low-frequency information on a pixel-by-pixel basis. If the function is being expanded discrete the resulting co-efficient is called DWT.

For example,

$f(n = f(x_0 + m\Delta x))$ Where, m=0,1,2,3,….N-1. (3)

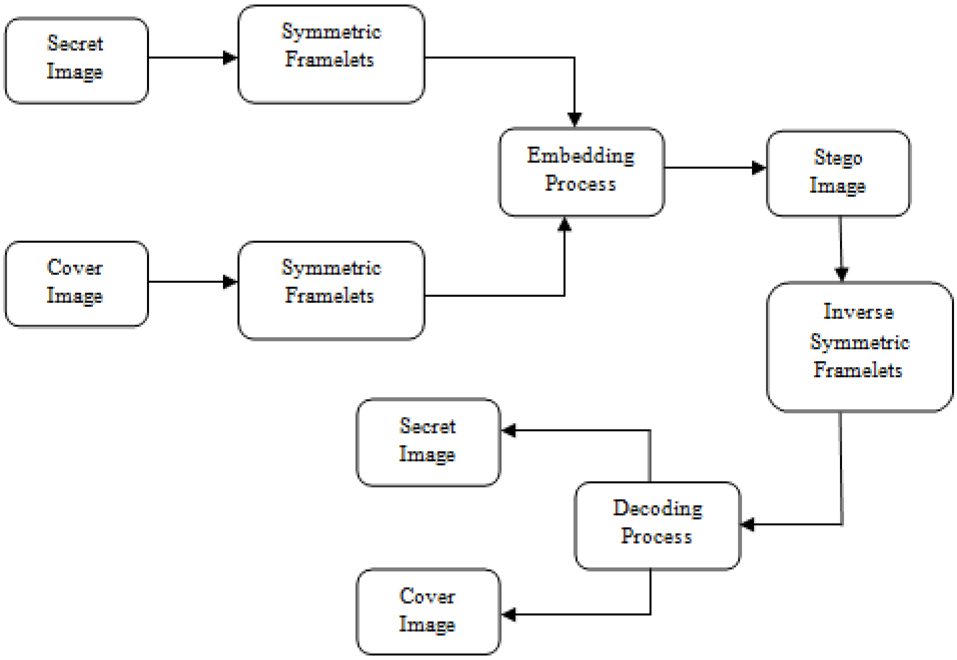

Fig.1. Block diagram of the system

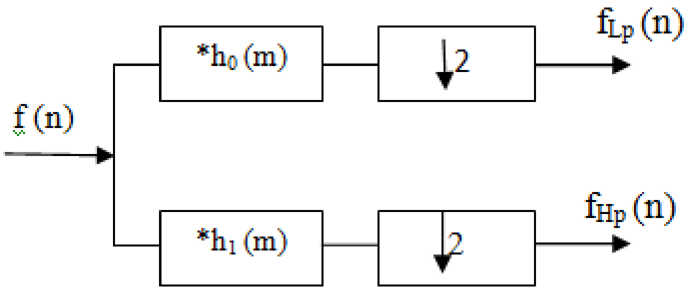

Fig.2. DWT [10]

The filter h0(z) and h1(z) are used to split the input signal f(n) into half-length sequence of flp(n) and fhp(n). The low pass filter h0(z) output is called approximation of f(n) and the high pass filter h1(z) output is called detail part of f(n) [11]. To reduce the number of computations down sampling is used. The resulting subbands can be further divided into four smaller subbands which can be spilt again. The resulting filtered output can be as follows approximation, vertical, horizontal and diagonal component.

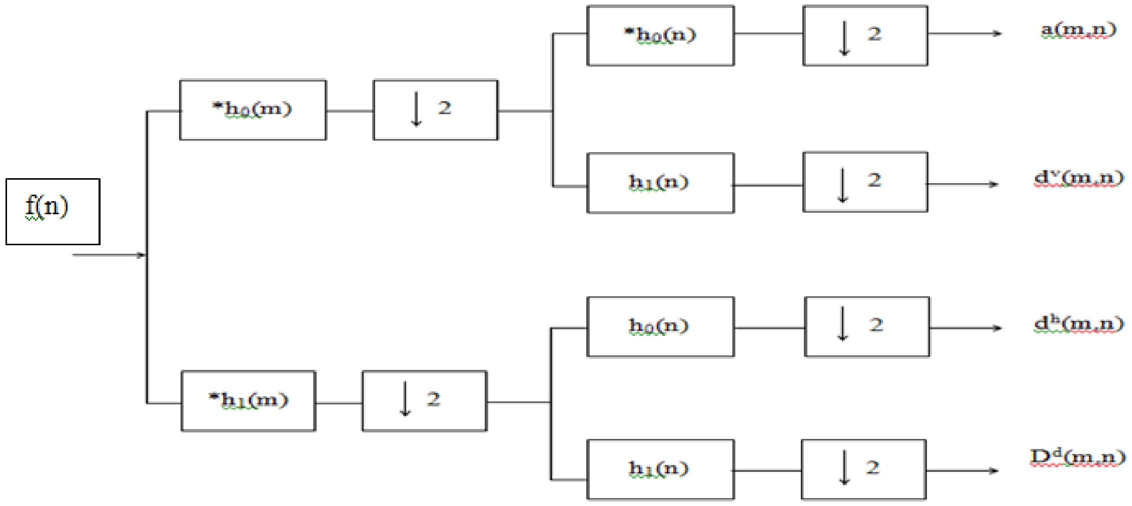

Fig.3. Two DWT [10]

B. Lifting Scheme

Wavelets based on the time domain can now be constructed and performed using the Lifting scheme. The lifting scheme has three phases. First, the data in Split is separated into even and odd components. Next, while predicting it uses a function to approximate the data set [12]. The odd parts of the data set are replaced with the discrepancies between the estimate and the actual data. The even elements remain unaltered and serve as the input for the subsequent transformation phase. Equation 4 describes the predict stage, in which the odd value is anticipated from the even value.

$$odd_{j+1,i} = odd_{j,i} - p(even_{j,i}) \quad (4)$$

An average is used in place of the even elements in the update. This makes the input for the wavelet transform's subsequent stage smoother. It is possible to create filters since the odd elements also approximate the original data set. The update phase follows the predict phase as shown figure 2. The original values of the odd elements and its even predictor is described in (5).

$$even_{j+1,i} = even_{j,i} + U(odd_{j+1,i}) \quad (5)$$

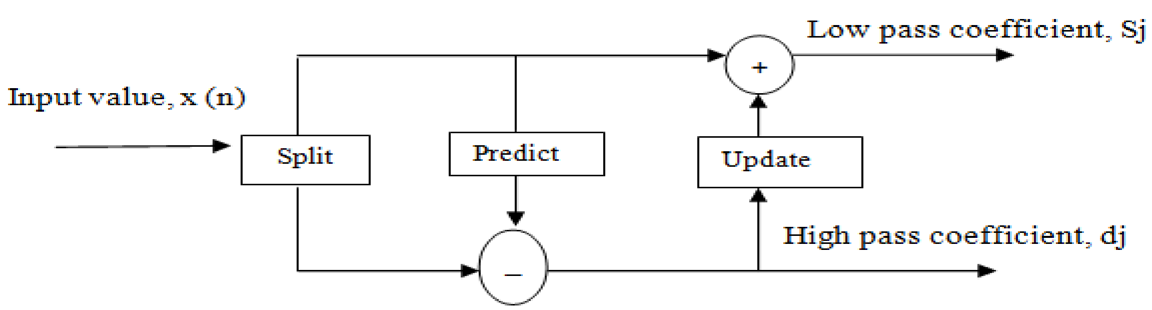

Fig.4.Lifting scheme [13]

When using 9/7 wavelet, there are two predict and update stages [13]

$$Predict\ P1: d[i] = x_0[i] + a(x_e[i] + x_e[i+1]) \quad (6)$$

$$Update\ U1: s[i] = x_e[i] + b(d[i-1] + d[i]) \quad (7)$$

$$Predict\ P2: Y_H[i] = d[i] + c(s[i] + s[i+1]) \quad (8)$$

$$Update\ U1: Y_L[i] = s[i] + d(Y_H[i-1] + Y_H[i]) \quad (9)$$

a,b,c,d, and k are coefficients of Predict, Update and scaling, derived from 9/7 filter coefficients.

Were,

a=-1.586134342,

b=-0.0529801185,

c=0.882911076,

d=-0.443506852 and

k=-1.149604398

$$Y_H[i] = kY_H[i] \quad (10)$$

$$Y_L[i] = 1/kY_L[i] \quad (11)$$

High and Low pass filters are used to implement the DWT and it is expressed as

$$p(z) = \begin{bmatrix} 1 & \alpha(1+z-1) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \beta(1+z) & 1 \end{bmatrix} \begin{bmatrix} 1 & \gamma(1+z-1) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \delta(1+z) & 1 \end{bmatrix} \begin{bmatrix} \zeta & 0 \\ 0 & 1/\zeta \end{bmatrix} \quad (12)$$

Where α=a, β=b, γ=c, δ=d and ζ=e

C. Symmetric Framelets

The set of wavelets Ψi, i=0, 1, 2…..N-1 constitutes a frame when for a 0<A<B<∞ any function f ∈L2. After decomposing an image, symmetric property is applied for the feature extraction. Here we extract maxim block frame called symmetric framelets from decomposed image [14]

$$A\|f\|^2 \le \sum_{n \in z} |< f, fn|^2 \le B\|f\|^2 \quad (13)$$

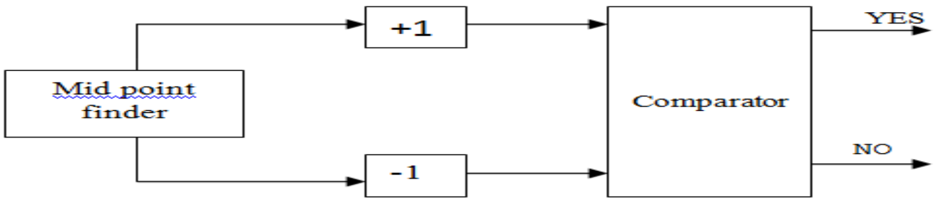

Fig.4.Symmetric checker

D. Inverse Discrete Wavelet Transform

IDWT retrieves the original picture pixels by using low pass and high pass coefficients that are derived from Forward DWT. To obtain even-positioned pixels, high pass coefficients are first added with their delayed coefficients, multiplied by Update, and then deducted from low pass coefficients. To create oddly positioned pixels, these even-positioned pixels are then multiplied by their delayed values, added to high pass coefficients, and finally multiplied by predict. To recover the original image pixels, both even and oddly positioned pixels are finally combined.

---

4. Results

The fig 5 shows the segmented and de-segmented values of a decomposed image using lifting scheme-based DWT. The divided data is provided in the complement of two. After serialization, the input data is transformed into signed digits. Following serial signing, the digits are sent into the DWT, which is divided into nine pipeline phases. Following the last step, the DWT-transformed data is once again transformed into two's complement, producing values that have been segmented and de-segmented.

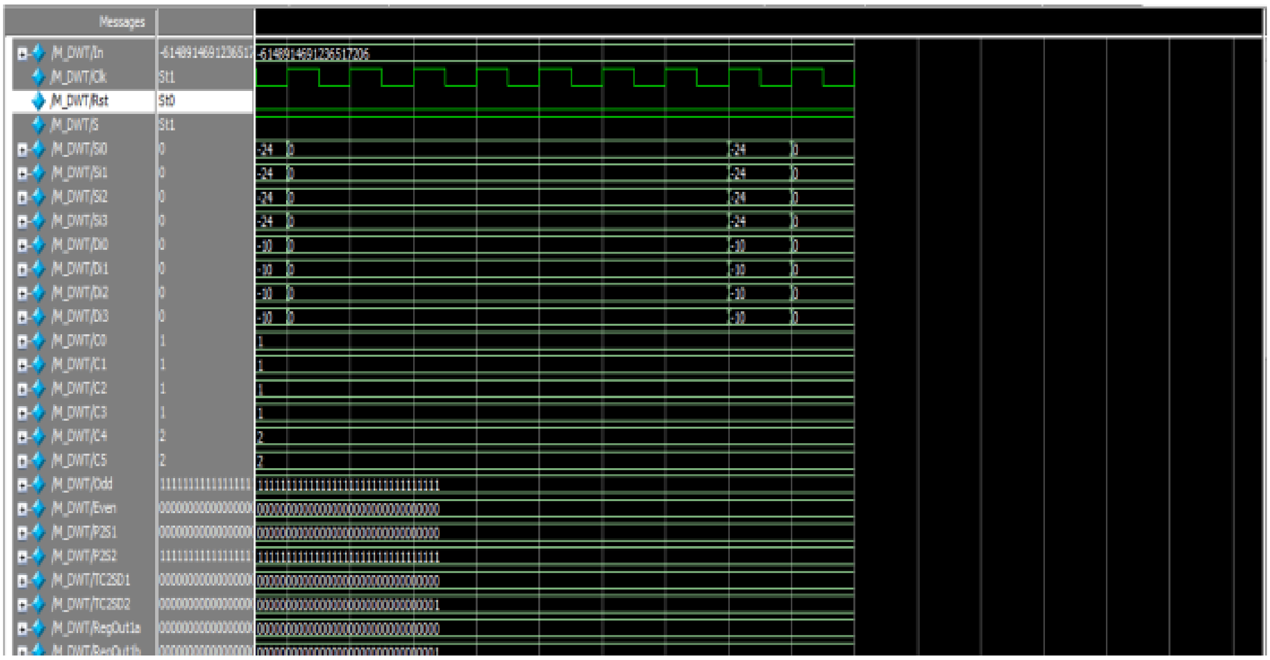

Fig.5. Functional Simulation of DWT module

The functional simulated output of symmetry checker is shown in Fig 6. The de-segmented values are then passed to symmetry checker for feature extraction.

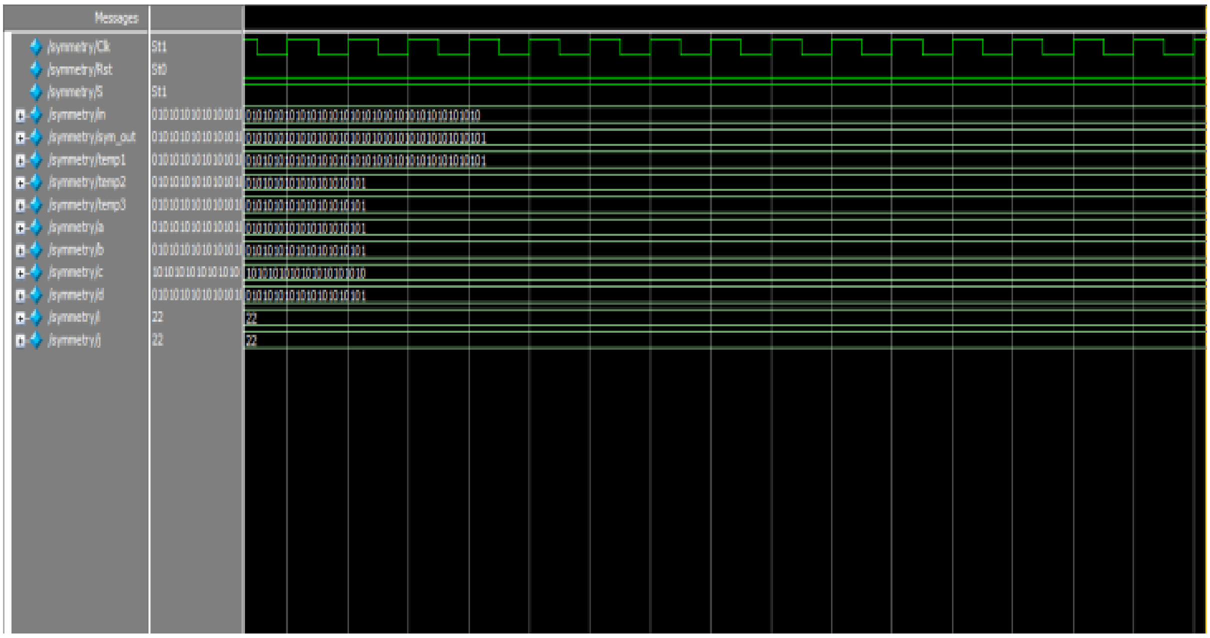

Fig .6. Functional Simulation of Symmetric module

The fig 7 shows embedding data into an image. Here, the original and modified image is transformed into bit map files, and then DWT is used for decomposition, and Symmetry Checker is used to extract features.

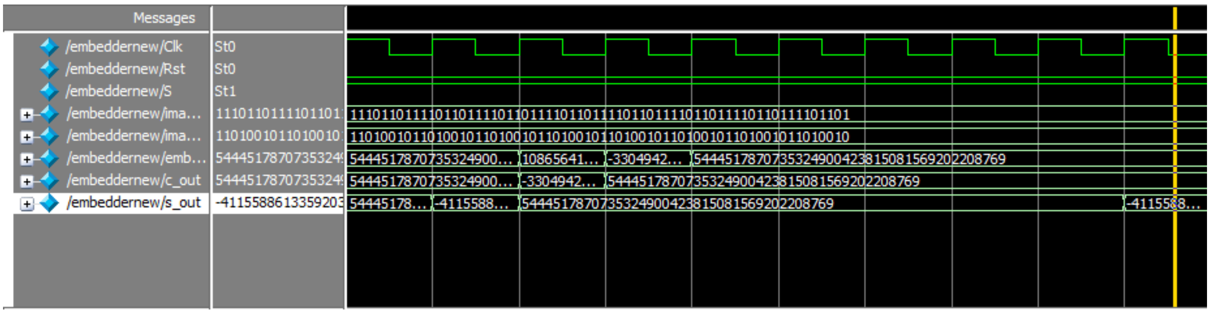

Fig.7. Functional Simulation of embedded module

The fig 8 shows the merged output of segmented and desegmented values of a decomposed image using lifting scheme based IDWT. The merged data is obtained from parallelized two's complement. The serialized input signed digits are initially passed into the IDWT, which is partitioned into 9 pipeline stages. After the final stage, the IDWT transformed data is converted back into two's complement giving merged segmented and de-segmented values.

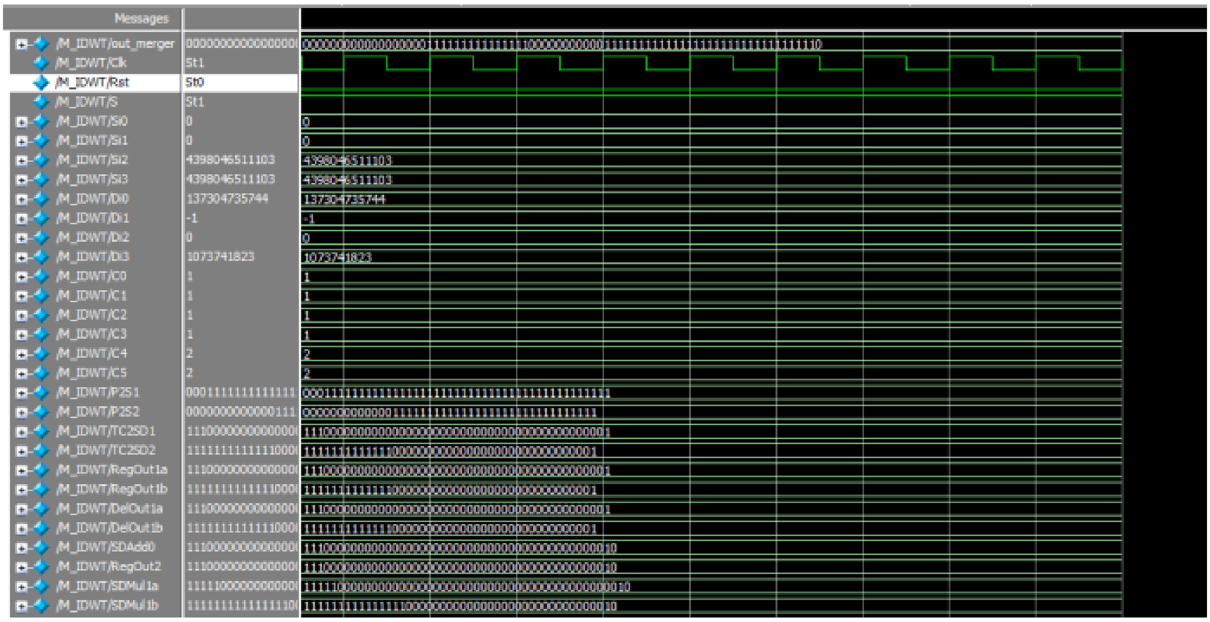

Fig.8.Functional Simulation of IDWT module

5. Conclusion

This paper, we notice that the secret image can be concealed in one cover image. The impact of using symmetric framelets for data hiding in a transformed domain results in high quality of the Stego image having good PSNR values compared to other methods. It has been concluded that using color images as a cover object is better than using gray scale images for data hiding. Symmetric components are used for data hiding to provide higher capacity while maintaining good Stego image quality. This approach can be implemented in FPGA to test computational speed with other methods.

Refrences

[1] Ali Al Ataby and Fawzi Al-Naima “A Modified High capacity Image Steganography Technique using Wavelet transform,” The international Arab Journal of information Technology, Vol. 7, No 4,October 2010.

[2] T. Morkel, J.H.P. Eloff and M. S. Olivier “An overview of Steganography,” South Africa conference, June/July 2015.

[3] Suvana Patil and Gajendra Singh Chandel “Performance analysis of Steganography based on 5-wavelets families by4 levels-DWT,” International journal of Advance research in Computer Science and Management Studies, Vol.1, December 2013.

[4] Syyed Amin Seyyedi and Vasili Sadau,Nick Ivanov “A secure Steganography method based on Integer Lifting Wavelet Transform,” International Journal of Network Security, Vol. 18, No 1, PP.124, Jan 2016.

[5] E.Prakash and G.Kanaganvalli “Realization of Steganography using LSB-Development information Hiding algorithm” International Journal on Concurrent Applied Research in Engineering and Management, Vol 1,May 2015.

[6] Mehdi safarpour and Mostafa Charmi “Capacity Enlargement of The PVD Steganography Metod using The GLM Technique”, International Journal of Network Security, Vol 5, 2014.

[7] Komal Hirachandani, Gauray Soni and Prof.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.

[8] Mamta Juneja and Parvinder Singh Sandhu “Improved LSB based Steganography Techniques for color Images in Spatial Domain,” International Journal of network Security, Vol.16, No 4, PP.366-376, July 2014.

[9] Sachin Mungmode, R. R. Sedamkar and Niranjan Kulkarni “An Enhanced Edge Adaptive Steganography Approach using Threshold Value for Region Selection”, June 2014.

[10] Ketan Shah, Sawti Kaul, Manoj S.Dhande “Image Steganography using DWT and Data Encryption Standard,” International ofter Science and research, Vol.3, Issue 5, May 2015.

[11] Somisetti Asha Latha and Maddireddy Sowjanya “FPGA Implementation of Digital watermarking using Discrete Wavelets Transformation,” International Journal of Scientific Engineering and Technology Research, Vol.3, Issue 27, September 2014.

[12] Basrnali Gupta Banli and Prof.Sanir K.Bandyopadhyay, “A DWT method for Image Steganography,” International journal of Advanced research in computer science and Software engineering, Vol. 3, Issue 6, June 2013.

[13] Chao-Tsung Huang, Po-Chin, Tsung and Liang-Gee Chen, “Flipping structure: An efficient VLSI Architecture for Lifting–Based DWT,” IEEE transaction of Signal Processing, Vol.52, No 4, April 2004

[14] Shashidhara, H. R., and A. R. Aswath. "A novel approach to circular edge detection for iris image segmentation." In *2014 Fifth International Conference on Signal and Image Processing*, pp. 316-320. IEEE, 2014.

[15] Wei-Hsin Chang, Yew-San Lee, Wen-Shiaw Peng and Chen-Yi Lee, “A Line-Based, Memory Efficient and Programmable Architecture for 2D DWT using Lifting Scheme,” IEEE transaction, 2001.

[16] A Farras Abdelour and Ivan W.Selesnick “Symmetric Nearly shift Invariant Tight Frame wavelets,” IEEE transaction on Signal Processing, Vol.53, No 1, January 2005.