

A NOVEL TECHNIQUE OF IMAGE STEGANOGRAPHY

Ravneet Kaur

Research Scholar(M.Tech)
Department of Computer Science and Engineering
CGC Technical Campus, Jhanjeri (Mohali)
Mohali, India
Kaurravneet27@gmail.com

Er Chander Prabha

Associatet Professor
Department of Computer Science and Engineering
CGC Technical Campus, Jhanjeri (Mohali)
Mohali, India
c.prabha.cgc@gmail.com

Abstract—Steganography is the technique of hiding secret information within any media like text, images, audio/video and protocol based network. Steganography is an important area of research in recent years involving a number of applications. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected. Transform domain methods hide messages in insensitive areas of the cover image which makes them more robust to attacks. DCT/DWT is used to transform cover image from spatial domain to frequency domain. The secret image or information is then embedded into the frequency domain coefficients. This paper proposed a novel technique for data hiding and compares it with DCT, DWT and hybrid transform domain technique for embedding secret image into cover image. The algorithms are compared for Signal to Noise Ratio (SNR) which is a measure of the difference between the cover image and the stego image.

Keywords: Data hiding, Cover-media, Cover-object, Stego-image, Stego-key, Image Steganography; Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT).

I. INTRODUCTION

Hiding secret data is of prime importance for security purposes. Multimedia is the key for achieving this, so, any of the media such as text, audio, video and image can be used to hide data for security. The formats that are more suitable are those with a high degree of redundancy. Image is a good cover medium for concealing secret data as it contains more redundant information. Image Steganography protects the data from illegal access by hiding the data into a cover image such that an unintended observer is not aware of the existence of the hidden data. Steganography basically consists of three things: cover object (used to hide secret message), secret message to be embed, and stego object (cover object after hiding the secret data) As human

eyes are not sensitive for identifying little changes in an image, this fact can be used for hiding data in an image[1].

To provide the overview of steganography, firstly some terms are explained as.

Steganography terminologies are as follows:-

- **Cover-Image:** Original objects which are used as a carrier for conceal the information.
- **Message:** Actual information which is used to be hide. Message could be a text or some other image.
- **Stego-Image:** After embedding message or secret information into cover object is known as stego-object.
- **Stego-Key:** A key is used for embedding or extracting the messages from cover-object and stego-objects.

Image steganography is a method of hiding the information into cover-image and generates a stego-image. That stego-image then sent to the other party by some known medium, where the third party does not know that this stego-image has hidden message. After receiving stego-image hidden message can simply be extracted with or without stego-key by the receiving end.

Basic diagram of image steganography is shown in given figure without stego-key,

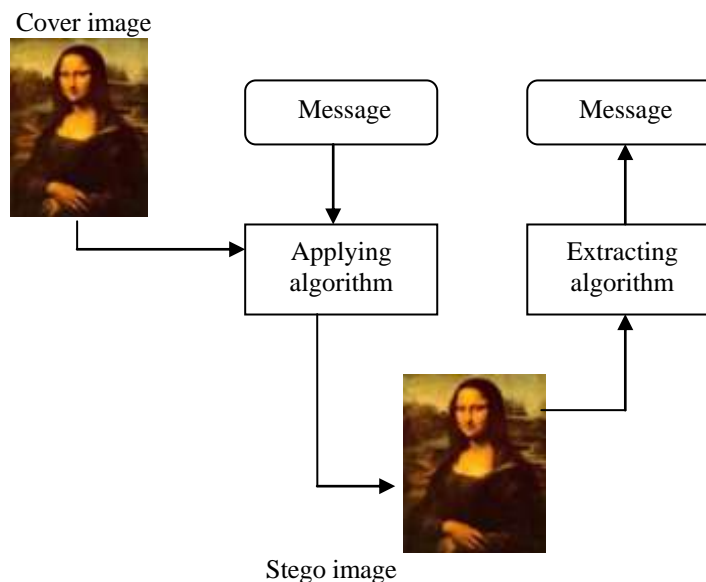


Figure 1. Image Steganography [9]

where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm extracts the message from stego-image[9].

II. RELATED WORK

Mukta Goel and Rohit Goel et.al This paper represents the hiding text in an image file using Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography and the Hybrid Image steganography which is a combination of DWT and DCT steganography and evaluate it on the basis of its factors that are PSNR and MSE[1].

Stuti Goel et.al This paper deals with hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography. The LSB substitution algorithm is implemented in spatial domain, in this the payload bits are embedded into the least significant bits of cover image to produce the stego-image whereas in DCT & DWT algorithm are implemented in frequency domain in which the stego-image is transformed from spatial domain to the frequency domain and in this the payload bits are embedded into the frequency components of the cover image. Then the performance and comparison of these three techniques is evaluated on the basis of these parameters PSNR, MSE, Capacity & Robustness.[15]

G.Arun Karthick et.al this paper represents a new scheme which is hybrid in nature, it combines two distinct domains 1)Steganography(Combination of Image + cryptography) .

2) Image Fusion – Fusing two images.

Steganography embeds the digital data message along with the media file where digital data may be text, image or hybrid. Although both Cryptography and steganography techniques are combined to provide security in some criteria yet advanced system of security is needed to share information without any interference. To overcome the real world problem, they proposed a novel algorithm called StegFuse where cryptography and steganography is applied on two various types of images, and then after applying steganography technique both of these images are subjected to image fusion so as to get the fused image. Wavelet transform technique is applied on both the image during fusion[4].

Inderjeet Kaur et .al The technique proposed is a combination of steganography and watermarking (TDSSW)which provides copyright protection to the information being transmitted secretly over communication channel. The proposed technique is a transform domain based technique. At end it was observed that the proposed technique comes up with good PSNR (Peak Signal to Noise Ratio) value and enhanced Security.

Sneha Arora et.al (May2013) This paper proposed a new technique for the image steganography using edge detection method for RGB images. There are many algorithms to hide data with precision level but they are also decreasing the quality of the image. In this proposed study, the edges of an RGB image will be detected by scanning method using a 3x3 window, and then text will be embedded in to the edges of the color image. So by doing this not only high embedding capacity will be achieved,but it also enhances the quality of the stego image from the HVS (human vision system)[16].

H. B. Kekre et.al(June2014) In this paper the author has proposed a Hybrid Approach so as to secure digital images. The proposed framework introduced is a combination of Information Hiding and Image Encryption. For Information Hiding, four different methods of Multiple LSB's

Algorithm are used in this paper and then they are evaluated. A number of parameters are also used to evaluate the performance of the proposed framework. At last Experimental results show a good performance.

III. TRANSFORM DOMAIN TECHNIQUES

New algorithms keep emerging prompted by the performance of spatial domain techniques due to rapid development of information technology and by the need for enhanced security system. As seen in the spatial domain techniques, LSB modification of images is an easy technique to embed information, but these are highly vulnerable to even small cover modifications [7]. An attacker can simply apply signal processing techniques in order to destroy the secret information entirely [8]. Most robust steganography systems known today actually operate in some sort of transform domain. Transform domain methods hide messages in insignificant areas of the cover image which makes them more robust to attacks. Many transform domain variations exist. One method is to use the Discrete Cosine Transformation (DCT) as a technique to embed information in images; another would be the use of wavelet transforms. Transformations can be applied over the entire image, to blocks throughout the image, or there may be other variations. However, a trade-off exists between the amount of information added to the image and the robustness obtained [1].

A. DISCRETE COSINE TRANSFORM (DCT)

The two dimensional DCT is the heart of the most popular lossy digital image compression systems today. This method encodes the secret information in the frequency domain by modulating the relative size of two or more DCT coefficients in an image.

It is an orthogonal transform, which has a fixed set of (image independent) basis functions, an efficient algorithm for computation, and good energy compaction and with correlation reduction properties.

The 1D DCT of a $1*N$ vector $s(j)$ is defined as

$$X_k = \frac{1}{2}(x_0 + (-1)^k x_{N-1}) + \sum_{n=1}^{N-2} x_n \cos \left[\frac{\pi}{N-1} nk \right]$$

Where $k = 0, 1, \dots, N - 1$

The DCT can be extended to the transformation of 2D signals or images [1]. This can be achieved in two steps: by computing the 1D DCT of each of the individual rows of the two dimensional image and then computing the 1D DCT of each column of the image[1]. In digital image processing, the two dimensional version of DCT is used which is given as:

$$X_k = \sum_{n=0}^{N-1} x_n \cos \left[\frac{\pi}{N} \left(n + \frac{1}{2} \right) k \right] \quad k = 0, 1, \dots, N - 1$$

B. DISCRETE WAVELET TRANSFORM (DWT)

A wavelet is simply a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficients and functions. These set of coefficients are called the Discrete Wavelet Transform (DWT) of a signal [10]. DWT has spatial frequency locality, which means that if signal is embedded, it will affect the image locally. Also, they do not take into account the fact that different regions in an image may have different frequency characteristics.

The forward 2-D DWT can be implemented using a set of up-samplers, down-samplers, and recursive two-channel digital filter banks. There are many available filters, but the most commonly used are Haar Wavelet filters, and Daubechies filters. Important properties of wavelet filters in digital image compression are symmetry (used for avoiding artifacts at the borders), orthogonality (fat algorithm), regularity, and degree of smoothness.

When applying DWT on an image, four different sub-bands are obtained, which are LL, LH, HL, and HH as shown in figure 2.

- LL: A coarser approximation to the original image containing the overall information about the whole image. Since human eyes are much sensitive to the low frequency part, this is the most important component in the reconstruction process.
- HL and LH: They are obtained by applying the high pass filter on one coordinate and the low pass filter on the other coordinate.
- HH: It shows the high frequency component of the image in the diagonal direction.

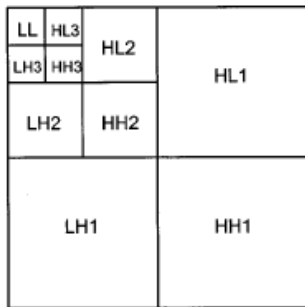


Fig. 2: Spectral Decomposition of a Cover Image in 2-D Plane[1]

For 2-D images, applying DWT separates the image into a lower resolution approximation image or band (LL), as well as horizontal (HL), vertical (LH), and diagonal (HH) detail components.

With the DWT, the significant part of the spatial domain image exist in the approximation band that consists of low frequency wavelet coefficients and the edge and texture details usually exist in high frequency wavelet coefficients bands such as HH, HL, and LH. The human eyes are not sensitive to small changes in the edges and textures of an image but to the small changes in the smooth parts [11].

C. HYBRID TRANSFORM DOMAIN TECHNIQUE

DCT and DWT are the most commonly used algorithms. The DCT has high energy compaction property and requires less computational resources [12]. The energy compaction property of an algorithm refers to the ability to concentrate most important information signal into as much as few low frequency components. On the other hand, DWT is a multi-resolution transform technique and variable compression can be easily achieved. The main disadvantages of DCT are introduction of false contouring effects and blocking artifacts at higher compression, and, that of DWT is requirement of large computational resources. So the idea of exploring the advantages of both algorithms generates the idea of combining the two techniques. Such combination of two algorithms is referred as hybrid algorithm.

Both DCT and DWT transform domain techniques are robust in nature and one technique outweighs another with respect to some parameter of importance. So, instead of using only one technique hybrid transform domain technique can be used [13] [14]. This allows for better imperceptibility and payload in comparison to using a single technique. The block diagram and the algorithm for image steganography using the concept of hybrid transform domain are as shown:

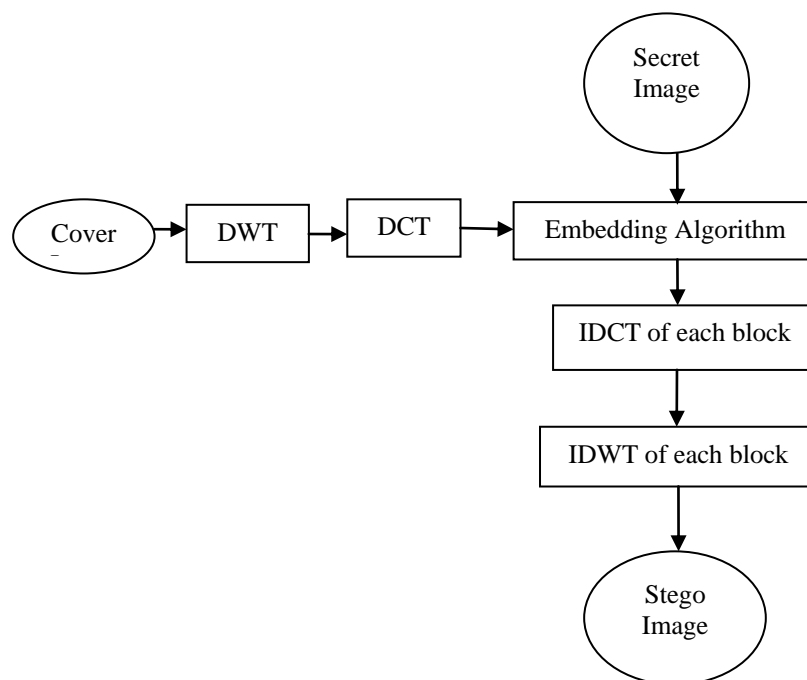


Figure. 3: Hybrid Transform Domain Technique for Hiding Secret Image in Cover Image[1]

D. PROPOSED TECHNIQUE

During the proposed embedding process, Firstly perform DWT on both the cover image and on the secret data, then apply DCT transform on both the images and then by using the fusion process we get fused image. Here the cover image is taken as hybrid image generated from previous technique. Apply IDWT and IDCT on fused image to get a stego image as shown as

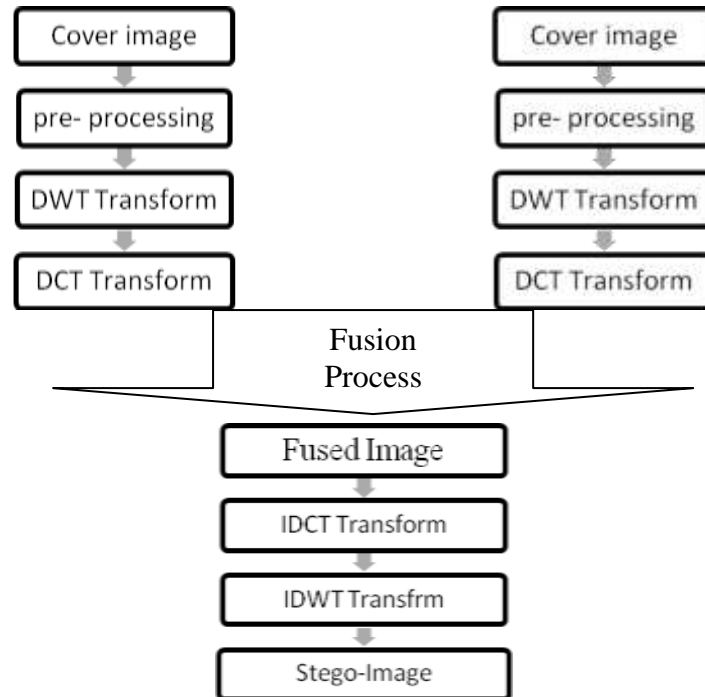


Figure4. Block Diagram of Embedding.

IV. PERFORMANCE EVALUATION MEASURES FOR IMAGE STEGANOGRAPHY METHODS

The quality of steganographic technique can be evaluated with the help of evaluation parameters like Mean Square Error, Peak to signal noise ratio, capacity etc[2].

A. Mean Square Error (MSE):

It is defined as the square of error between cover image and stego image. The distortion in the image can be measured using MSE and is calculated using this equation[2].

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

Where I is a noise free $m \times n$ monochrome image and K is its noisy approximation. Lower Mean square error is preferable, as it considered that lower the MSE better performance of steganography technique.

B. Signal to Noise Ratio

Signal-to-noise ratio is defined as the ratio of the power of a signal (meaningful information) and the power of background noise (unwanted signal):

$$SNR = \frac{P_{signal}}{P_{noise}}$$

where P is average power. Both signal and noise power must be measured at the same or equivalent points in a system, and within the same system bandwidth.

Signal to noise ratio (SNR) should be as large as possible Which means that the content of signal in the output is large and the noise is less

$$SNR = \frac{S_A}{S_B}$$

Here S_A, S_B are the mean intensity value of image and the background respectively.

C. Peak Signal to Noise Ratio (PSNR):

It is the measure of quality of the image by comparing the cover image with the stego image, i.e. it measures the percentage of the stego data to the image percentage.

$$\begin{aligned}
 PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\
 &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)
 \end{aligned}$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with B bits per sample, MAX_I is $2^B - 1$. For color images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Alternately, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space, e.g., YCbCr or HSL

Higher the peak signals to noise ratio, better the performance of steganography technique.

E. Capacity:

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp). Maximum embedding capacity is considered [2].

V. IMPLEMENTATION OF ALGORITHMS AND METODOLOGY

A. DISCRETE COSINE TRANSFORM

Another way of hiding data is by way of a direct cosine transformation (DCT). The DCT algorithm is one of the main components of the JPEG compression technique. This works as follows:

- First the image is split up into 8 x 8 squares.

- Next each of these squares is transformed via a DCT, which outputs a multi dimensional array of 63 coefficients.
- A quantizer rounds each of these coefficients, which essentially is the compression stage as this is where data is lost. Small unimportant coefficients are rounded to 0 while larger ones lose some of their precision.
- At this stage you should have an array of streamlined coefficients, which are further compressed via a Huffman encoding scheme or similar.
- Decompression is done via an inverse DCT.

Hiding via a DCT is useful as someone who just looks at the pixel values of the image would be unaware that anything is amiss. Also the hidden data can be distributed more evenly over the whole image in such a way as to make it more robust.

B. DISCRETE WAVELET TRANSFORM

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one.

Detailed procedures of a 2-D Haar-DWT are described as follows:

- At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).
- Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described above is called the first-order 2-D Haar-DWT.

C. PROPOSED TECHNIQUE

In Proposed Technique firstly, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described above is called the first-order 2-D Haar-DWT.



ISSN: 2348 9510

**International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 5, August 2015**

Then the watermark image is split up into 8×8 squares. Each of these squares is transformed via a DCT, which outputs a multidimensional array of 63 coefficients.

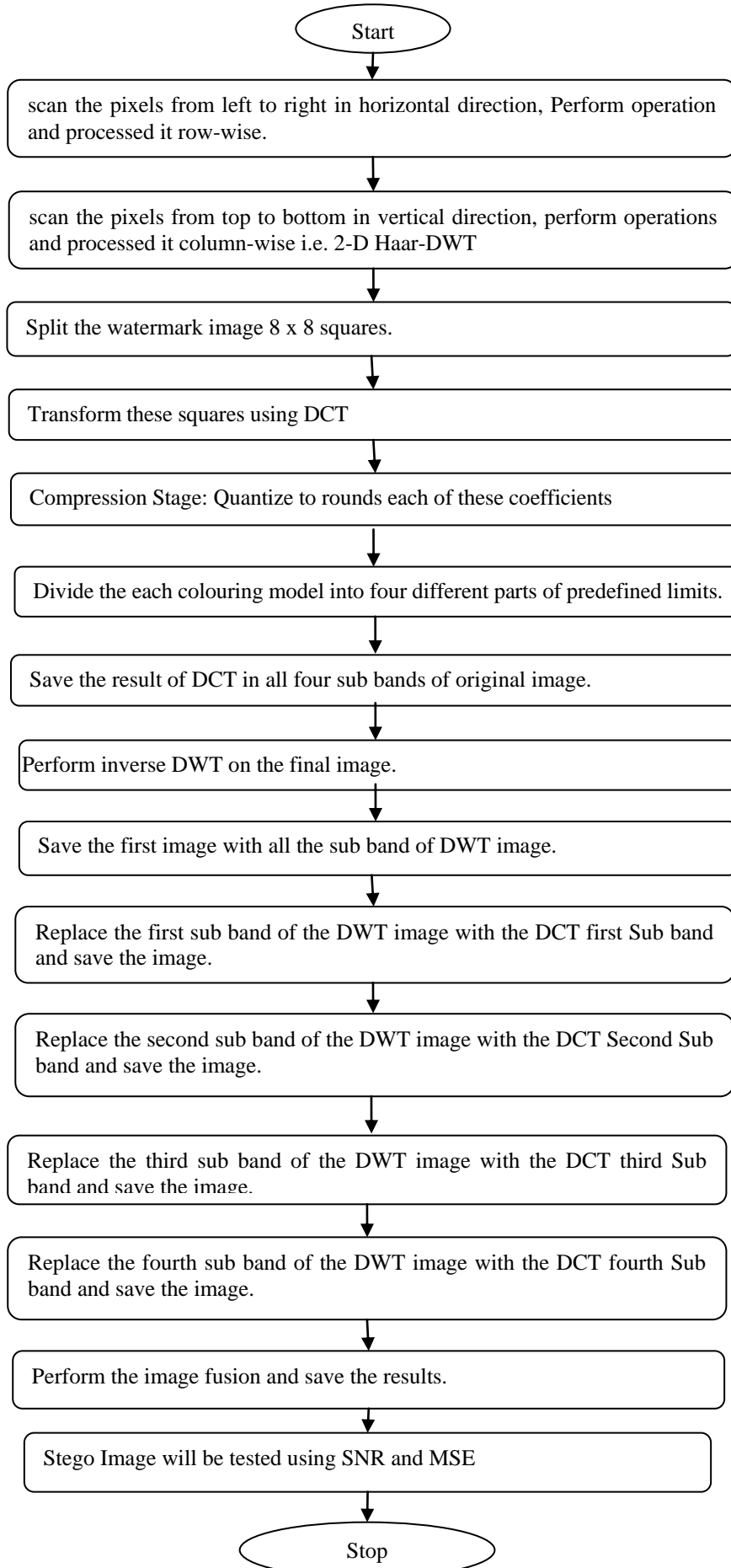


Figure5: Flow Chart of proposed technique

After that a quantizer rounds each of these coefficients, which essentially is the compression stage as this is where data is lost. Small unimportant coefficients are rounded to 0 while larger ones lose some of their precision.

At this stage you should have an array of streamlined coefficients, which are further compressed via a Huffman encoding scheme or similar and then Divide the each coloring model into four different parts of predefined limits and Save the result of DCT in all four subbands of original image. Again Perform inverse DWT on the final image and Save the first image with all the subband of DWT image. Then Replace the first subband of the DWT image with the DCT first Subband and save the image. Similarly Replace the second subband of the DWT image with the DCT Second Subband and save the image. Then Replace the third subband of the DWT image with the DCT third Subband and save the image. Similarly Replace the fourth subband of the DWT image with the DCT fourth Subband and save the image. At the end Perform the image fusion and save the results.

D. HYBRID TECHNIQUE

Hybrid Steganography is the combination of the two techniques that are DCT and DWT technique. It includes the idea of exploring the advantages of both algorithms. Detailed procedures of a hybrid technique is described as follows:

At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described above is called the first-order 2-D Haar-DWT.

After that split up the watermark image is into 8 x 8 squares.

Next each of these squares is transformed via a DCT, which outputs a multidimensional array of 63 coefficients.

Then a quantizer rounds each of these coefficients, which essentially is the compression stage as this is where data is lost. Small unimportant coefficients are rounded to 0 while larger ones lose some of their precision. At this stage you should have an array of streamlined coefficients, which are further compressed via a Huffman encoding scheme or similar. Then divide the each coloring model into four different parts of predefined limits. Save the result of DCT in all four subbands of original image. Perform inverse DWT on the final image.

V. RESULTS AND CONCLUSION

A. DCT RESULTS



Figure 6: Results of DCT Technique.

Mean Squared Error (MSE) = $2.3586e^4$

Signal to Noise Ratio (SNR) = -45.0407 (Negative)

B. DWT RESULTS



Figure 7: Results of DWT Technique.

Mean Squared Error (MSE) = $2.0683e^3$

Signal to Noise Ratio (SNR) = 12.8670

C. HYBRID RESULTS

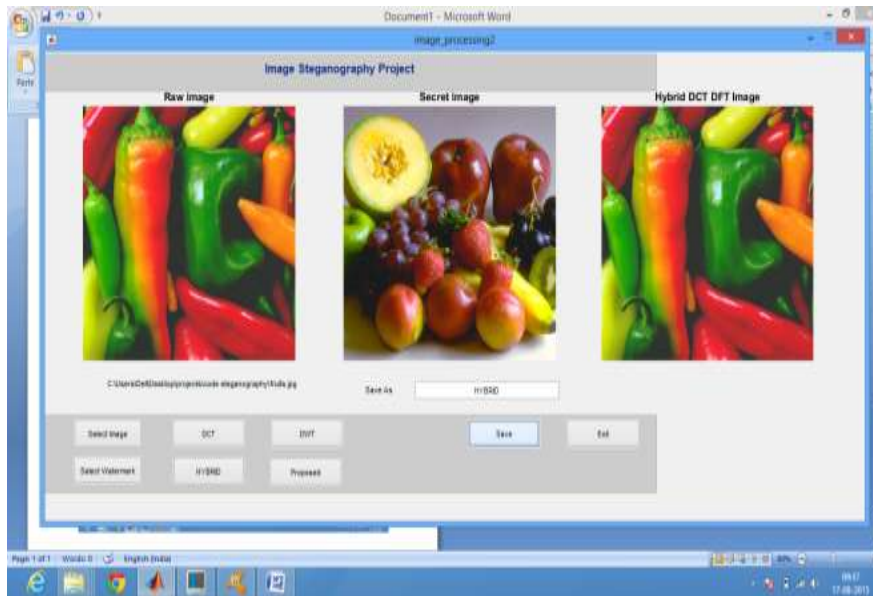


Figure 8: Results of HYBRID Technique.

Mean Squared Error (MSE) = 1.0568

Signal to Noise Ratio (SNR) = 43.5300

D. PROPOSED TECHNIQUE



Figure9: Results of PROPOSED Technique.

Mean Squared Error (MSE) = 0.1744

Signal to Noise Ratio (SNR) = 51.3527

VI. COMPARISON OF RESULTS

Technique Name	MSE	SNR
DCT	2.3586e ⁴	-45.0407
DWT	2.0683e ³	12.8670
HYBRID	1.0568	43.5300
PROPOSED	0.1744	51.3527

VII. CONCLUSION

The results show that proposed technique is better in terms of signal to noise ration and also mean square error is less. The Hybrid Technique also performs better than individual DCT and DWT techniques. Results of DWT show that DWT performs better than DCT technique.

In future the algorithm can be further improved in terms of different parameters like Normalized absolute error, Absolute Contrast Error and in Entropy. Also this algorithm can be further improved in terms of used paramters.

ACKNOWLEDGMENT

The author's wants to heartily thank their guide, Er. Chander Prabha- Associate. Prof. – CGCTC, Punjab technical university for their critique discussion, constant encouragement, valuable suggestion and timely guidance

REFERENCES

- [1]. Mukta Goel and Rohit Goel ,” Comparative Analysis of Wavelet Filters on Hybrid Transform Domain Image Steganography Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.
- [2]. Dr. Sudeep Thepade and Smita S. Chavan , “Appraise Of Multifarious Image Steganography Techniques ”, /International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March -April 2013, pp.1067-1174.
- [3]. Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar,” A Novel Technique for Image Steganography Based on DWT and Huffman Encoding” International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6).
- [4]. Usha B.A1, Dr.N.K Srinath, Dr. Ravikumar C N, Puttaraju, Manu and Vijaykumar , “Hybrid Fusion Methods in Image Steganography for Secured Data Transmission”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015.
- [5]. Veerdeep Kaur Maan and Harmanjot Singh Dhaliwal,” 32×32 Vector Quantization Based Colour Image Steganography”, International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463 Vol. 2 Issue 9, September-2013, pp: (28-33)
- [6]. K B Shiva Kumar , Sabyasachi Pattnaik and K B Raja ,” Hybrid Domain in LSB Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 19– No.7, April 2011.
- [7]. Kuang Tsan Lin, “Digital Image Hiding in an Image using n-graylevel Encoding”, The 1st International Conference on Information Science and Engineering (ICISE 2009), IEEE Computer Society, Washington, DC, USA, pp. 1720-1724, 2009.
- [8]. Giacomo Cancelli, Gwenael Doerr, Ingemar J. Cox, and Mauro Barni, “Detection of ± 1 LSB Steganography Based on The Amplitude of Histogram Local Extrema”, 15th IEEE International Conference on Image Processing (ICIP 2008), San Diego, CA, USA, pp. 1288-1291, 12-15 October 2008.
- [9]. Mehdi Hussain and Mureed Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology Vol. 54, May, 2013.

- [10]. Rakesh Dugad, Krishna Ratakonda, and Narendra Ahuja, "A New Wavelet-Based Scheme for Watermarking Images", International Conference on Image Processing, Chicago, USA, pp. 419-423, October 1998.
- [11]. Ahmed A. Abdelwahab, and Lobna A. Hassaan, "A Discrete Wavelet Transform based Technique for Image data Hiding", 25th National Radio Science Conference (NRSC 2008), Tanta University, Egypt, pp. 1-9, March 2008.
- [12]. Chin-Chen Chang, Chi-Lung Chiang, and Ju-Yuan Hsiao, "A DCT Domain System for Hiding Fractal Compressed Images", Proceedings of IEEE 19th Conference on Advanced Information Networking and Applications, Volume 2, pp. 83-86, March 2005.
- [13]. Khalid Negrat, Raoof Smko, and Abdelsalam Almarimi, "Variable Length Encoding in Multiple Frequency Domain Steganography", 2010 2nd IEEE International Conference on Software Technology and Engineering (ICSTE), pp. 305-309, 2010.
- [14]. Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi, "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation", Third 2008 IEEE International Conference on Convergence and Hybrid Information Technology, Iran, pp. 539-544, 2008.