Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 2, February 2013, pg.91 – 101

RESEARCH ARTICLE

A COMPARATIVE STUDY OF IMAGE STEGANOGRAPHY IN WAVELET DOMAIN

Sushil Kumar[1], S.K.Muttoo[2]

[1]Department of Mathematics, Rajdhani College, University of Delhi, Delhi India

azadsk2000@yahoo.co.in

[2]Department of Computer Science, University of Delhi, Delhi, India

skmuttoo@cs.du.ac.in

Abstract*— In this paper we present a comparative study of four different image steganography algorithms based on orthogonal Haar Wavelet Transform and biorthogonal CDF9/7 Transform. One can divide the steganography techniques into two categories: Reversible techniques and Irreversible techniques. There are applications such as medical image system and law enforcement where it is desirable to recover the original cover image with no distortion. In this paper we shall discuss the four different embedding techniques: three are irreversible, namely, Modified (or Randomized) LSB method, LSB varying mode method and Fusion method and one is reversible, known as distortionless (or reversible or lossless) thresholding technique. The four basic requirements of Steganography are Imperceptibility, Security, Embedding payload and robustness to common statistical attacks and image processing operations. For measuring the robustness against common statistical attacks we present the histogram analysis between the original and stego-image. We apply self-synchronization variable length code, namely T-codes in place of Huffman codes for source encoding to provide security and better compression of original message. The Modified LSB method is simple, high payload, fast and most popular steganography embedding technique but fails to be robust against common channel noise such as Gaussian, Salt-n-peppers and others. The LSB Varying mode technique based on Haar transform is proposed by chen and lin [6]. The authors have shown that their method provides acceptable PSNR value, though one require extra space for key-matrix along with stego-image in the transmission. We modify this technique using T-code as source encoder and compare the results with cdf9/7 transform. The Wavelet-based Fusion method is proposed by Tolba and Ghonemy [17]. This is a high capacity cover-screw algorithm with the results of high invisibility. From the experimental results we observe that Fusion method is best for high capacity, high invisibility and robustness to common attacks in compare to other techniques and the reversible thresholding technique gives better imperceptibility in Haar domain than cdf9/7 domain.

Indexed Terms: - Image Steganography, Haar wavelet, cdf9/7, PSNR.

I. INTRODUCTION

Data Hiding or Steganography is the science of secret communication which has received much attention from the scientific community recently. Conferences dedicated to steganography have become more popular and its presence in high impact journals has also increased [2, 5, 8, 13, 19]. The four main objectives of steganography are: Imperceptibility (or undetectibility), Security, embedding payload, and Robustness (required against common attacks). However, steganography can protect data by hiding it in a cover object but using it alone may not guarantee total protection. Thus, the use of encryption in steganography can lead to 'security in depth'. To protect the confidential data from unauthorized access, an advanced encryption standard (AES) has been suggested by the researchers [11]. Many different carrier file formats can be used, but steganography in digital images has attracted the researchers as one can find high degree of redundancy present in a digital representation of an image (despite compression) and in many scenarios they are 'innocent' data types to eavesdroppers [9].

There are three basic issues in the design of steganographic techniques [19]:
1. First is the choice of accurate cover and to find a strategy that modify the cover in an imperceptible way.
2. Deciding the maximal embedding capacity for each pixel is an open issue. For increasing the embedding capacity, two or more bits in each pixel can be used to embed messages. But the risk of making the embedded statistically detectable increases as also the image quality degrades. So, deciding the appropriate number of bits embedded in each pixel to minimize statistical variation and maintaining image quality becomes an important issue of image steganography.
3. Third issue is of designing an efficient algorithm for embedding and extracting the information.

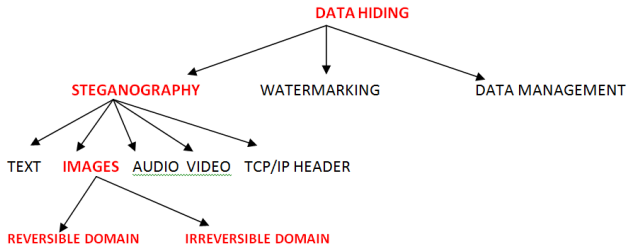


Fig. 1 Classification of Data Hiding

We can broadly classify the image steganographic methods into two categories: Reversible and Irreversible. Reversible methods are those that allow embedding data inside an image and later not only the hiddent data can be retrieved but the exact copy of original image can also be found. In the irreversible methods it is not desirable to recover the original image after the hidden data is retrieved.

In this paper we present a comparative study of the image steganography algorithms based on Wavelet transform using four different techniques: MLSB, LSB Varying mode, Fusion technique and Thresholding technique. Modified (or randomized) LSB technique is simple, fast, high capacity method, however, not found to be robust against common statistical attacks or image processing operations. LSB varying mode method is a high capacity image steganography proposed by chen and Lin [6] in the Haar Wavelet transform that provides better PSNR with respectable security. This method has weakness that it needs extra information, key matrix, to be sent alongwith the stego-image to the receiver. Wavelet Fusion method is another high embedding steganography technique for color image proposed by Tolba and Ghonemy [17]. Their method provides the high invisibility as well as the large hiding capacity. The reversible thresholding technique was introduced by G. Huang et al [20] which is a reversible steganography technique required for the applications such as medical, astronomical,and military iamge due to legal reasons [1]. We present the comparative study of these methods based on four basic characterisitics of data hiding and their requirements given as follows:

IMPERCEPTIBILITY	SECURITY	CAPACITY	ROBUSTNESS
High	High	High	High

In the next subsequent section 2, we review the discrete wavelet transforms and their families. In section 3, we summarize the different image steganographic techniques used in this paper. In section 4, we give the embedding and extraction process of proposed algorithms. Experimental results are described in section 5. Conclusion and Future scope is given in section 6.

I. DISCRETE WAVELET TRANSFORM

The DWT is a multi-resolution technique that can analyze different frequencies by different resolutions. The basis function used for decomposition of signals are of two types, called mother wavelet (or simply wavelet) $\psi(t)$ and scaling function $\varphi(t)$. Any finite energy signal f(t) can be decomposed in terms of wavelets and scaling function as follows [22]:

$$f(t) = \sum_{n\varepsilon(-\infty,\infty)} c(n)\ \varphi(t-n) + \sum_{j\varepsilon(0,\infty)} \sum_{n\varepsilon(-\infty,\infty)} d(j,n)\ 2^{j/2}\ \psi(2^j t - n)$$

where scaling coefficients, c(n) and wavelet coefficients, d(n), are computed as follows:

$$c(n) = \int_{t\varepsilon(-\infty,\infty)} f(t)\ \varphi(t-n)\ dt\ , \text{ and } \quad d(j,n) = 2^{j/2} \int_{t\varepsilon(-\infty,\infty)} f(t)\ \psi(2^j t - n)\ dt$$

where 'j' is scale factor.

In 2D wavelet transforms the scaling and wavelet functions are two variable functions φ(x, y) and ψ(x, y). In DWT, an image is filtered into four sub bands at each resolution and the sub band which has lowest frequency sub band is further subdivided through an iterative process to provide the multi resolution representation.
DWT of 2D function f(x, y) of size M x N is given by

$$W\varphi(j_0,m,n) = 1/\sqrt{MN} \sum_{x\varepsilon[0,M-1]} \sum_{y\varepsilon[0,N-1]} f(x,y)\ \varphi_{j0,m,n}(x,y)$$

$$W\varphi^{i}(j,m,n) = 1/\sqrt{MN} \sum_{x\varepsilon[0,M-1]} \sum_{y\varepsilon[0,N-1]} f(x,y)\ \varphi^{i}_{j,m,n}(x,y), \qquad i\varepsilon\{H,V,D\}$$

The image is decomposed into four sub band: Wφ (j, m, n) denotes the low frequency approximation, LL and WψH, WψD, WψV denotes the high frequency sub bands in horizontal (H), vertical (V) and diagonal (V) orientation, denoted by LH, HL and HH respectively.

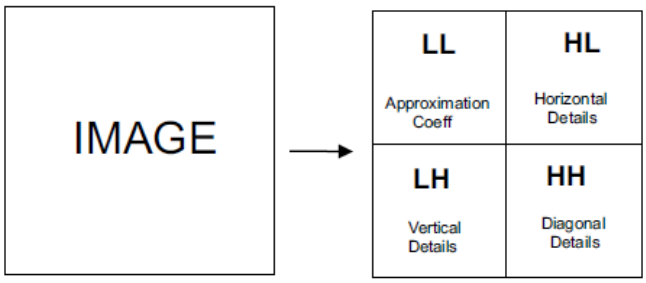


Fig. 2 Output of 1-level 2-D decomposition

The wavelet research community has presented several wavelet families such as Haar, Daubechies, Symlets, Coiflets, Morlet,Mexican Hat, Meyer, cdf2/2, cdf9/7 etc. Each of them have different shapes and lengths of mother wavelet leading to different wavelet filters with different properties. The JPEG 2000 compression standard uses the cdf5/3 wavelet, also known by cdf(2, 2) wavelet, for lossless compression and cdf9/7 wavelet for lossy compression. Cohen-Daubechies-Feauveau (CDF) wavelets are a family of biorthogonal wavelets introduced by Ingrid Daubechies. The standard orthogonal wavelet transform has some shortcomings that make it less than ideal for use in a coding system. One shortcoming is that the total number of input coefficients, *N*, does not equal the total number of wavelet coefficients, *L*, using the maximally decimated wavelet transform. In general *L* is greater than *N* and the wavelet transform results in "coefficient expansion." The lack of linear phase filters in orthogonal wavelets led to research in extending wavelet analysis to more general forms, which would allow for linear phase filters. The research resulted in a more general form of wavelets known as "biorthogonal wavelets" [4, 9]. The orthogonal and biorthogonal wavelets transforms are analogous to orthogonal and nonsingular matrix transforms, respectively. Both the orthogonal and nonsingular matrix transforms are invertible, but only the orthogonal matrix transform is energy preserving. The main advantage in using the biorthogonal wavelet transform is that it permits the use of a much broader class of filters, and this class includes includes symmetric filters. Since, the biorhtogonal wavelet cdf9/7 are linear phase biorthogonal filter coefficients which are "close" to being orthogonal, we propose it for the image steganography in this paper.

II. EMBEDDING TECHNIQUES

In the literature, many techniques about data hiding have been proposed [2, 5, 8,19].

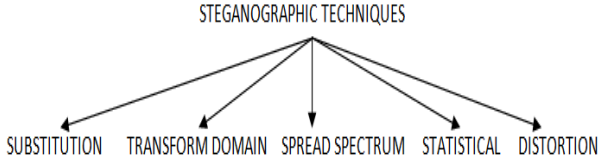


Fig. 3 Techniques of Steganography

We review in the subsequent sub-sections the four embedding techniques proposed in this paper

3.1 LSB (Substitution) method

The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image. The basic idea of LSB embedding is to embed the message bit at the rightmost bits of pixel value so that the embedding method does not affect the original pixel value greatly. The formula for the embedding is as follows:

$$x' = x - x \bmod 2^k + b$$

where k is the number of LSBs to be substituted.

The extraction of message from the high frequency coefficients is given as: $b = x \bmod 2^k$

There are two types of LSB insertion methods, fixed-sized and variable-sized. The former embeds the same number of message bits in each pixel of the cover-image. On embedding fixed four random bits in the four LSBs of each pixel, some false contours can occur. The unwanted artifacts may arise suspicion and defeat the purpose of steganography. To treat this problem, either fewer bits must be used for message embedding or a variable-sized method needs to be applied. For the variable-sized embedding method, the number of LSBs in each pixel used for message embedding depends on the contrast and luminance characteristics. Thus the most important requirement is maintaining the image fidelity while adapting these local characteristics to estimate the maximum embedding capacity.

3.2 Wavelet Fusion Method

The Wavelet fusion method is the High bit rate data hiding. In this method the fusion process takes place between the DWT of the secret data and the DWT of the cover image. Since the ordinary wavelet filters have floating point coefficients, a normalization operation is applied on the cover image so that the wavelet coefficients are converted in the range of 0.0 and 1.0. The fusion technique then merges the wavelet decomposition of both the cover image and the secret message into a single fused result using the following equation:

$$f^*(x, y) = f(x, y) + \alpha * g(x_m , y_m)$$

where f^* is the modified DWT coefficient, f is the normalised wavelet coefficient, g is the normalized message coefficient, and alpha (α) is the embedding strength which ranges form 0.0 to 1.0. To overcome the problem of overflow or underflow, the cover's normalized pixels are adjusted before the embedding process takes place so that the reconstructed pixels do not go out of range. The secret message is converted to binary bits and if the bit is 1 the +alpha is added to the cover image wavelet coefficient and if it is 0 the –alpha is added to the wavelet coefficient of the cover image. The embedding is applied on each color plane separately. M. Fahmy Tolba and Al-said Ghonemy [17] have proposed this method where the secret data is another color image.

3.3 LSB varying mode in Wavelet Domain

Po-Yueh Chen and Hung-Ju Lin[6] have proposed LSB based image steganography techniques in wavelet domain. The embedding procedure is classified into two modes: Varying mode and Fix mode. In fix code, there is a specific range for required capacity whereas in varying mode the range of capacity is not specific and differs. In the Varying mode case, first every 2 consecutive bits of binary string are combined to form a decimal value from 0 to 3. Every 2 consecutive values in the resulted decimal sequence are further combined to perform subtraction operation and form a differential sequence ranging from -3 to 3. The four possine absolute values (0,1,2 and 3) are embedded in sub-band HH by substituting 2 LSBs of coefficients of HH with 00, 01, 10, and 11 respectively. The Subtration pairs, embedding is done in LH and HL sub-bands. The remaining bits of message are embedded at those unused LSBs in LH and then HL bit by bit. Since after embedding and taking the inverse DWT, some pixels in stego-image are not integers, we record the 4 possible non-integer situations (0.0, 0.25, 0.5, and 0.75) in the key-matrix, K. This matrix is required to perfectly reconstruct the secret message bits in the extracting procedure. Chen and Lin have observed after the implementation of other algorithms on different images that the PSNR is a satisfactory value even when the highest capacity case is applied and Key-matrix provides an additional layer of security.

3.4 ReversibleThresholding method

Threshold embedding method for the lossless data hiding is given by Xuan et al. [20]. We predefine a threshold value. To embed data into a high frequency coefficient of sub-band HH, LH or HL, the absolute value of the coefficient is compared with T. If the absolute value is less than the threshold, the coefficient is doubles and

message bit is added to the LSB. No message bit is embedded otherwise, however, the coefficients are modified as follows:

$$x' = \begin{cases} 2*x + b & \text{if } |x| < T \\ x + T & \text{if } x \geq T \\ x - (T-1) & \text{if } x \leq -T \end{cases}$$

where T is the threshold value, b is the message bit, x is the high frequency coefficient and x' is the corresponding modified frequency coefficients.
To recover the original image, each high frequency coefficient can be restored to its original value by applying the following formula:

$$x = \begin{cases} x'/b & \text{if } -2T < |x'| < 2T \\ x' - T & \text{if } x' \geq 2T \\ x' + T - 1 & \text{if } x' \leq -2T + 1 \end{cases}$$

III. **PROPOSED ALGORITHMS**

The proposed image steganography algorithms embeds data into the first level high frequency subbands of the cover image obtained after applying the Haar/cdf9/7 transform. Preprocessing is performed prior to data embedding to ensure that no overflow/underflow takes place. The stego-image carrying hidden message is obtained after taking the inverse wavelet transform.

4.1 Performance Measure

The performance of the proposed techniques given in the consequent sections are evaluated according to the widely used metric, PSNR.

4.1.1. Imperceptibility

This aspect measures how much difference (distortion) was caused by data hiding in the original cover, where the higher the stego-image quality, the more invisible the hidden message. We can judge the stego-image quality by using Peak Signal to Noise Ratio (PSNR). The PSNR for an image of size NxN is given as follows:

$PSNR = 10 \log_{10} (255^2 / MSE)$**, (dB)**
where $MSE=(1/N*N) \sum\sum (xij - x'ij)^2$,

The *MSE* is the Mean Square Error, *P(x, y)* stands for the image pixel value in the cover image and *P'(x, y)* is for the pixel value at position *(x,* in the image after inserting secret message. A high value of PSNR means better image quality (less distortion), it is recorded that in grayscale images that the human visual system (HVS) can not detect any distortions in stego-images having PSNR that goes beyond 36 dB.

Yang, Lin and Hu [21] have recently proposed a simple reversible data hiding scheme on the IWT. They have embedded data by adjusting the coefficient of IWT so that the distortion is minimum. They have shown that their method is robust to image processing operations.

The embedding and extraction algorithms of the steganography used in this paper are summarized below:

Algo1.1: MLSB Embedding

……..
Input: Message,M, cover image, I, an 8-bit grayscale image, of size 256 X 256 and random-key, k.
Output: stego-image, I'

Step1. First, obtain the secret data,M', with encoded key, K, by applying best T-codes as a source encoder to the given input message,M.
Step2: Apply pre-processing to I, to prevent possible "overflow" during embedding, i.e., replacing the grayscale values 0 to 1 and 255 to 254 of cover image.
Step3. Decompose the cover image, I, into 4 subbands, viz., HH, HL, LH and LL, by applying Haar wavelet and CDF9/7 wavelet.
Step4. The frequency coefficients of middle and high sub-bands, HH, HL and LH obtained through CDF9/7 are converted into integer values using threshold T=0.9.

Step5. Permute the coefficients of sub-bands, HL, LH and HH randomly using a random-key, k, and obtain new sub-bands LH', HL' and HH'.
Step6. Embed the secret message in the middle and high frequency bands, LH', HL' and HH' using the modified LSB method.
Step7. Apply the inverse of step4 to adjust the coefficients values and then obtain the stego sub-bands LH, HL and HH respectively, applying inverse operation of random permutation.
Steg8. Form the embedded image, E, of size 256 X 256 by merging the stego sub-bands with low sub-band LL
Step9. Obtain stego-image, I' by taking the inverse haar transform/ inverse CDF9/7 tranform of E
……..

Algo1.1 : MLSB Extraction

Input: stego-image,I', stego-key,k, encoded key, K
Output: original message, M

Step 1. Apply Haar/ CDF97 transform to the stego image to obtain 4 sub-bands, LL, HL, LH and LL
Step2. Permute the coefficients of sub-bands HL, LH and HH using the stego- key, k to obtain the sub-bands HL', LH' and HH'.
Step2. Extract secret data, M', from these middle and high frequency sub-bands by inverse modified LSB technique.
Step3. Recover the original image, M, by applying T-decoding using the encoding key, K.
……

Algo 1.2: LSB Varying Mode Embedding

Input: 8-bit gray-level cover image, I, Message,M , random-key, k, encoding key, K
Output: Stego-image,I'

Step1.First, obtain the secret data,M', with encoded key, K, by applying best T-codes as a source encoder to the given input message,M.
Step2. Make the dimensions of cover image, I, of power of 2, if not, by required padding.
Step3. Obtain the 4 sub-bands LL, HL,LH and HH by applying Haar/CDF97 transform on C.
Step4. The frequency coefficients of middle and high sub-bands, HH, HL and LH obtained through CDF9/7 are converted into integer values using threshold T=0.9.
Step5. Permute the coefficients of sub-bands, HL, LH and HH randomly using a random-key, k, and obtain new sub-bands LH', HL' and HH'.
Step6. For the first MxN secret bits, combine every 2 consecutive bits of secret message to form decimal value ranging from 0 to 3 and then subtract every 2 consecutive values to form a sequence ranging from –3 to 3.
Step7. Embed the 4 possible absolute values in HH' using 2 LSBs. The information of their different subtraction pairs is embedded in the corresponding positions of HL' and LH'.
Step8. The remaining secret bits are embedded in the unused LSBs of LH' and HL', bit by bit.
Step9. Apply the inverse of the random permutation to obtain stego sub-bands LH, HL and HH respectively.
Steg10. Form the embedded image, E, of size 256 X 256 by merging the stego sub-bands with low sub-band LL
Step11. Take the inverse Haar/CDF97 transform of modified coefficient matrix, E. Let the resulting stego image be E'. Let I' be the rounded version of E' to integer matrix.
Step12. Record in the Key matrix, key, the 4 possible non-integer situations while rounding pixel values of E.
……..

Algo1.2: LSB varyiung Mode Extraction

Input: stego-image, I', random-key, k, encoding-key,K and key-maatrix, key
Output: original message, M

Step1. Using the matrix, key modify the coefficients of stego- image, I'.
Step2. Obtain the 4 sub-bands, LL', HL', LH', HH' from stego-image,I' by the application of Haar/CDf97 transform.
Step3. Permute the coefficients of sub-bands HL', LH' and HH' using the random- key, k to obtain the sub- bands HL, LH and HH.
Step4. Extract the secret message from the high frequency coefficients of HH,HL and LH .

Step5. Decode the secret message using the encoding-key, K and T-decoding algorithm to obtain the original message, M.

Algo: Fusion Embedding

Input: Cover image,I, original text,M, alpha, num, random-key,k
Output: the Stego-image, I'.

Step1. Normalize the cover image,I. i.e., the pixel values made to lie between 0.0 and 1.0.
Step2. Apply preprocessing on cover image: choose 'alpha' (preferably between 0 and 0.1) and reconstruct pixels to lie in the range [alpha, 1 – alpha]. This will ensure that pixels from the fused coefficients (during embedding) would not go out of range and hence the secret message will be recovered correctly.
Step3. Apply 2D Haar transform/CDF97 transform on each color plane separately.
Step4. Encode the original message,M, using the T-codes. The resulting secret message is a bit-stream of 0 and 1, denoted by (m_1 m_2…. m_n), where n is the embedding message length and it generate an encoding key, K.
Step5. Generate pseudorandom permutation, using a random-key,k, of the size equal to the length of cover image.
Step6. Enter the number of times the message to be embedded, num.
for i = 1 to num do
6.1Select wavelet coefficient of the transformed image randomly, say f(j, k)
6.2 Embed the secret message bit, m (i), into the transformed image in the following way:

```
if  m(i) = '1'
  f (j,k) = f (j,k) + alpha;
else
  f (j,k) = f (j,k) – alpha;
```

Step7. Apply the inverse 2D Haar transform on each color plane separately.
Step8. Denormalize the image, and obtain the stego-image, I'

.....

Algo1.3 : Fusion Extraction

…….

Input: Stego-image,I', random-key, k, encoding-key, K
Output: Original message, M.

Step1. Apply 2D Haar transform/CDF97 on each color plane of the stego-image,I'
Step2. Enter num, number of times message being embedded
Step3. Initialize the hiddenmessage to zero.
for j= 1 to num do
3.1 Select the embedded coefficients, i, using the PRNG based on the random-key, k, same as used in the embedding procedure.
3.2 Extract the embedded value of alpha by subtracting the original cover image from the stego image in the wavelet domain
3.3 Obtain the secret message bit, m(i) as follows:

```
If alpha >0
    m(i) = '1'
else
     m(i)='0';
```

3.4 hiddenmessage += m(i);
*end; /*for(j)*/*
Step4. hiddenmessage /=num;
Step5. Decode the hiddenmessage using T-decoding algorrrithm using the encoded- key, K.

……..

Algo 1.4: Thresholding Embedding

Input: Cover Image, I, message, M, random-key,k
Output: Stego-image,I', encoded-key,K

Step 1: Obtain the secret message by encoding the message, M with T-encoding. This also generates an encoding-key, K.
Step 2: Read the cover image,I, into a two dimensional decimal array to handle the file data more easily.
Step 3:
Histogram modification is done to prevent overflow/underflow that occurs when the changed values
In integer wavelet coefficients produce stego-image pixel values to exceed 255 or to be smaller than 0.

This problem was found to be caused by the values near 255 or 0. The problem is solved by mapping the lowest 15 grayscale levels to the value of 15 and the highest 240 grayscale levels to the value 240.

Step 4: (Integer wavelet Transform): transform the cover image to the transform domain using 2D Haar integer wavelet transform resulting LL, LH, HL and HH.

Step 5: Calculate hiding capacity (number of bits to be used in hiding message bits) of each coefficient of middle and high sub-bands, using the appropriate threshold, Thresh, to enhance the stego-image quality (usually Thresh= 35).

Step6. The frequency coefficients of middle and high sub-bands, HH, HL and LH obtained through CDF9/7 are converted into integer values using threshold T=0.9.

Step7. Permute the coefficients of sub-bands, HL, LH and HH randomly using a random-key, k, and obtain new sub-bands LH', HL' and HH'.

Step 8: Embed the secret message into the corresponding randomly chosen coefficients.
(Random selection of coefficients provides more security where the sequence of the message is only known to both sender and receiver by using a previously agreed upon secret key.)

Step9. Apply the inverse of the random permutation to obtain stego sub-bands LH, HL and HH respectively.

Steg10. Form the modified image, E, of size 256 X 256 by merging the stego sub-bands with low sub-band LL.

Step11. Finally, obtain stego-image,I', by taking the inverse Haar/CDF97 transform of the modified image, E.

……

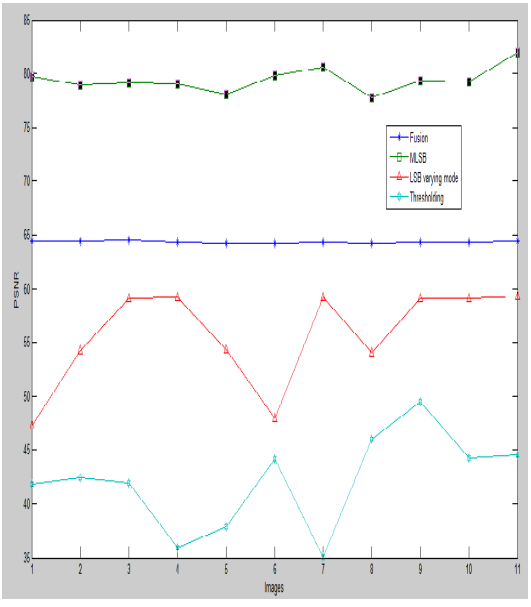
In all the above proposed algorithms we obtain the secret message to be embedded from the original message by applying T-codes. T-codes are proposed by Titchner [16] and Ulrich [18] has described its importance in his thesis as a self-synchronizing variable length codes that can synchronize the errors after one to three words at decoding stage. It has been shown that T-codes are better option than Huffman for compression and image processing applications. Sushil Kumar and S.K.Muttoo have proposed image steganography using T-codes in Wavelet domains and they have found that their proposed methods provides better imperceptibility in terms of PSNR [14-15].

IV. **EXPERIMENTAL RESULTS**

To evaluate the performance of the proposed data hiding algorithm, we have used 256 x256 gray scale and color images . Simulations were done using MATLAB 8.0. In table 1, we give the results of PSNR obtained from the proposed algorithms in the Haar domain.

Table 1: PSNR values for Haar wavelet based method with embedding capacity= 2000 ASCII characters (*1000 ASCII characters).

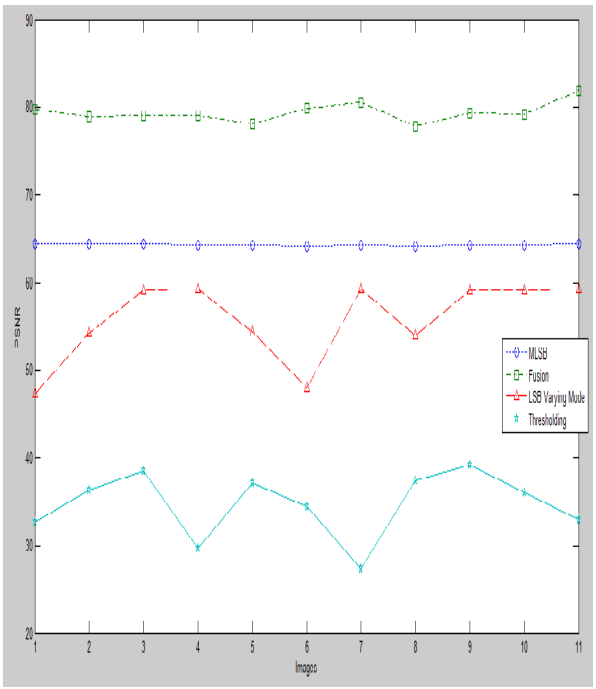
Image	MLSB	Fusion	Varying Mode LSB	Thresholding
c3.jpg	64.401391	79.762532	47.286145	41.857999
Tulips.jpg	64.409907	78.972952	54.206086	42.432005
New7.tif	64.477624	79.111836	59.08492	41.936554
New8.tif	64.352814	79.079916	59.216496	35.878400
New11.tif	64.239363	78.071977	54.346299	37.876080
New12.tif	64.222879	79.857524	47.971216	44.171170
Baboo.bmp	64.325852	80.587144	59.213094	35.022358
C2.bmp	64.168396	77.821579	54.045355	45.953009
Zoneplate.png	64.252756	-	54.419268	30.309481*
Tooth1.jpg	64.349138	79.303201	59.074202	49.470903
PEPPERS.PNG	64.289423	79.226603	59.126392	44.262010
C1.png	64.394475	81.913874	59.273883	44.564382

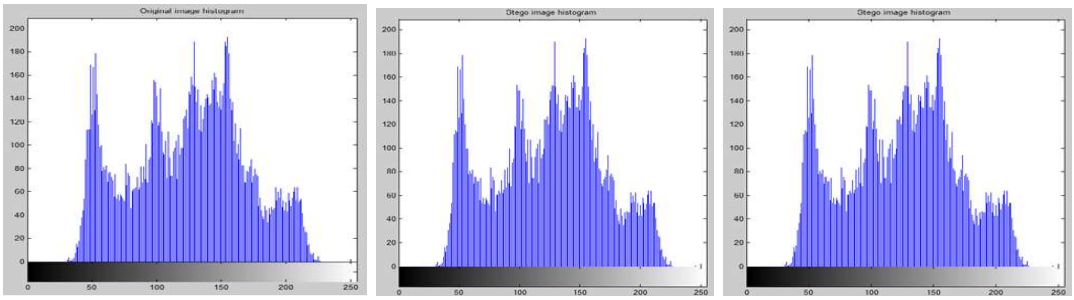


In table 1, we show the comparison of PSNR values for different image formats for the proposed algorithms with the embedding capacity = 2000 ASCII characters. We observe that fusion method shows best high invisibility than the other methods. The thresholding method which is a reversible method shows the PSNR values in the acceptable range of PSNR (30 db-50 db). It is observed that PSNR values decreases as we increase the embedding capacity.
In table 2, we give the results of PSNR obtained from the proposed algorithms in the bi-orthogonal cdf9/7 domain. In table 3, we summarize these techniques based on Haar Wavelet. We observe that fusion method is good in terms of imperceptibility, have high embedding capacity and robustness. The Thresholding method is a reversible steganography which provides acceptable imperceptibility, embedding capacity varies with threshold. The LSB Varying Mode method provides high invisibility with satisfactory amount of embedding capacity and finally, the Modified LSB is a fast, high embedding but not a robust method.
The Histogram of lena.jpg image and the corresponding histograms of stego-images obtained through proposed algorithms are given at the end show that Haar based techniques have satisfactory results than the cdf 9/7

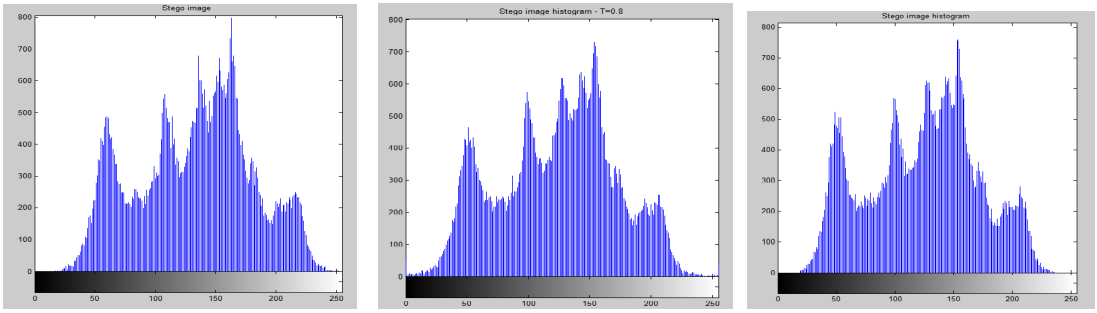
Table 2: PSNR values for cdf9/7 wavelet based method with embedding capacity= 2000 bytes.

Image	MLSB	Fusion	LSB Varying Mode	Thresholding
c3.jpg	49.4976	72.87786	51.88085	27.74672
Tulips.jpg	49.619299	72.49752	51.89486	24.823396
New7.tif	48.620927	72.28791	53.06515	25.993797
New8.tif	49.816201	70.25964	53.0167	21.746396
New11.tif	49.466484	71.37421	52.67455	24.131382
New12.tif	48.711405	72.84008	52.48861	26.774769
Baboo.bmp	49.868782	70.24871	53.10975	21.856399
C2.bmp	49.466034	73.40234	51.43187	30.791012
Zoneplate.png	50.578165	-	53.28726	8.671013
Tooth1.jpg	48.442376	74.56165	52.93161	33.829992
PEPPERS.PNG	48.619296	73.68977	52.67304	28.842123
C1.png	48.748451	74.72542	53.05607	31.545956





(a) (b) (c)



(d) (e) (f)

Fig. 6 Histograms: (a) Lena.jpg (b) stego-image (MLSB Haar based) (c) stego-image (MLSB cdf9/7 based) , (d) stego-image (thresolding- haar based), (e) stego-image (thresholding-cdf9/7 based), (f) stego-image (LSB Varying Mode- Haar based

V. CONCLUSIONS

We have presented a comparative study of image steganography in the wavelet domain using four different embedding techniques. The embedding techniques used have their own applications and importance in terms of what characteristics of image steganography are desired. We have performed experiments in Matlab 8.0 and comparison of proposed algorithms is done through the imperceptibility measure, PSNR It is found that Haar wavelet(i.e., IWT) is better option than bi-orthogonal cdf9/7 for the reversible thresholding technique as well as for others. The best choice for image steganography in wavelet domain is based on Fusion method for color images. For gray image, LSB Varying mode method may be considered a better option as it provides a respectable capacity and satisfactory security along with good imperceptibility.

Table 3: Comparison of MLSB, Varying mode, fusion and thresholding embedding methods using Haar wavelet transform

Method	Impercep -tibilty (PSNR)	Robustness (against Gaussian/ Salt-n-Peppers attack)	Embedding Capacity	Security Against Detectibilty
MLSB	High	Poor	High	Poor
Varying Mode	Satisfactor y	Poor	Respectable	Satisfactory
Fusion	High	Good	High	Satisfactory
Thresholdi ng	Satisfactor y	Poor	Depends on the selection of threshold	Average

REFERENCES

[1] M. Awrengjeb, *An Overview of reversible Data Hiding*, ICCIT 2003, Jahangir nagar University, Banladesh, Dec. 19-21, pp. 75-79, 2003

[2] W. Bender, D. Gruhl, N. Morimoto and A. Lu, *Techniques for data hiding*, IBM Systems Journal, Vol. 35, Nos. 3 &4, pp. 313-336, 1996.

[3] C. Cachin,*An information-theoretic model for steganography*, 2nd Inter-national Workshop Information Hiding, vol. LNCS 1525, pp. 306{318, 1998.

[4] A. R. Calderbank, 1. Daubechies, W. Sweldens and B. Yeo.,*Wavelet transforms that map integers to integers*, Applied and Computational Harmonic Analysis, vol.5, noJ, pp.332-369, 1998.

[5] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, *A Comparative Analysis of Steganographic Tools*, Proceedings of the Seventh IT&T Conference. Dublin, Ireland .

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

[7] Ali K. Hmood, Hamid A.Jalab, Z.M.Kasirun, B.B. Zaidan and A.A. Zaidan, *On the capacity and security of steganography approaches: An overview*, Journal of Applied Sciences, 10(16), pp. 1825-1833, 2010

[8] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, *Image Steganography: Concepts and Practice*, WSPC/Lecture Notes Series, April 22, 1:49, 2004

[9] M. K. Mandal, S. Panchanathan and T. Aboulnasr, *Choice of Wavelets for Image Compression*, Lecture Notes in Computer Science Vol. 1133, pp. 239-249

[10] S.K.MUTTOO and SUSHIL KUMAR, *Robust Source coding Steganographic technique using Wavelet Transforms*, International Journal of Information Technology(IJIT), Vol. 1, No. 2, July – December, New Delhi, 2009, Website: www.bvicam.ac.in

[11] S.K.MUTTOO and SUSHIL KUMAR**,** *A mulltilayred secure, robust and high capacity image steganographic algorithm*, World of Computer Science and Information Technology Journal (*WCSIT*), ISSN 2221-0741, vol. XXX, No. XXX, 2011

[12] S.K.MUTTOO and SUSHIL KUMAR , *Secure Image Steganography based on Slantlet Transform*, Proceeding of the International Conference on Methods and Models in Computer Science, ICM2CS 2009, Dec. 14-15, pp.1-7, 2009.

[13] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, *Information hiding—a survey*, *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[14] Sushil Kumar, S.K. Mutttoo, *Data Hiding techniques based on Wavelet-like Transform and Complex Wavelet Transform*, International Symposium on Intelligence Information Processing and Trusted Computing, IPTC 2010, Huanggang, China, Oct. 28-29, 2010

[15] Sushil Kumar and S.K. Muttoo, *Distortionless Data Hiding based on Slantlet Transform*, Proceeding of the first Intenational conference on Multimedia Information Networking & Security (Mines 2009) , Wuhan, China, Nov. 17- 20, Vol. 1, pp. 48-52, IEEE Computer Society Press, 2009

[16] Titchener, M.R. (1996), Generalised T-codes: extended construction algorithm for self- synchronization codes, IEE Proc. Commun., Vol. 143, No.3, pp. 122-128.

[17] M.F. Tolba, M.Al-Said Ghonemy,I.A.-H. Taha,; A.S. Khalifa, *High Capacity Image Steganography using Wavelet-Based Fusion*, Computers and Communications, 2004, Proceedings. ISCC2004. Ninth International Symposium, Volume 1, Issue, 28 June-1 July 2004, Vol.1, 430-435.

[18] Ulrich G. (1998), *Robust Source Coding with Generalised T-codes*, a thesis submitted in the University of Auckland.

[19] N. Wu and M. Hwang, *Data Hiding: Current Status and Key Issues*, International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan.2007.

[20] G. Xuan, J. Zhu, Y. Q. Shi, Z. Ni, and W. Su., *Distortionless data hiding based on integer wavelet transform*, IEE Electronic Letters, 38(25): 1646--1648, Dec. 2002.

[21] Ching-Yu Yang, Chih-Hung Lin and Wu-Chih Hu, *Reversible Data Hiding for High-Quality Images Based on Integer Wavelet Transform*, Journal of Information Hiding and Multimedia Signal Processing , Volume **3**, Number **2**, April 2012

[22] B. Chinnaro, M. Madhavilatha,*Improved image denoising algorithm using dual tree complex wavelet transform*, International journal of computer applications, vol. 44, no. 20, April 2012

