A Comparative Study of Transform Based on Secure Image Steganography

Sushil Kumar[1]

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

* Corresponding author. Tel.: 09711234705; email: skazad@rajdhani.du.ac.in; azadsk2000@yahoo.co.in

Manuscript submitted July 22, 2014; accepted December 16 , 2014.
doi: 10.17706/ijcce.2015.v4.389

Abstract: In this paper, a comparative study of steganography in the transform domain for the grayscale images is presented. The embedding technique used is based on the modified LSB Varying mode method. The main goal of Steganography includes hiding information or information file into another information file in an undetectable way both perceptually and statistically. To provide an additional layer of security, Cryptography and source encoding methods are used in conjunction with Steganography. In addition to proposing transform based Steganography, we propose to use Self-Synchronizing variable length codes, called T-codes as source encoder to obtain the secret data from the original embedding data. We demonstrate through the experiments that Contourlet performs better than the CDF9/7 and Slantlet transforms in terms of PSNR, SSIM and KLDiv. Comparing Haar Transform with Contourlet it is found that though Haar Wavelet based LSB varying mode method provides better PSNR, SSIM and KLDiv values than Contourlet, the Contourlet lowers detectability and provides more embedding capacity.

Key words: DWT, SLT, CTT, PSNR, SSIM, KLDiv.

1. Introduction

The Contourlet transform (CTT), introduced by Do and Vetterli [1], overcomes the difficulty in exploring the geometry in digital images due to the discrete nature of the image data. It possesses the important properties of directionality and anisotropy which wavelet do not possesses. It can represent a smooth contour with fewer coefficients compared with wavelets. The Fig. 1 illustrates the successive refinement by the two systems near a smooth contour, which is shown as a thick curve separating two smooth regions.

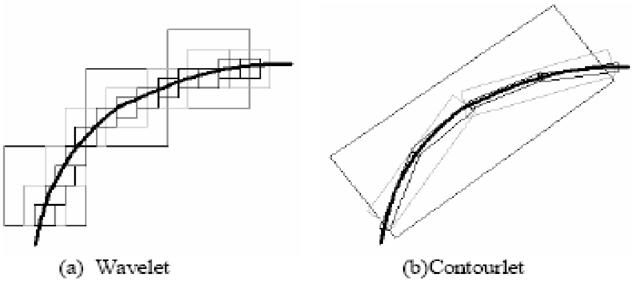


Fig. 1. Wavelet versus Contoulet [1].

The CTT is based on a double filter bank structure by combining the Laplacian Pyramid (LP) with a directional filter bank (DFB) (Fig. 2). The Laplacian pyramid (LP) is used to decompose an image into a number of radial subbands and the directional filter bank (DFB) decompose each LP details subband into a number of directional sub-bands. The required number of directions can be specified by the user.

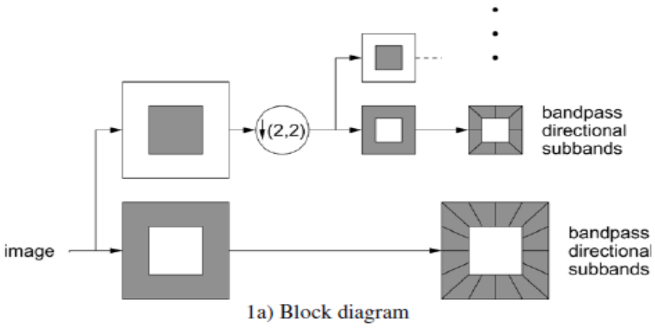


Fig. 2. LP and DFB filter banks [1].

Contourlet has the following properties:

1) Multiresolution, i.e., representing images from a coarse level to fine-resolution level
2) Localization, i.e., basis elements can be localized in both the spatial and the frequency domains
3) Critical sampling, i.e., representation form a basis, or a frame with small redundancy
4) Directionality, i.e., representation of basis elements oriented at variety of directions and
5) Anisotropy, i.e., capturing of smooth contours in images.

The first three properties are also provided by separable wavelets. It is known that the wavelet transform divides the high frequency only into three sub-bands at each Level, whereas it is possible to divide the high frequency into more sub-bands in the contourlet transform. This fact provides the variety of sub-bands for embedding the secret data. The Fig. 3(a) is the level 1 decomposition of image 'aeroplane.tif'. Original image is decompose into 5 contourlet sub-bands, and each sub-band contains part of the original image frequency content. Fig. 3(b) shows the contour basis of level 4.

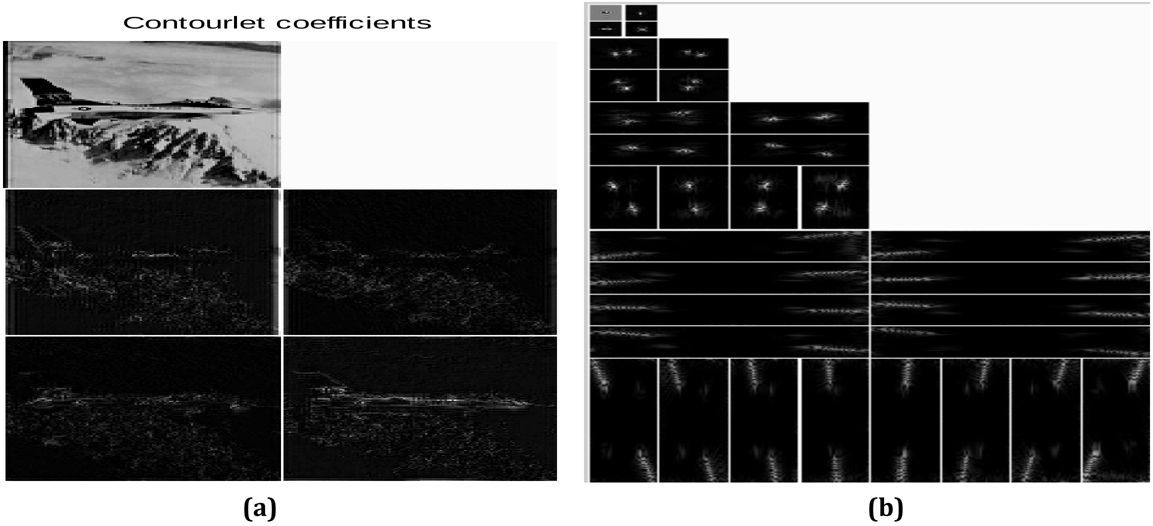


Fig. 3. (a) Contourlet decomposition of level 1 of image: new3.tif; (b) Contour basis of level 4.

Moreover, in spite of the sub-bands in wavelet transform that are correlated, the sub-bands in the Contourlet transform are linearly independent and hence uncorrelated . This could lead to more security in steganography, since there is lower possibility of detecting. The Contourlet transform is more suitable for data hiding applications as Contourlet gives more edges. Moreover more data can be hidden in the high frequency regions without perceptibility distorting the original image.

Massebi and Moghaddam [2] have proposed a new image hiding method based on the Contourlet transform based on storing information in high frequency subbands of Contourlet transform. They have shown that their algorithm has a higher robustness against to common steganalysis approaches. Furthermore, through experimental results their approach show robustness with respect to Gaussian noise and other attacks such as JPEG compression.

Sajedi and Jamzad [3] proposed the embedding of secret data in the block of Contourlet coefficients by the rule that if the coefficient value does not match with the secret bit value, increase its negative value to become positive to represent 1 or decrease its positive value to become negative to represent a 0 bit. Their experimental results show that their method can resist the state-of-the-art steganalysis with embedding capacity of about 0.02 bits per pixel for forced cover images and 0.06 bits per pixel for exact cover selection scheme.

Navas *et al.* [4] have proosed a novel blind data hiding algorithm for telemedicine applications using Non-subsampled Contourlet Transform (NSCT) and have shown that it performs better in terms of minimum BER, higher WPSNR and large embedding capacity.

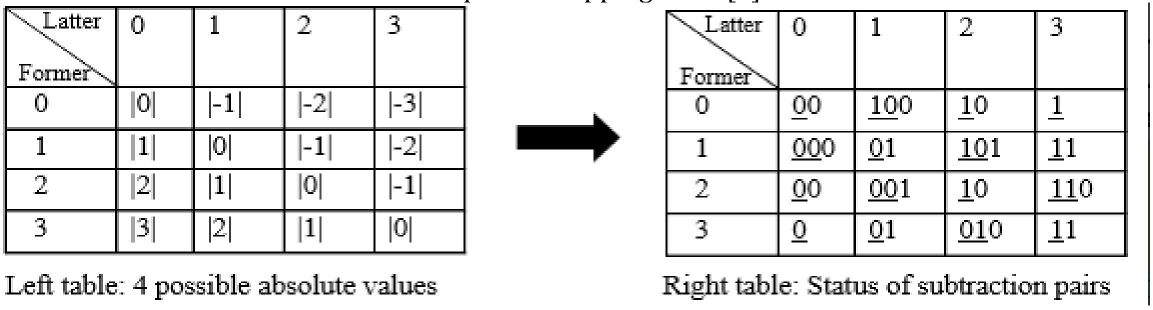
Manoharan [5] proposed the use of T-codes [6] to encode messages prior to embedding the messages in the cover media. The extracted messages need to he decoded before use. According to him, this system will be more tolerant to media transformations that result in some bit losses or bit inversions in the hidden message.

Kumar and Muttoo [7]-[11] have studied the non-reversible image steganography based on fixed LSB using Slantlet transform [12], Contourlet transform and Complex wavelet transforms alongwith T-codes for the compression of message before embedding. They have also presented reversible image steganography based on thresholding technique using T-codes [13]-[14]. They have found that T-codes provides better results than the Huffman codes for steganography. In this paper we investigate the role of Contourlet transform in place of wavelet transform in the image steganography using variable LSB method (proposed by Chen and Lin [15]) and present a modified high rate and secure image steganographic technique which also fulfills the main characteristics of steganography such as imperceptibility and undetectability. The wavelet based image steganography using variable LSB method is reviewed in the next section.

2. Review of Wavelet Based Image Steganography

Chen & Lin [15] 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, shown in Table 1.

Table 1. Sequence Mapping Table [1]



Latter / Former	0	1	2	3
0	|0|	|-1|	|-2|	|-3|
1	|1|	|0|	|-1|	|-2|
2	|2|	|1|	|0|	|-1|
3	|3|	|2|	|1|	|0|

Left table: 4 possible absolute values

Latter / Former	0	1	2	3
0	00	100	10	1
1	000	01	101	11
2	00	001	10	110
3	0	01	010	11

Right table: Status of subtraction pairs

The four possible 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 Subtraction 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.

However, due to the LSB substitutions, some pixels in E are not integers ranging from 0 to 255. As shown in Fig. 4, we employ a so-called "Key matrix"- K to record the 4 possible non-integer situations (0.0, 0.25, 0.5 and 0.75). The rounded pixel values of E are used to show the stego-image. In order to perfectly reconstruct the secret message bits, K is necessary in the extracting procedure.

$$E = \begin{bmatrix} 173\underline{.75} \\ 174\underline{.0} \\ 174\underline{.25} \\ 174\underline{.5} \\ 174\underline{.75} \\ 175\underline{.0} \end{bmatrix} \Rightarrow K = \begin{bmatrix} \underline{11} \\ \underline{00} \\ \underline{01} \\ \underline{10} \\ \underline{11} \\ \underline{00} \end{bmatrix}$$

Fig. 4. Generation of the Key matrix.

The algorithm proposed by Chin and Lin [15] requires to restore the key-matrix which increases the data need to transmit or restore. To reduce the extra data in the stego-images, authors have suggested that we can compress the size of "Key matrix" as far as possible. As a result, the file sizes of the original image and that of the corresponding stego-image will not differ too much. Also according to them, Key-matrix provides an additional layer of security.

3. Proposed Algorithm

In this section we present the proposed image steganographic algorithm based on LSB varying mode method using Contourlet Transform and compare it with other existing algorithms using other transforms such as Haar transform, CDF9/7 transform and Slantlet transform.

The embedding and extraction algorithms are summarized as follows:

Algo 3.1: Embedding

Input: message, cover-image,

Output: stego-image, key

1. Make the dimensions of cover-image of power of 2, if not, by required padding.
2. Apply normalization process or called pre-processing to avoid underflow and overflow while embedding data in image.
3. Apply 1-level of contourlet transform to cover image (256 x256) and obtain the one low-level sub-band LL (of size, 128 x128) and 4 high-level sub-bands (each of size, 128 x 128) .
4. Apply the soft thresholding to the frequency coefficients of high subbands, using the threshold, T, based on the method, called Normal Shrink, to enable larger space for hiding secret data with minimal error.
5. Encode the original message using T-codes to obtain secret message. Let the key generated is, key1
6. 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.

7. Permute the coefficients of high sub-bands randomly using a random-key, k and obtain the new high subbands, say H1, H2, H3 and H4.
8. Round the coefficients of subbands H1, H2, H3 and H4, for obtaining 8-bit quantization.
9. Embed the 4 possible absolute values in H1 using 2 LSBs. The information of their different subtraction pairs is embedded in the corresponding positions of H2 and H3 (see Chin & Li[1] for more details).
10. The remaining secret bits are embedded in the unused LSBs of H3 and H2, bit by bit in H4 (see Chin & Li[1] for more details).
11. Apply the inverse of the random permutation to stego sub-bands H1, H2, H3 and H4, respectively.
12. Form the embedded image, E, of size 256 X 256 by merging the stego sub-bands with low sub-band LL
13. Take the inverse Contourlet transform of embedded image, E. Let the resulting stego image be E'. Let I' be the rounded version of E' to integer matrix.
14. The possible rounded non-integer situations are stored in a matrix, key, K, which is required to reconstruct the secret message perfectly.

Algo 3.2: Extraction

Input: stego-image, *I', key1, key*

Output: original message

1. Using the matrix, key modify the coefficients of stego- image, I'.
2. Obtain the 4 sub-bands H1, H2, H3, and H4 from stego-image, I', by the application of Contourlet transform.
3. Permute the coefficients of sub-bands H1, H2, H3 and H4 using the random- key, k to obtain the randomized sub- bands H1', H2', H3' and H4', respectively.
4. Extract the secret message from the high frequency subbands, H1', H2', H3' and H4', in a similar way as described in steps 9and 10 of embedding,
5. Decode the secret message using the key, key1 and decoding algorithm to obtain the original message.

In Step 4 of Algo 3.1, the selection of T is based on the adaptive threshold estimation method for image denoising, known as Normal Shrink .The parameters required for estimating this threshold depend on subband data. The threshold is computed by $\beta\sigma^2 /\sigma_y$, where σ and σy are the standard deviation of the noised and the subband data of noisy image respectively. β is the scale parameter, which also depends upon the subband size and number of decompositions. Their experimental results show that Normal Shrink removes noise significantly and outperforms other denoising threshold methods. The soft thresholding is preferred over the hard thresholding as the latter is discontinuous and yields abrupt artifacts in the recovered images especially when the noise energy is significant. The soft thresholding is:

$$\begin{aligned} \rho_T(x) &= x - T && \text{if } (x > T); \\ &= x + T && \text{if } (x < -T); \text{ and} \\ &= 0 && \text{if } \mathrm{abs}(x) \leq T. \end{aligned}$$

We note that the Step 2 of normalization is necessary because the inverse transform has components out of the valid range. Further, Step 8 of rounding the coefficients convert the real coefficients into integers, that is necessary for 8-bit quantization. However, when normalization and rounding are applied, the error is increased in a considerable form, which has undesirable impact on the image reconstruction.

The proposed algorithm provides two layer of security- one at the time of compression of the original message using T-codes (self-synchronizing VLC [9-15]) and another at embedding stage, where randomization is performed on the coefficients of high subbands of Contourlet decomposition before embedding the secret message.

4. Experimental Results

We have implemented the proposed algorithm with Matlab 7.8 version on different digital image formats. The Imperceptiblity measure used is PSNR. For structural similarity we have computed SSIM and for the security of the method, according to Cachin, we have obtained the result based on KLDiv. The results based on PSNR, MSSIM and KLDiv are summarized in the Tables 2 to 4 for some of test images (shown in Fig. 10) of size 256 x 256. For comparison purpose we have shown the results for the same capacity= 6000 bytes, however, CTT has more embedding capacity than DWT as explained in the introduction.

Table 2. Comparison of PSNR Between Different Transform Based Steganography Using Varying Mode LSB With Embedding Capacity=6000 Bytes

Image	Haar	CDF9/7	SLT	CTT
c3.jpg	54.203939	47.286145	47.150056	49.031461
tulips.jpg	54.206086	47.503210	47.554904	48.937997
tooth1.jpg	54.458066	48.265404	48.208363	49.018983
new7.tif	54.330525	48.244674	48.154326	48.925461
new8.tif	54.337436	48.309994	48.215047	48.941553
new11.tif	54.346299	48.006234	48.039070	48.994194
new12.tif	54.329420	47.971216	47.955977	49.196095
c2.bmp	54.045355	47.029246	46.974672	49.225948
baboo.bmp	54.373554	48.302680	48.252845	48.929476
c1.png	54.358515	48.226955	48.114862	48.965929
zoneplate.png	54.419268	48.433912	48.366995	49.052598
peppers.png	54.301617	47.828892	47.892471	49.063055

Table 3. Comparison of SSIM Between Different Transform Based Steganography Using Varying Mode LSB with Embedding Capacity=6000 Bytes

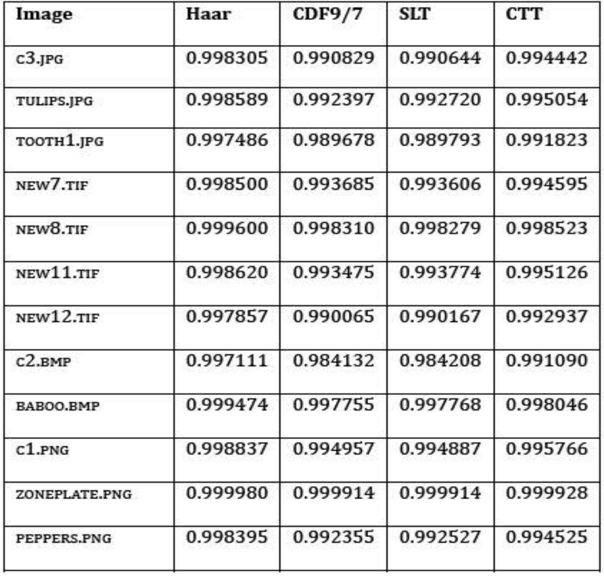


Image	Haar	CDF9/7	SLT	CTT
c3.JPG	0.998305	0.990829	0.990644	0.994442
TULIPS.JPG	0.998589	0.992397	0.992720	0.995054
TOOTH1.JPG	0.997486	0.989678	0.989793	0.991823
NEW7.TIF	0.998500	0.993685	0.993606	0.994595
NEW8.TIF	0.999600	0.998310	0.998279	0.998523
NEW11.TIF	0.998620	0.993475	0.993774	0.995126
NEW12.TIF	0.997857	0.990065	0.990167	0.992937
c2.BMP	0.997111	0.984132	0.984208	0.991090
BABOO.BMP	0.999474	0.997755	0.997768	0.998046
c1.PNG	0.998837	0.994957	0.994887	0.995766
ZONEPLATE.PNG	0.999980	0.999914	0.999914	0.999928
PEPPERS.PNG	0.998395	0.992355	0.992527	0.994525

Table 4. Comparison of Kldiv Between Different Transform Based Steganography Using Varying Mode LSB With Embedding Capacity=6000 Bytes

Image	Haar	CDF9/7	SLT	CTT
c3.jpg	0.000020	0.000103	0.000120	0.000074
tulips.jpg	0.000021	0.000106	0.000677	0.000245
new11.tif	0.000119	0.000229	0.000338	0.000321
c2.bmp	0.000091	0.000467	0.000466	0.000358
baboo.bmp	0.000026	0.000111	0.000144	0.000129
c1.png	0.000015	0.000061	0.000078	0.000056
peppers.png	0.000037	0.000159	0.000188	0.000132

From Fig. 5 and Fig. 6, we observe that CTT outperforms than the CDf9/7 and SLT in terms of PSNR and SSIM whereas Haar wavelelt still outperforms to other transforms.

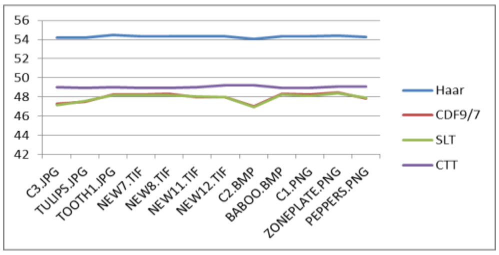
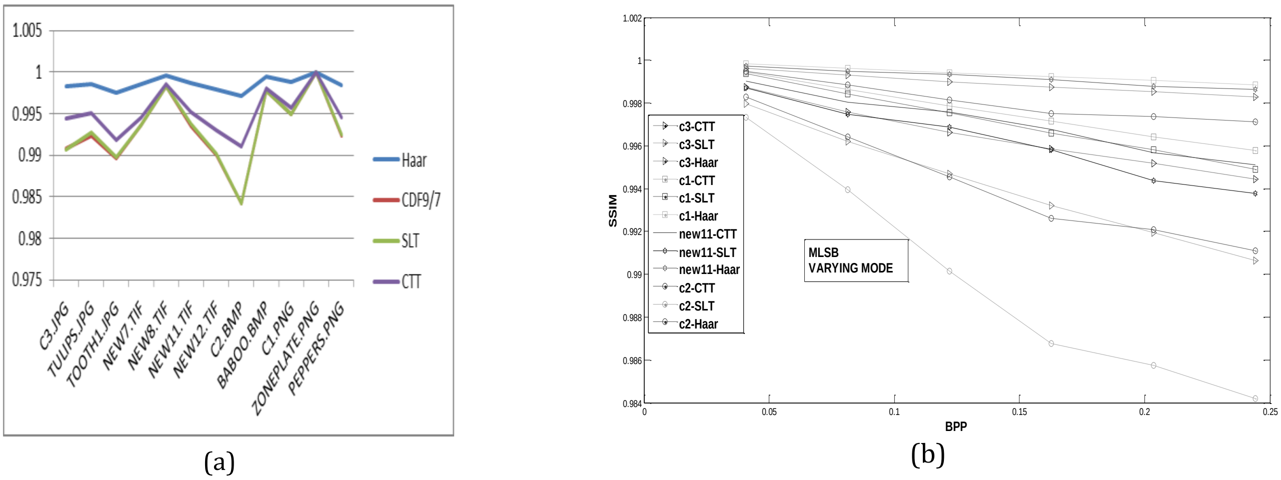


Fig. 5. Comparasion between Haar, CDF9/7, SLT and CTT based Varying Mode LSB techniques in terms of PSNR.

From Fig. 6, it can be seen that CTT shows better provable security than the SLT, whereas Haar is still showing slightly better candidate of provable security than CTT. In Fig. 6(b), it is observed that irrespective of image format, Haar based modified Varying LSB scheme is of rank 1 (in the range [0.997, 0.998] showing best results of structural similarity (SSIM), CTT are at rank 2 and SLT are at rank 3. Moreover as BPP increases the Haar based scheme is almost constant (consistent) whereas CTT shows slow downward results from 0.998 to 0.991and SLT is showing sharp fall from 0.998 to 0.984 as compare to other transforms, though all the transforms have acceptable structural similarity.



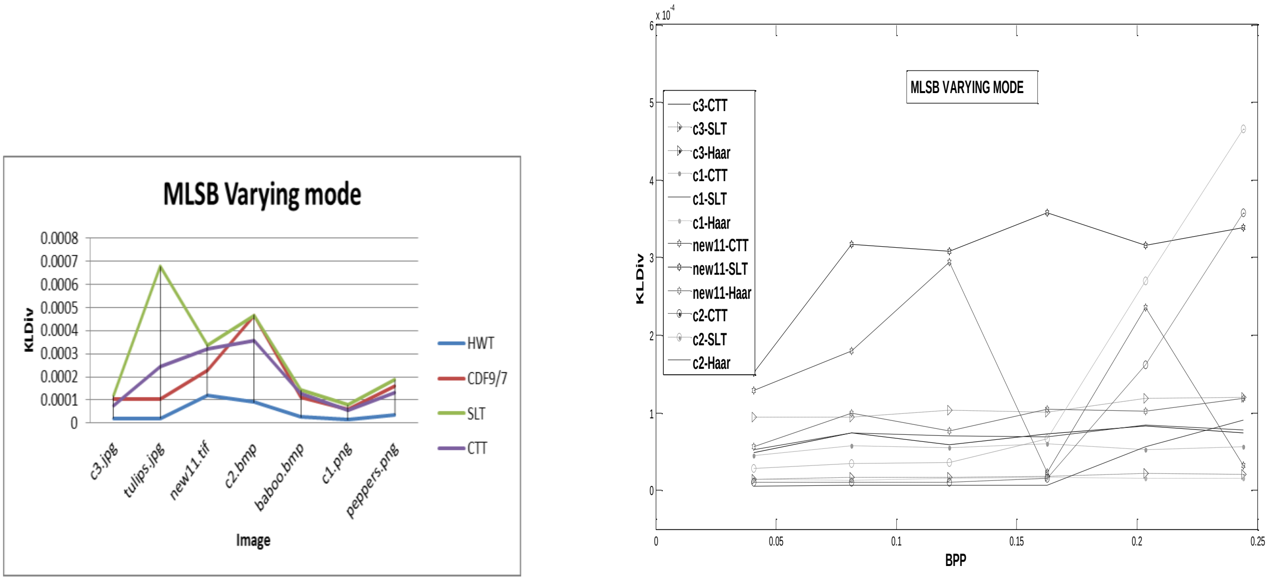
(a)

(b)

Fig. 6. Comparasion between Haar, CDF9/7, SLT and CTT based Varying Mode LSB techniques in terms of SSIM (a) for different image formats, and (b) with respect of BPP.

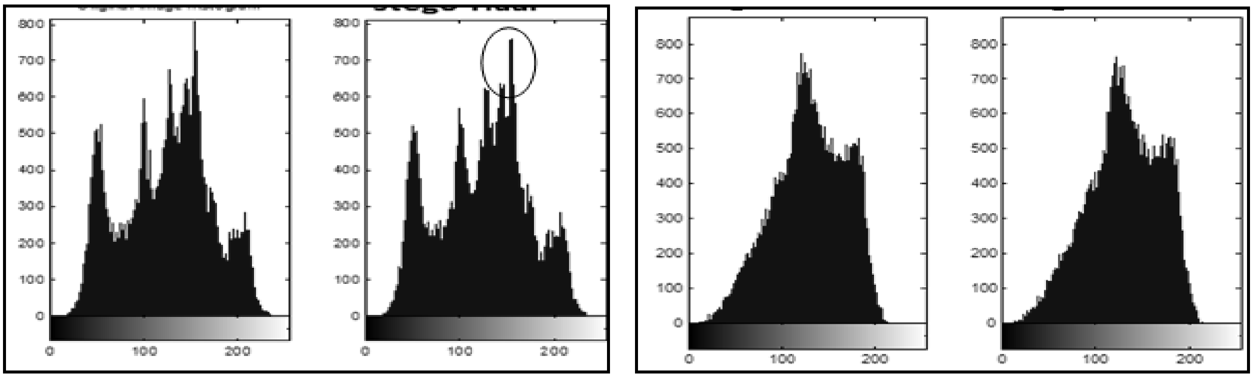
From Fig. 7, it can be seen that CTT shows better provable security than the SLT, whereas Haar is still showing slightly better candidate of provable security than CTT. It is further seen in Fig. 7 (b) that Haar and CTT, both shows consistent results for provable security (KLDiv) as BPP increases whereas SLT based algorithm shows varying results.

However it is known that even if KLDiv value is near zero, it is still not predictable that the method is secure from statistical attacks. For this we also analyze histograms of the stego-images obtained. Through the Fig. 8 and Fig. 9, where histograms of the original and stego-images are shown based on the Haar and CTT based Varying LSB schemes, it is observed that the image formats .bmp, .jpg, and .png can resist the statistical attacks whereas the .tif format images fails to such attacks.



(a) (b)

Fig. 7. Comparasion between Haar, SLT and CTT based Varying Mode LSB techniques in terms of KLDiv (a) for different image formats, and (b) with respect of BPP.

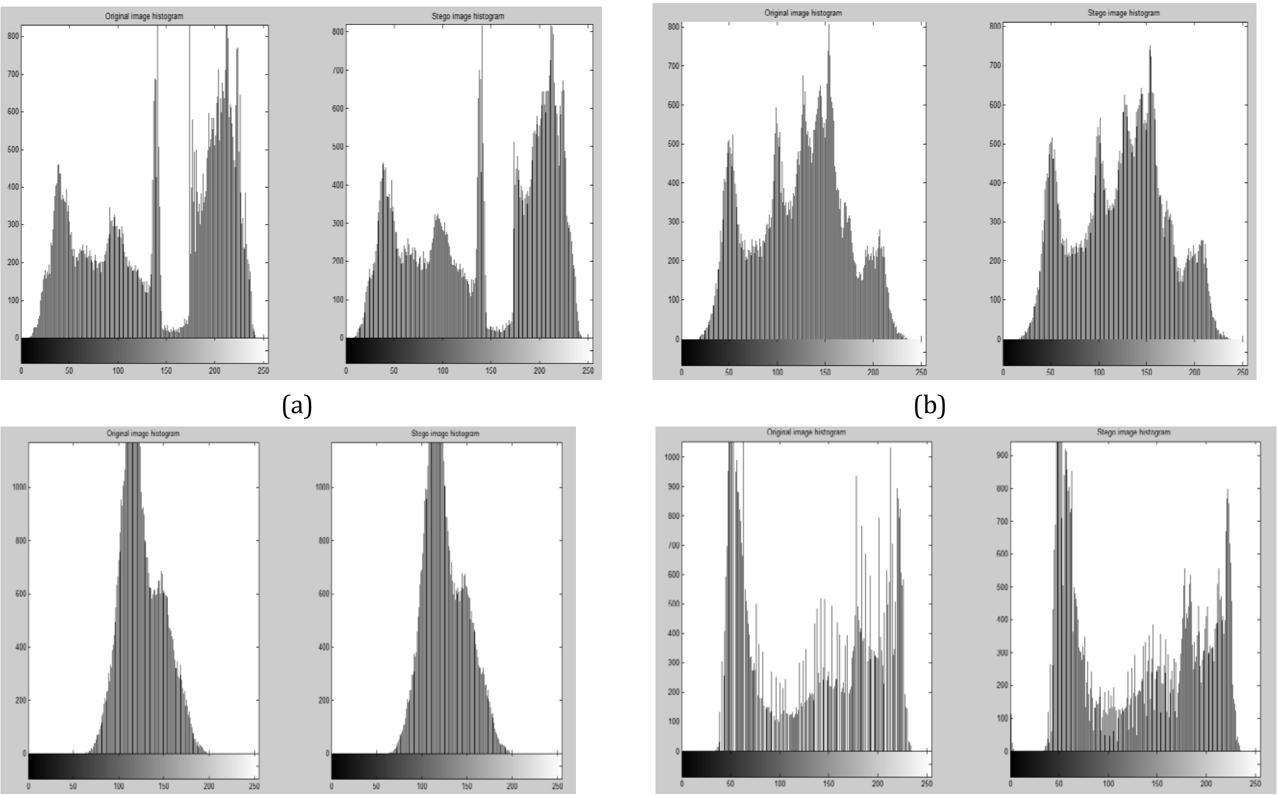


(a) (b)

Fig. 8. Original and corresponding stego-images with histograms for Haar based varying mode LSB method (a) Lena.jpg, (b) Baboo.bmp.

5. Conclusion

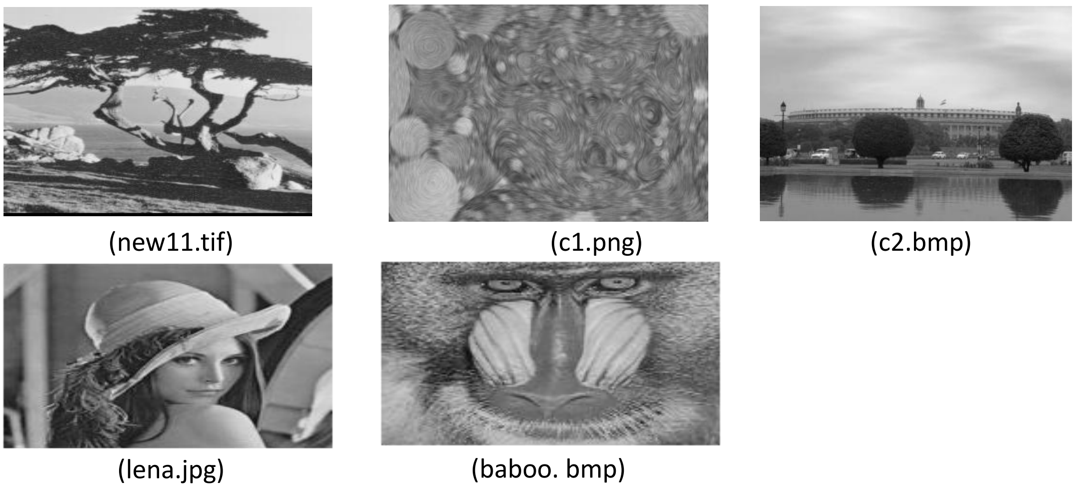
We have proposed a high embedding rate and secure image steganographic algorithm based on Contourlet transform. Contourlet transforms are better than Wavelets in many sense for steganography as described in the introduction. We have compared our algorithm with the existing algorithms based on wavelet transform (Haar and CDF9/7) and wavelet like transform (Slantlet transform). For obtaining secret message, the original message is encoded with Self Synchronizing Variable Length Codes (T-codes) that proves to be a better candidate than the existing Huffman codes [8]. For extra security level, we have used randomization at the embedding in selecting the coefficients of high frequency subbands of cover image obtained through Contourlet 2-level decomposition. For the performance of the algorithm, we have used imperceptiblity measure, PSNR, Structural similarity measure, SSIM and provable security measure, KLDiv, respectively. Apart from this we have present the histogram analysis for finding the effects of statistical attacks. We have observed that CTT are better candidate than existing transforms as they provide high payload, reasonable perceptibility and provable security.



(a) (b)

(c) (d)

Fig. 9. Histograms of original and stego-images obtained of proposed algo 3.1 (a) c2.bmp, (b) lena.jpg, (c) c1.png, (d) new11.tif.



(new11.tif) (c1.png) (c2.bmp)

(lena.jpg) (baboo. bmp)

Fig. 10. Test images.

References

[1] Do, M. N., & Vetterli M. (2005). The Contourlet transform: An efficient directional multiresolution image representation. *IEEE Transaction on Image Processing, 1*, 469-472.

[2] Masaebi, S., & Moghaddam, A. M E. (2012, October). A new approach for image hiding based on contourlet transform. *International Journal of Electrical and Computer Engineering (IJECE)*, *2(5)*, 699 -708.

[3] Sajedi, H., & Jamzad, M. (2010). Using contourlet transform and cover selection for secure steganography. *International Journal of Information Security*, *9*, 337-352.

[4] Navas, K. A., Mathew, N. M., & Sasikumar, M. (2009). Contourlet based data hiding in medical images. CSI.

[5] Manhoran, S. (2003). Towards robust steganography using T-codes. *Proceedings of Video/Image Processing and Multimedia Communications*.

[6] Gunther, U. (1998). Robust source coding with generalised t-codes. Retrieved from http;//www.tcs.Auckland.ac.nz/~ultivh/phd.pdf.

[7] Kumar, S., & Muttoo, S. K. (2013, Febuary). A comparative study of Image algorithms in Wavelet domain. *International Journal Of Computer Science And Mobile Computing (IJCSMC)*.

[8] Kumar, S., & Muttoo, S. K. (2013, Febuary). Image steganography based on wavelet families. *Journal Of Computer Engineering And Information Technology*.

[9] Kumar, S., & Muttoo, S. K. (2010, October). Data hiding techniques based on wavelet-like transform and complex wavelet transform. *Proceedings of International Symposium on Intelligence Information Processing and Trusted Computing* (pp. 1-4). Huanggang, China.

[10] Kumar, S., & Muttoo, S. K. (2011, June). Steganography based on contourlet transform. *International Journal of Computer Science and Information Security (IJCSIS), 90(6)*.

[11] Kumar, S., & Muttoo, S. K. (2013, April). Image steganography based on complex double dual tree wavelet transform. *Proceedings of 3rd International Conference on Signal Acquisition and Processing (ICSAP 2011)*. Singapore.

[12] Selesnick, I. W. (1998, May). The slantlet transform. *IEEE Transactions On Signal Processing*, *47(5),* 1304-1312.

[13] Kumar, S., & Muttoo, S. K. (2009, November). Distortionless data hiding based on slantlet transform. *Proceedings of The First Intenational Conference on Multimedia Information Networking & Security* (pp. 48-52). Wuhan, China.

[14] Kumar, S., & Muttoo, S. K. (2013, Febuary). A reversible image steganography based on slantlet transform. *Bharatiya Vidyapith International Journal of Information Technology*.

[15] Chen, P. Y., & Lin, H. J. (2006). A dwt based approach for image steganography. *International Journal of Applied Science and Engineering*, *4(3)*, 275-290.

Sushil Kumar is an associate professor in the Department of Mathematics, Rajdhani College, University of Delhi, New Delhi. He has received his MSc degree in mathematics, MPhil in mathematics, MTech degree in computer science and PhD degree in computer science from University of Delhi, Delhi.

He has been teaching graduate and under-graduate students for last 34 years. He is the author of three books with titles as Computer fundamental and Software, Scientific and Statistical Computations using Fortran 77 and Theory of Computations.

Dr. Kumar is a reviewer of national and international journals. He has presented talks, attended national and international conferences and published number of research papers *on different subjects such as image steganography, cloud computing, fuzzy topology, parallel computing. He is a life member of CSI.*