A REVERSIBLE DATA HIDING IN TRANSFORM DOMAIN

Sushil Kumar
Rajdhani College, University of Delhi,
New Delhi-110015, India
Mobile: 91-9711234705
azadsk2000@yahoo.co.in

ABSTRACT
The reversible data hiding algorithms based on complex wavelet transform (DD DT DWT) and wavelet-like transform (SLT) using the Companding technique with self-synchronizing variable length code (T-codes) and AES is presented in this paper. A Comparative study is done with the existing algorithm based on DWT. It is shown that the DD DT DWT is a better option in place of DWT in the steganography system in terms of imperceptibility, Structural Similarity and embedding capacity.

Keywords
REVERSIBLE STEGANOGRAPHY, SECURITY, RDH, DD DT DWT, SLT, PSNR, SSIM

1. INTRODUCTION
The reversible data hiding (RDH) technique enables cover image to be restored to their original form without any distortion after removing the hidden data from the stego-image. This technique is useful in many fields such as law enforcement, medical imagery, astronomical research, content authentication of multimedia data and so on. Yang and Lin [2] discusses two kinds of RDH schemes: Perceptual quality schemes that provides a perceived high quality in stego-images with a high embedding rate and Robustness-oriented schemes which are robust to image processing operations. In this poster, a robustness-oriented reversible image steganography scheme based on Slantlet Transform (SLT) [3] and complex wavelet transforms, viz., DD DT DWT [4] in conjunction with AES and self-synchronizing variable length codes, viz., T-codes. A comparison is provided with the RDH based on wavelet transform. The embedding technique used is one of the Companding technique, viz., *thresholding technique* [7]. The use of encryption technique in the proposed algorithm leads to 'security in depth'. To protect the confidential data from unauthorized access, an advanced encryption standard (AES) has also been suggested by the some researchers [2, 8]. AES algorithm is a very secure technique for cryptography and the steganographic techniques which use frequency domain are considered more secures using them at the pre-processing stage. The reference to this work can also be found in [10-13].

2. COMPANDING TECHNIQUE
The Companding is the process of signal compression and expansion. The compression function, C maps large range of original signals x, into narrower range, y = C(x) whereas expansion, E is the reverse process of compression, x = E(y). After expansion, the expanded signals are close to the original ones. Assume the original signals are x. If the equation E[C(x)] = x is satisfied, then this kind of Companding could be applied into reversible data hiding.

3. SELF-SYNCHRONIZING VARIABLE LENGTH CODES (SSVLCs)
In these years of advancement in image compression, many algorithms were proposed to construct self-synchronizing codes. Our approach uses a class of VLCs that poses an extraordinary capability for self-synchronization, called *T-Codes*. Suppose a binary alphabet S={0,1}.To obtain the first set of code words from S, we apply T-augmentation on it, i.e. we remove one of the elements from S and augment it with both the elements of

Titchner [5] proposed the general formula as:

$$S^{(k)}_{(p)} = \bigcup_{i=0}^{k} p^i[S - \{p\}] \cup p^{k+1}$$

where S is a finite alphabet, a string $p \in S$ (called the *T-prefix)* and a positive integer *k* (called the *T-expansion parameter)*.

4. PROPOSED ALGORITHM
The proposed algorithm given below and is illustrated in Figure 3.

Algo 1: Embedding /Extraction

……..

Step1. *First encode the original message using best T-codes to obtain the compressed binary data. This also generates a encoded key required later by receiver at decoding stage.*

Step2. *Apply Modified AES encryption algorithm on the compressed binary data (Step 1) to obtain secret data.*

Step3. *The cover image is transformed into four subbands- LL, LH, HL and HH, using 2-level of SLT and into 12 sub-bands using 1-stage of 2D DD DT DWT.*

Step4. *The encrypted codeword (obtained of Step 2) is then embedded in the randomized coefficients of high frequency subbands using reversible thresholding method and stego key.*

Step5. *The stego image is transmitted through the channel.*

Step6. *The hidden encrypted codewords are extracted from the high frequency subbands obtained of stego image using stego key.*

Step7. *Improved AES decryption algorithm is applied on the extracted codes to obtain the encoded message.*

Step8. *T-decoding is applied to obtain the original message*

Step9. *The original image is constructed by applying reversible thresholding method.*

……..

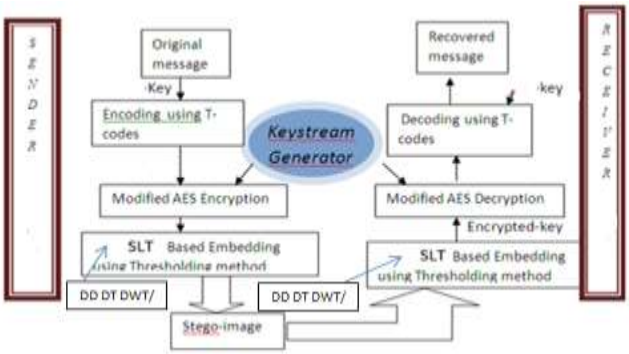

Figure 3. Embedding and Extraction process for Algo 1

5. EXPERIMENTAL RESULTS

The proposed algorithm Algo 1 is tested using number of standard images and medical images. The results of the PSNR of the proposed method based on Wavelet transform, Slantlet transform and DD DT DWT (the embedding capacity =5000 bits) using Huffman codes and AES with and without Gaussian noise are shown in Figure 1 and using T-codes and AES with and without Gaussian noise are shown in Figure 2.. The results are shown here for the four tested images, I1:Cameraman.tif, I2: Lena.jpg, I3: Nature.jpg and I4: Scenery.jpg.

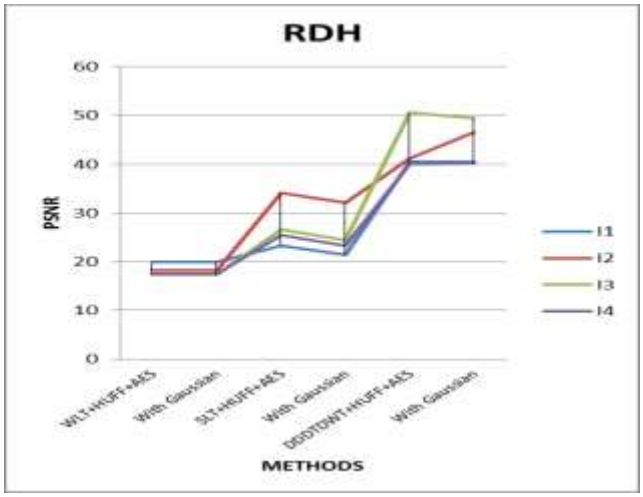

Figure 1. **PSNR values for Algo 1 based on different transforms with AES and Huffman codes**

From Figures, it is observed that using AES at preprocessing stage of algorithm based on DD DT DWT with Huffman codes as encoder results into better imperceptibility whereas WLT based corresponding algorithm does not show much change. In T-codes based algorithm, results improve slightly. It is observed that T-codes alongwith the application of AES provides not only better PSNR values but also robustness against the Gaussian attack. The best results are found for the image 'nature.jpg' as the other images have more edges (contours) and point discontinuities. There is no artifact obtained in the stego-image and the original image is recovered with low image degradation from the stego-image. The integration of Compression technique (T-codes) and cryptography technique (Modified AES) with Steganography use three keys – encoding key, encryption key and threshold value that make the present algorithm a more secured from the eavesdropper. The time complexity of proposed scheme increased when AES used, but overhead (time complexity) is not considered as an important characteristic for steganography scheme by researchers.

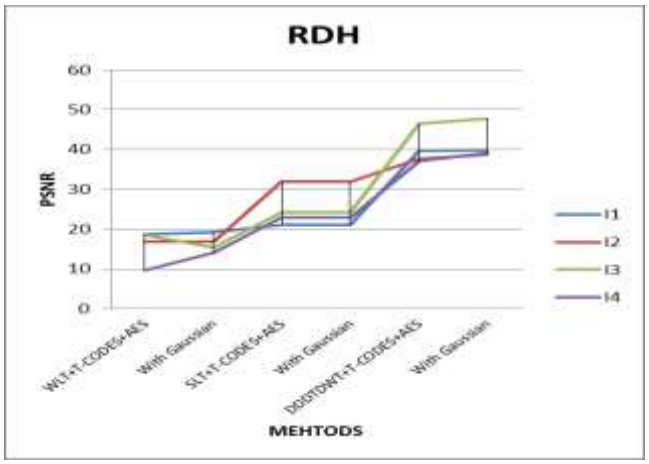

Figure 2. **PSNR values for Algo 1 based on different transforms with AES and Huffman codes**

6. CONCLUSIONS

The DD DT DWT based reversible data hiding using self-synchronizing variable length codes and AES shows better results than DWT in terms of PSNR and is found to be robust to Gaussian effect (same results have been observed for salt and pepper). The DD DT DWT also provides more embedding capacity than DWT. The use of T-codes helps the receiver at decoding stage to retrieve the correct message from stego image. AES applied at the preprocessing stage provides not only more security but also robustness to common carrier attacks. The original image is recovered almost 100% from the stego-image.

REFERENCES

[1] Bloisi D.D., Iocchi L. (2007). Image based Steganography and cryptography, Computer Vision theory and applications volume 1, pp. 127-134.

[2] Yang Ching-Yu and Lin Chih-Hung (2012, June). High-Quality and Robust reversible data hiding by coefficient shifting algorithm, ETRI Journal, Vol. 34, NO. 3.

[3] Selesnick Ivan W. (1998, May).The Slantlet Transform, IEEE transactions on signal processing, Vol. 47, No. 5, pp. 1304-1312.

[4] Selesnick I.W. (2004). The Double-density dual-tree DWT, IEEE Trans. On Signal Processing, 52(5), pp. 1304-1314.

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

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

[7] Kumar S. and Muttoo S.K. (2013, April). A Reversible Image steganography based on Slantlet Transform, BIJIT, vol. 4, Impact Factor 0.605 for the year 2012

[8] Muttoo S.K. and Kumar S. (2011, A multi-layer 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