

# A Multilayered Secure, Robust and High Capacity Image Steganographic Algorithm

S.K.Muttoo  
Department of Computer Science,  
University of Delhi,  
Delhi, India  
[skmuttoo@cs.du.ac.in](mailto:skmuttoo@cs.du.ac.in)

Sushil Kumar  
Department of Mathematics,  
Rajdhani college, University of Delhi,  
New Delhi, India  
[skazad@rajdhani.du.ac.in](mailto:skazad@rajdhani.du.ac.in)

---

**Abstract**— It is observed that all of the current steganographic algorithms rely heavily on the conventional encryption systems which do not serve well in the context of image steganography. Advanced encryption standard (AES) is one of the most powerful techniques of cryptography which can be used as an integral part of steganographic system for better confidentiality and security. In this paper we propose a reversible image steganographic embedding algorithm consisting of three parts. First, we use the self-synchronization variable codes, viz., T-codes for encoding/compressing the original text message. Next, the encoded binary string is encrypted using an improved AES method. The encrypted message is then embedded in the high frequency bands obtained from the cover image by applying the 1-level decomposition of Double Density Dual Tree Discrete Wavelet Transform (DD DT DWT). This algorithm provides three layer of security- one layer at each level of compression, encryption and embedding, respectively. Thus, there is no chance that the intruder may detect the original message after couple of attacks. The algorithm is compared with the corresponding algorithm based on Discrete Wavelet Transform (DWT) and found to be better in terms of imperceptibility, robustness and embedding capacity.

**Keywords**-T-codes; AES; DD DT DWT; DWT; PSNR; SSIM.

---

## I. INTRODUCTION

There has been a vast research for the number of years to find a robust, secure and high capacity steganographic technique. One of the solutions suggested by the researchers is the integration of cryptography with steganography. Due to the recent fast progress in mobile technology and cloud computing, a large digital data exchange is taking place between handset systems and cloud servers. It is now convenient for people to transmit mass data in the form of text, images, audio and video through Internet. However, there is always a threat from the hackers of stealing the valuable information. The organizations such as banking, commerce, diplomacy and medicine, private communications are essential. Thus, it has increased the need of large data storage centers and their security.

We further note the need of storing large amounts of data and due to the bandwidth and storage limitations it is must that the data is compressed before transmission and storage. Usually, Huffman codes have been applied for data compressed. However there has been a search of finding self synchronizing variable length codes since 1970. One of the best self synchronization variable length codes which can replace Huffman codes are T-codes [22-23]. We have applied these codes for data compression in the proposed algorithm. This

also adds another security as the receiver will require an encoding key to encode the secret message after extracting it from stego-image.

Steganography, the science of secret communication, 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. The main goal of steganography include hiding information in undetectable way both perceptually and statistically. The security is also important issue to prevent extraction of hidden information by any third party. Robustness is another issue on which scholars have different views. According to Cox [3], steganography as a process that should not consider robustness as it is then difficult to differentiate from watermarking. Katzenbeisser [7], on the other hand, has mentioned that robustness is a practical requirement for a steganography system. It is also rational to create an undetectable steganography algorithm that is capable of resisting common image processing manipulations that might occur by accident and not necessarily via an attack.

There are number of applications where steganography has proved to be a useful process. For example, it can assist in transmitting electronic patient records across distances to

hospitals and countries through the Internet without worrying about security breaches on the network, such as eavesdroppers' interception. In medical profession and law enforcement fields, it is not only the hiding and recovery of message required perfectly but also the recovery of original image is important for the examination. Further, suppose one wants to email an executable program file to a friend. Normally one will not be able to send executable files through email. Through this technique you can send such files.

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 [1, 26]. We apply a modified AES technique and a key stream (A(5/1), W7) given by Zeghid et al. [26] in our proposed algorithm for this purpose.

The general embedding process is defined in a way that a cover and the corresponding stego-object are perceptually similar.

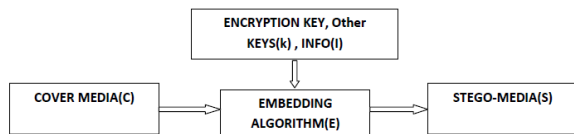


Figure 1: Embedding process

The extraction process is usually a reverse process of embedding.

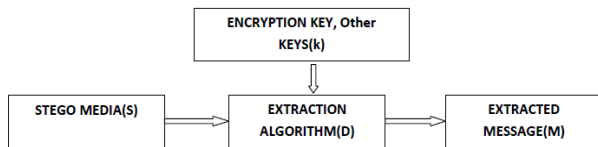


Figure 2: Extraction process

It has been observed that embedding information in the frequency/transform domain of a signal can be much more robust than embedding in the spatial domain. Transform domain methods hide information in insignificant areas of the cover objects which makes them more robust to attacks, such as compression and communication channel noise, remaining imperceptible to the human sensory system. Moreover, the reason of choosing the image steganography is that images are the most popular cover objects for steganography. There exists many different image file formats, most of them for specific applications. Many transform domain methods are independent to image format and may survive conversion between lossless and lossy formats. Moreover, the images provide high degree of redundancy in their representation.

Kumar and Muttou [19] have proposed a novel distortionless data hiding technique based on a Wavelet-like transform, viz., Slantlet transform. Their

experimental results have demonstrated better imperceptibility than the DWT based scheme.

This paper has investigated a novel approach to image steganography which provided enhancements to the current available steganography algorithms. The focus is not just on the embedding strategy, as is the trend in recent research, but is also on the pre-processing stages such as payload encryption and embedding capacity.

In the next section II we give a summary of double density dual tree discrete wavelet transforms (DD DT DWT), review the features of AES, and formula of reversible thresholding algorithm. In section III we give our proposed algorithm, and in section IV, we analyse the experimental results obtained using Matlab 7.4.

## II. REVIEW OF COMPLEX TRANSFORMS AND AES

### A. DD DT DWT

Though the DWT is a powerful tool, it does have three disadvantages, viz., shift sensitivity, poor directionality and absence of phase information. To overcome this, several different methods suggested [10, 15-17]. Two of these methods are Complex Steerable pyramid and the dual tree wavelet transform. The Complex steerable pyramid is approximately shiftable, directional and provides useful phase information, but has high transform redundancy and lacks perfect reconstruction. The dual tree wavelet transform (DTWT), created by Kingsbury [10], is a redundant, complex wavelet transform with excellent directionality, reduced shift sensitivity and explicit phase information. The DTWT not only overcomes the above three disadvantages of DWT, it is perfectly reconstructing and has a small fixed amount of redundancy. The DTWT can discriminate between opposing diagonals with six different sub-bands oriented at  $15^\circ$ ,  $75^\circ$ ,  $45^\circ$ ,  $-15^\circ$ ,  $-75^\circ$ , and  $-45^\circ$ . This also allows for a better representation of vertical and horizontal features.

Hussain and Salman [5] have observed that for the same compression ratio the compressed image using the 2D DT-CWT is more smoothing and have lower RMS error compared with other methods based wavelet techniques and DCT technique.

The *double-density dual-tree DWT*, which is an overcomplete discrete wavelet transform (DWT) designed to simultaneously possess the properties of the double-density DWT [16] and the dual-tree complex DWT [17]. The double-density DWT is based on a single scaling function and two distinct wavelets, where the two wavelets are designed to be offset from one another by one half—the integer translates of one wavelet fall midway between the integer translates of the other wavelet. On the other hand, the development of the dual-tree DWT was motivated by the special properties of complex wavelet transforms.

After the 1-level decomposition, 2-D DT-CWT has four decomposition – each has LL, LH, HL and HH components in

it and 2-d DD DT DWT has 4 decomposition – each has LL, LH<sub>1</sub>, LH<sub>2</sub>, H<sub>1</sub>L, H<sub>1</sub>H<sub>1</sub>, H<sub>1</sub>H<sub>2</sub>, H<sub>2</sub>L, H<sub>2</sub>H<sub>1</sub>, H<sub>2</sub>H<sub>2</sub> in it.

The DT-CWT though introduces limited redundancy ( 4:1 for 2-d signals) and allows the transform to provide approximate shift invariance and directionally selective filters while preserving the usual properties of perfect reconstruction and efficient order-n computation, places restrictions upon the embedding algorithm [21]. So, we decided to use DD DT DWT developed by Selsenick [16].

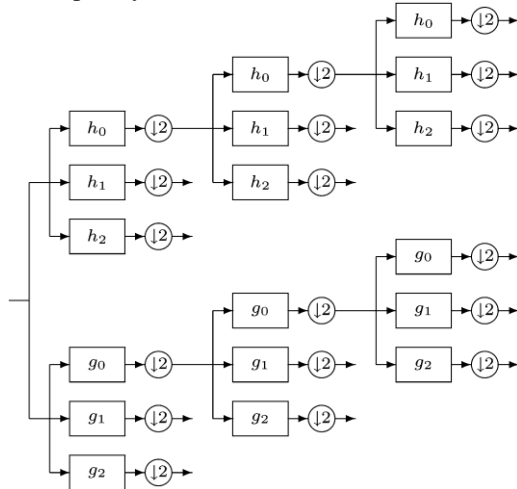


Figure 3: Iterated filterbank for the double-density dual-tree DWT.

**B. AES**

The basic encryption and decryption techniques of AES are shown in figure below.

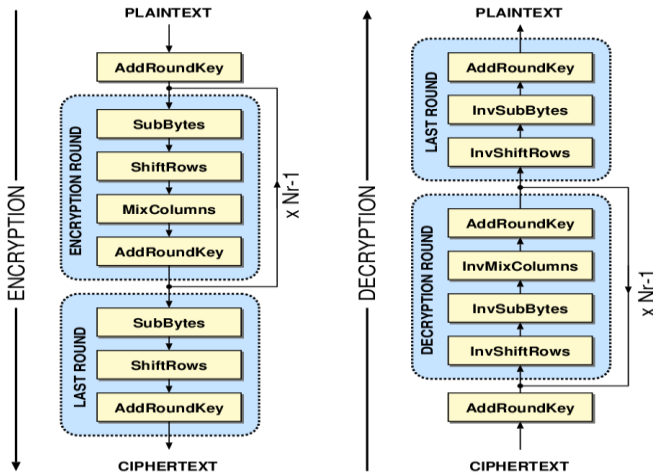


Figure 4: Encryption and Decryption process: AES algorithm

The encryption procedure consists of several steps. After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr=10,12,14 times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The

transformations Inv-Bytesub, the Inv-Shiftrows, the InvMixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption. The decryption process is the reverse of the encryption process.

AES ensures a high security for ciphered image. But the security of the scheme is based on the complexity of AES and the image properties. With AES same data is ciphered to the same value; which is the main security weakness of that mode and the image scheme encryption. Hence, A new encryption scheme has been proposed by M. Zeghid et al. [25] is show in fig. 3.

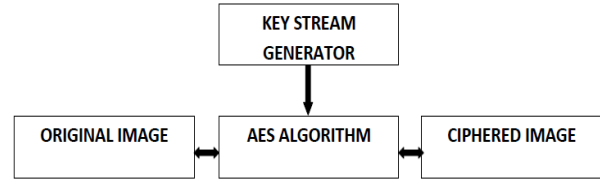


Figure 5: A modified AES algorithm

This algorithm inculcates as an extension to the AES algorithm - a key stream generator. The key stream generator has two different forms: (i) A5/1 key stream generator and (ii) W7 key stream generator.

**III. PROPOSED ALGORITHM**

Our proposed steganographic algorithm is shown in fig. 6.

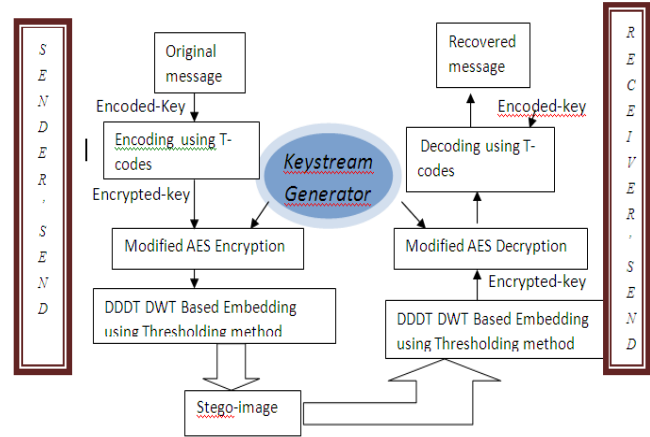


Figure 6: The principal model of proposed Image-steganography

The steps involved in the proposed algorithm may be stated as follows:

**At the Sender’s end**

1. First the original message is encoded using best T-codes.
2. Modified AES encryption algorithm [26] is applied on the compressed data.

3. The cover image is transformed using DD DT DWT .
4. The encrypted code is then embedded in the high frequency bands using reversible thresholding method [25].
5. The stego image is transmitted through the channel.

**At the Receiver’s end**

1. The hidden encrypted codes are extracted from the received stego image.
2. Improved AES decryption algorithm[] is applied on the extracted codes to obtain the actual encoded T-codes.
3. T-decoding is applied to obtain the original message
4. The original image is constructed by applying reversible thresholding method.

*C. Thresholding Algorithm*

Threshold embedding method for the lossless data hiding is given by Xuan et al. [25]. 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:

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

**IV. EXPERIMENTAL RESULTS**

We have compared the performance of the proposed steganographic method based on DD DT DWT using T-codes as encoder, improved AES as encryption and reversible thresholding technique as embedding with the corresponding

steganographic method based on Wavelet. We have tested number of images such as standard images and medical images. We have used two metrics PSNR and SSIM for measuring the stego-image quality.

Table I shows the test results for these methods using only Huffman codes as encoder, Table II shows test results using only T-codes as encoder, Table III shows the results using Huffman codes and improved AES encryption, and Table IV shows the results using T-codes and modified AES encryption. We have shown the results for the four images (see fig. 7), I1: Cameraman.tif, I2: Lena.jpg, I3: Nature.jpg, and I4: Scenery.jpg.

Table I. PSNR values based on Wavelet and DD DT DWT using Huffman encoding (secret message = 5000 bits)

IMAGE	WLT+HUFF	WLT+HUFF (adding Gaussian)	DDDT+HUFF	DDDT+HUFF (adding Gaussian)
I1	19.921678	19.921678	40.687392	40.589223
I2	18.203956	18.203956	40.123817	40.583823
I3	17.292666	17.292666	50.479282	48.986364
I4	17.453638	17.453638	37.276831	38.268783

Table II. PSNR values based on Wavelet and DD DT DWT using T-code encoding (secret message = 5000 bits)

IMAGE	WLT + TCODE	WLT + TCODE (adding Gaussian)	DDDT+ TCODE	DDDT+ TCODE (adding Gaussian)
I1	19.276835	18.739734	39.792321	39.854537
I2	16.892371	16.798323	37.898924	37.872873
I3	15.368473	18.578029	48.868234	47.682376
I4	14.086282	9.738723	39.192321	37.867824

Table III. PSNR values based on Wavelet and DD DT DWT using Huffman encoding and AES encryption (secret message = 5000 bits)

IMAGE	WLT +HUFF +AES	WLT +HUFF +AES (adding Gaussian)	DDDT +HUFF +AES	DDDT +HUFF +AES (adding Gaussian)
I1	19.922627	19.922627	40.478902	40.487912
I2	18.188314	18.188314	41.165721	46.575330
I3	17.292913	17.292913	50.548792	49.478912
I4	17.454110	17.454110	40.027812	40.109042

Table IV. PSNR values based on Wavelet and DD DT DWT using T-codes encoding and AES encryption (secret message = 5000 bits)

IMAGE	WLT+TC ODE +AES	WLT +TCODE +AES (adding Gaussian)	DDDT+TC ODE +AES	DDDT+T CODE +AES (adding Gaussian)
I1	18.739734	19.276835	39.676462	39.798961
I2	16.798323	16.892371	37.689309	38.854126
I3	18.578029	15.368473	46.578229	47.867634
I4	9.738723	14.086282	37.078896	39.212389

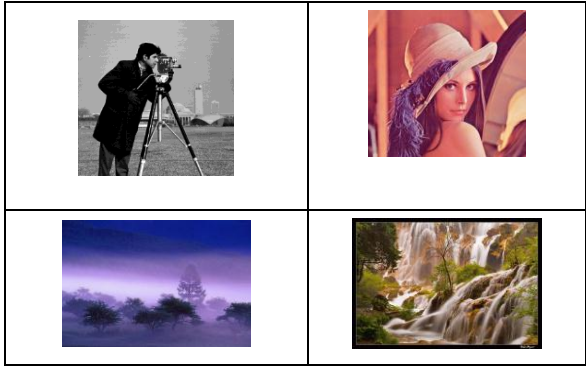


Figure 7: Cover images I1, I2, I3 and I4

The figures 8 and 9 shows the values of PSNR with increase in the embedding capacity and bits per pixels (bpp) rate of the above said methods.

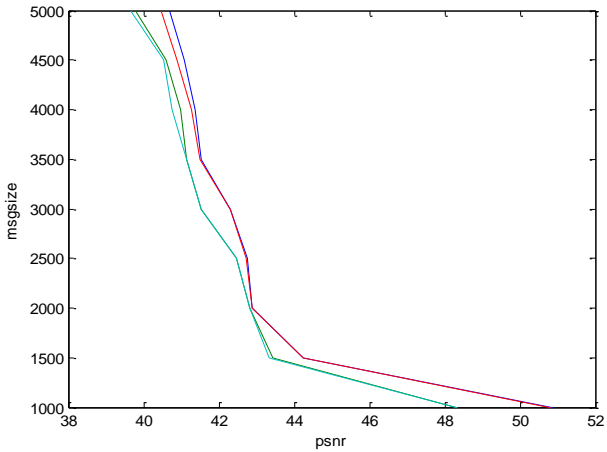


Figure8: Comparison between PSNR and embedded message of DD DT DWT+Huff (green), DD DT DLT+T-code (sky blue), DD DT DWT+Huff +aes (blue), and DD DT DWT+tcode+aes (red) for image I1

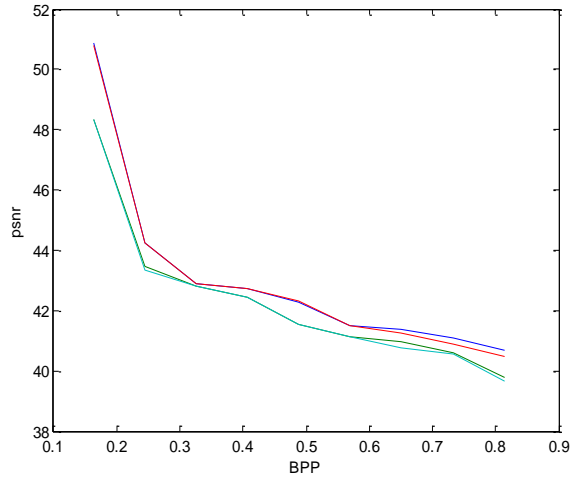


Figure9: Effect of Gaussian noise: PSNR vs msgsize of DD DT DWT+Huff (green), DD DT DWT+tcode (sky blue), DD DT DWT+Huff +aes (blue), and DD DT DWT+tcode+aes (red) for image I1

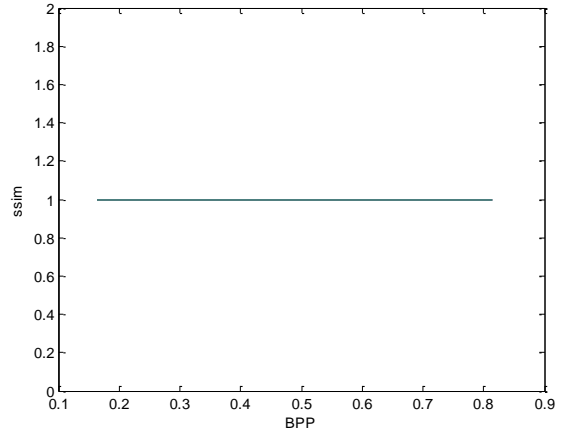


Figure10: Comparison between SSIM and BPP of DD DT DWT+Huff (green), DD DT DWT+tcode(sky blue), DD DT DWT+Huff +aes (blue), and DD DT DWT+tcode+aes (red) for image I1

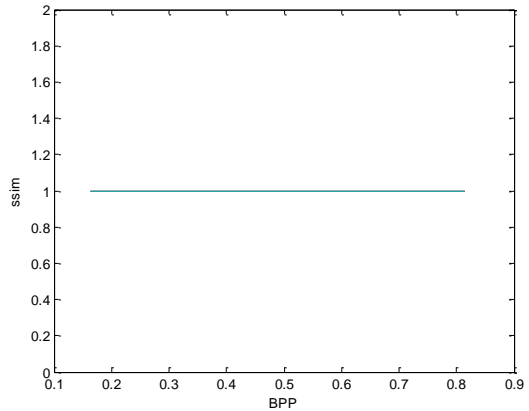


Figure11: Effect of Gaussian noise: SSIM vs BPP of DD DT DWT+Huff (green), DD DT DWT+tcode(sky blue), WLT+Huff + aes (blue), and DD DT DWT+tcode+aes (red) for image I1

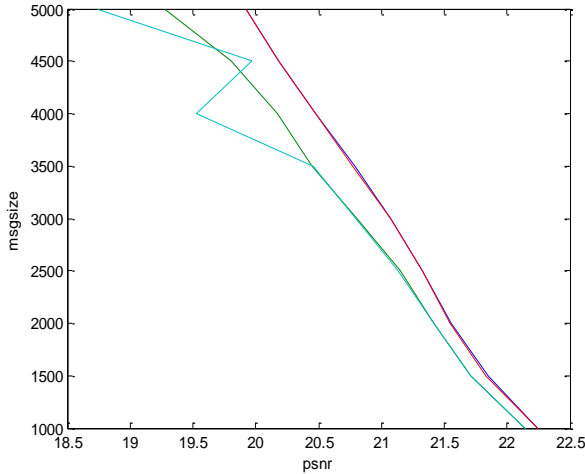


Figure12: Comparison between PSNR and embedded message of WLT+Huff (green), WLT+tcode (sky blue), WLT+Huff+aes (blue), and WLT+tcode+aes (red) for image II

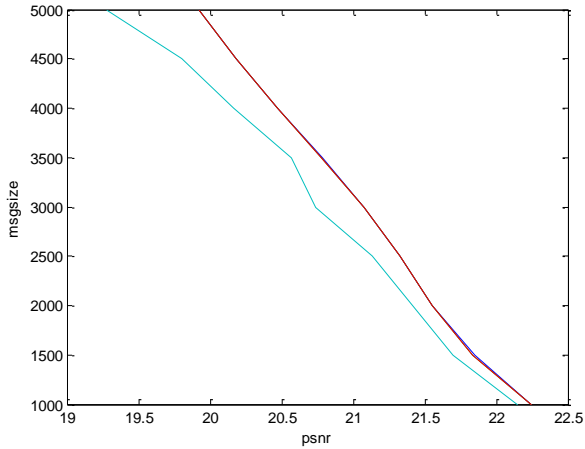


Figure13: Effect of Gaussian noise: PSNR vs msgsize of WLT+Huff (green), WLT+tcode (sky blue), WLT+Huff+aes (blue), and WLT+tcode+aes (red) for image II

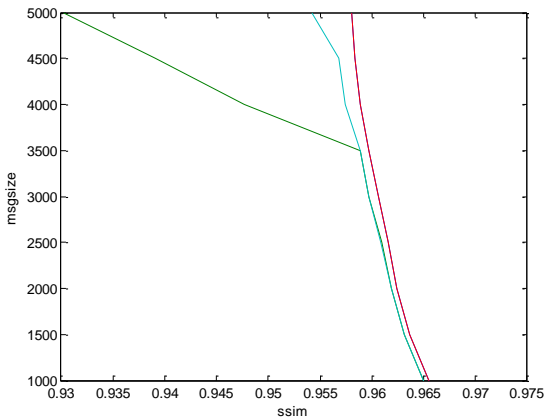


Figure14: Comparison between SSIM and embedded message of WLT+Huff (green), WLT+tcode (sky blue), WLT+Huff+aes (blue), and WLT+tcode+aes (red) for image II

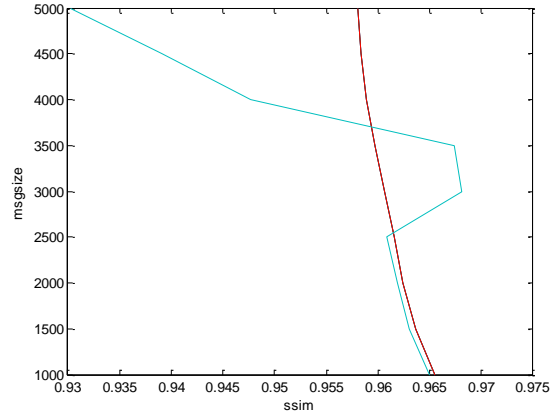


Figure15: Effect of Gaussian noise: SSIM vs msgsize of WLT+Huff (green), WLT+tcode (sky blue), WLT+Huff+aes (blue), and WLT+tcode+aes (red) for image II

We observe the following from the above tables and graphs:

1. The DD DT DWT is a better option than DWT for the steganography system as it provides not only better imperceptibility in terms of PSNR and SSIM, but also provides more embedding capacity .
2. From the above tables it can be seen that DD DT DWT along with Huffman compression technique and AES encryption method has slightly better PSNR values than DD DT DWT along with T-codes and AES method, but the later has better SSIM values (=1) than the earlier method (see figures 10 and 14).
3. From figures 9 and 13, it can be observed that DD DT DWT based steganographic method is robust to Gaussian effect (same results have been observed for salt and pepper).
4. From the fig. 16, it can be seen that the original image is recovered almost 100% from the stego-image, proving the validity of our proposed algorithm.

### V. CONCLUSION

In this paper we have presented

1. a new variable length codes, viz., T-codes for the compression of embedding message.
2. An improved AES for the encryption of the encoded message
3. DD DT DWT in place of DWT as they provide better perceptibility and high capacity
4. The reversible thresholding technique [25] so that one can recover the original image from the stego-image.

The T-codes are self-synchronizing codes shown to be better than Huffman codes in the decoding process. They also provide a layer of security in the system as one needs encoding key to encode the secret message obtained from the extraction process.

AES algorithm is a very secure technique for cryptography and the techniques which use frequency domain are

considered highly secured for system for the combination of steganography.

Thus the integration of Compression technique (T-codes) and cryptography technique (Modified AES) with Steganography use three keys – encoding key, encrypted key and threshold value, making the present algorithm a highly secured method. The proposed method provides not only acceptable image quality but also has almost no distortion in the stego-image after adding Gaussian noise or Salt and Pepper noise. The use of DD DT DWT has shown better results than DWT in terms of image metric ‘SSIM’ and embedding capacity.

REFERENCES

[1] Domenico Daniele Bloisi, Luca Iocchi, “Image based Steganography and cryptography”, Computer Vision theory and applications volume 1 , pp. 127-134 .

[2] Cheddad, A., Condell, J., Curran, K. & Mc Kevitt, P., “Digital image steganography: survey and analysis of current methods”, Signal Processing, 90(3), pp.727-52, 2010 <http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf>

[3] Cox, I., “Information hiding, watermarking and steganography”, Public Lecture. Londonderry: University of Ulster at Magee Intelligent Systems Research Centre, 2009

[4] Frith, D., “Steganography approaches, options, and implications”, Network Security, 8, pp.4-7, 2007

[5] Dr. Hussain S. and Salman A.D., “Image Compression Based on 2D Dual Tree Complex Wavelet Transform (2D DT-CWT)”, Eng. and Tech. Journal, Vol. 28, No. 7, 2010

[6]. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, 31(2)(1998) 26-34

[7] Stefan Katznbesser, Fabien.A., P.Petitcolas editors, “Information Hiding Techniques for Steganography and Digital watermarking”, Artech House, Boston, London, 2000.

[8] Lou, D.C., Hu, M.C. & Liu, J.L., “Multiple layer data hiding scheme for medical images”, Computer Standards and Interfaces, 31(2), pp.329-35, 2009

[9] Mehdi kharrazi, husrev T. Sencar and Nasir Memon, “Image Steganography: concepts and practice” WSPC/ Lecture Notes series, April, 2004.

[10] Kingsbury N.G., “Image processing with complex wavelets”, Philos. Trans. R. Soc. London A, Math. Phy. Sci., 357(1760) (1999) 2543-2560

[11] Jeng-Shyang Pan et al, “Information Hiding and Applications”, Studies in Computational Intelligence, Vol. 27, Springer Verlag Berlin Heidelberg, 2009

[12] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, 01 (3)(2003)32-44

[13] K. B. Raja, Vikas, K. R. Venugopal and L.M. Patnaik, “High capacity lossless secure image steganography using wavelets,” advanced computing and communications, pp 30-235, Dec 2006

[14] Raja, K.B. et al., “Robust image adaptive steganography using integer wavelets”, In Proceedings of the 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE’08. Bangalore, India, 2008. 5-10 Jan. pp.614-621.

[15] Selesnick I. W., “The double density DWT”, in: Wavelets in Signal and Image Analysis: From theory to Practics, A. Petrosian and F. G. Meyer, (Eds), Norwell, MA: Kluwer, 2001

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

[17] Selesnick I. W., R. Baraniuk, and N.G. Kingsbury, “The dual-tree complex wavelet transform: A coherent framework for multiscale signal and image processing”, IEEE Signal Proc. Magazine, (2005) 123-151.

[18] Shih, F., “Digital watermarking and steganography, fundamentals and techniques”, USA: CRC Press, 2008

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

[20] Sushil Kumar and S.K.Muttoo, “Data Hiding techniques based on Wavelet-like Transform and Complex Wavelet Transform”, International Symposium on Intelligence Information Processing and




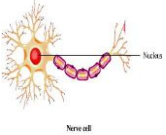
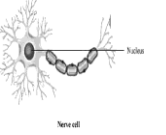
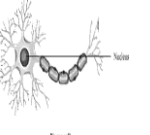






Original Image	Stego Image	Recovered Image
		
		
		
		

Figure16. The original images, Stego-images and recovered images on applying the proposed algorithm with embedding capacity = 5000 bits

ACKNOWLEDGMENT

The authors wish to thank their students Bhavya Ahuja and Deepika Aggarwal for helping in implementation of the codes of this paper on Matlab 7.4.

Trusted Computing, IPTC 2010, Huanggang, China, Oct. 28-29, 2010.

[21] Thompson A. I. et al., "Watermarking for Multimedia Security using Complex Wavelets", Communicated for publication

[22] Titchener, M.R., "Generalised T-codes: extended construction algorithm for self- synchronization codes", IEEE Proc. Commun., Vol. 143, No.3, pp. 122-128, 1999

[23] Ulrich G., "Robust Source Coding with Generalised T-codes", a thesis submitted in the University of Auckland, 1998.

[24] G.Xuan, J.Zhu, J.Chen, Y.Q. Shi Z.Ni and W.Su, "Distortionless data hiding based on integer wavelet transform", IEE Electronics Letters, Dec. 2002, pp. 1646-1648

[25] G. Xuan, Y.Q.Shi, C.Yang, Y.Zhang,D. Zou and P. Chai, "Lossless Data Hiding using integer wavelet transform, and threshold embedding technique", IEEE International conference on Multimedai & Expo (ICME05), Amsterdam, Netherlands, July 6-8, 2005.

[26] M. Zeghid, M. Machhout, L.Khriji, A. Baganne and R. Tourki, "A Modified AES Based Algorithm For Image Encryption", World Academy Of Science, Engineering and Technology 27, 2007

#### AUTHORS PROFILE

1. S. K. Muttoo is an Associate Professor at Department of Computer Science, University of Delhi, Delhi. He is M.Tech. (CSDP) from IIT Kharagpur (1990) and Ph.D. (1982) from University of Delhi in Coding Theory. He has teaching experience of more than 35 years to graduate and postgraduates. His research areas include Coding theory, Steganography and Digital Watermarking. He is a member of CSI, ACM and reviewer of national and international journals.
2. Sushil Kumar is an Associate Professor at Rajdhani College, University of Delhi, New Delhi. His research areas include Information Hiding, Cloud Computing, Parallel Computing and Fuzzy topology. He is a life member of CSI, India and reviewer of national and international Journals.