



# Performance Comparison of Block-DCT, Kekre's Wavelet and Haar Transform using LZW and Huffman Encoding in Image Steganography

Archana B. Patankar, PhD

Associate Professor,  
(Computer Engg. Department)  
Thadomal Shahani Engg. College,  
Mumbai-50, India

Sana Naik

ME (Computer Engineering).  
Thadomal Shahani Engineering College,  
Mumbai-50, India

## ABSTRACT

This paper proposes the use of various transforms for image steganography. It focuses on use of wavelet transform such as Kekre's Wavelet and Haar transform to compress cover image and use of compression mechanisms such as LZW for secret image. Wavelet transform is generated from their respective orthogonal transform. Image Steganography is the art of hiding information into a cover image. A novel technique for image steganography using transforms such as Kekre's wavelet transform and Haar transform along with LZW is used to convert original image (cover image) from spatial domain to frequency domain. In the proposed methodology the secret message is encoded using LZW technique. Then encrypted image/message is embedded in the transformed carrier image. The experimental results show the comparative results between Huffman coding and LZW compression using Kekre's Wavelet transform, Haar transform and DCT. Moreover PSNR and RMSE between the cover image and stego image shows the better results in comparison with other existing steganography approaches. The perceptual difference between the stego image and original image is imperceptible to human eye. The results show an improvement over PSNR and MSE compared to the existing approach. Further high security is maintained since the secret message/image cannot be extracted without knowing decoding rules and Decoding table.

## Keywords

Kekre's Wavelet Transform, Kekre's Transform, Steganography, Haar Transform

## 1. INTRODUCTION

Images are an important medium of communication from many years. The digital Images comprises significant portion of information in multimedia communication [9]. These numbers of images used in our day to day life is generated from many sources. Transmission of such digital images requires large bandwidth and it takes more time [9]. Thus requirement of image compression mechanism arises. Image compression reduces the number of bits required to represent the image [9]. It saves memory space required to store the image as well as time needed to transmit it [9].

Various image compression methods are available today. Thus Cryptography and steganography are used together for providing security at a higher end. Steganography is basically hiding of a secret message within a container such as an image in an imperceptible way. Steganography takes

cryptography a step farther by hiding an encrypted message so that no one suspects it exists [8].

Transforms provide excellent compression mechanism and they also support information hiding which makes it more useful in steganography. Transform such as Discrete Cosine Transform (DCT) has a very high energy compaction property and hence gives a higher compression ratio. But it eliminates correlation across the boundaries and hence results in blocking artifacts. This drawback can be avoided by using wavelet transforms [9]. Therefore wavelets can be used to improve the results of steganography.

## 2. LITERATURE REVIEW

In paper [8], a novel technique for Image steganography based on Block-DCT, where DCT is used to transform original image (cover image) blocks from spatial domain to frequency domain is proposed [8]. Firstly a gray level image of size  $M \times N$  is divided into non-joint  $8 \times 8$  blocks and a two dimensional Discrete Cosine Transform (2-d DCT) is performed on each of the  $P = MN / 64$  blocks [8]. Then secret messages/images are encrypted using Huffman encoding and then each bit of Huffman code of secret message/image is embedded in the frequency domain by altering the least significant bit of each of the DCT coefficients of cover image blocks. The results of the paper show that the algorithm has a high capacity and a good invisibility [8]. The PSNR of cover image with stego-image in [8] show better results in comparison with other existing steganography approaches. It also states that reliable security is maintained since the secret message/image cannot be extracted without knowing decoding rules and Huffman table [8].

In [19] technique for image steganography using transforms such as Kekre's wavelet transform and Haar transform along with Huffman coding one at a time to convert original image (cover image) from spatial domain to frequency domain are given.

In [9] use of wavelet transforms in image compression. Wavelet transform is generated from respective orthogonal transform is proposed. Image compression using Walsh wavelet, Kekre Wavelet and Slant Wavelet transforms are generated from Walsh transform, Kekre Transform and Slant Transform respectively [9]. Four different size combinations of component orthogonal transforms are used. Size of local component transform is varied as  $N=32, 16, 8$  and  $4$  [9]. Experiments are performed on twenty sample colour images of size  $256 \times 256 \times 3$  [9]. The results compare the performance

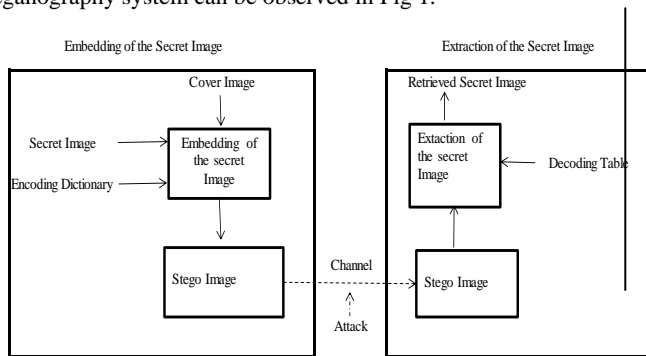
of three wavelet transforms in terms of compression ratio and bit rate. Each wavelet transform shows different performance when different component size used. It states that Kekre wavelet Transform of 4 any size can be generated from Kekre's transform.5r

Generation of Kekre's Wavelet (KW) transform from Kekre's transform and application of Kekre's wavelet for steganography is shown in [7]. The full cover image is transformed using Kekre's Wavelet transform. This transformed image is then divided into 16 equal non-overlapping blocks. Then energy of each block is computed. The secret data is embedded into lower energy blocks of the transformed image. Hiding capacity of 56.25% of the cover image size with 100% retrieval of secret data are obtained in [7]. There is no difference between the quality of the stego image to original one. Finally the results of Haar transform, Modified Haar transform and Kekre's Wavelet transform are compared [7].

### 3. PROPOSED METHODOLOGY

Here, Kekre's Wavelet transform and Haar Transforms are generated using respective orthogonal component transforms. Size of component transforms is varied to obtain wavelet transform of same size.

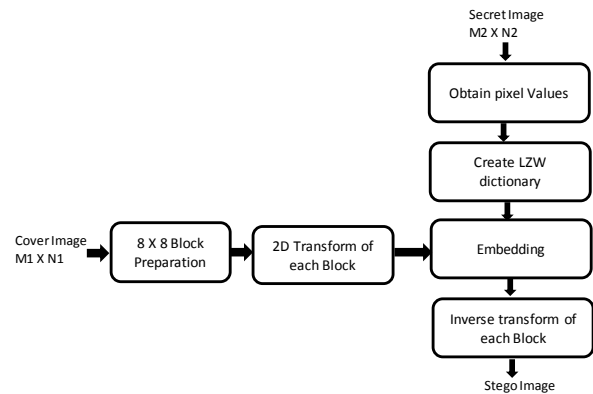
The work done previously in Image Steganography was by default in spatial domain and frequency domain was by using LSB approach but since the data hidden by using LSB bit sustain to attacks. A new technique is proposed in frequency domain by hiding the data in the decimal coefficient of each last element of each transformed 8X8 block of the cover image. The data to be hidden are the encoded bits obtained by compressing secret image by using either Huffman Encoding or LZW compression technique. This encrypted data is hidden in last coefficient of each transformed 8X8 block of the cover image. The cover image is transformed from spatial domain to frequency domain by using Kekre's Wavelet transform or Haar transform. The steganography system can be observed in Fig 1.



**Fig 1 Block Diagram for Image Steganography**

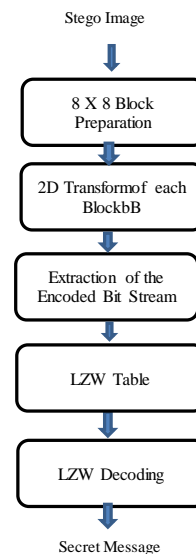
Separation of Red, Green and Blue plane of cover images is carried out and then the image is divided into 8X8 blocks, padding is done in case of uneven blocks. Then wavelet transform is applied on each block of the cover image. The image thus obtained is the transformed image. The secret image is compressed using LZW compression algorithm. Thus an encoded bit stream of stego image is generated after compression using LZW algorithm. Then this encoded bit stream is hidden one by one after the decimal point of the last value of each 8X8 block of the transformed cover image. The inverse transform of each block gives Stego image. This

process is referred as embedding of the secret image and is shown in Fig 2.



**Fig 2 Embedding of the Secret Image**

Now the stego image is divided into 8X8 blocks and respective transform such as Kekre Wavelet Transform or Haar is applied. Then the encoded bit stream present after the decimal point of the last value of each 8X8 block is extracted. This bit stream is then referred in the LZW table and then the LZW decoding is done on this bit stream to obtain the secret image. This entire extraction of the secret image process is shown in Fig 3.



**Fig 3 Extraction of the Secret Image**

Since the secret message/image in the spatial domain can easily be extracted by unauthorized user, a frequency domain steganography technique for hiding a large amount of data with high security, a good invisibility and no loss of secret message is proposed

The main purpose to hide information in the frequency domain is to alter the magnitude of all of the transformed coefficients of cover image. The transform method converts the image blocks from spatial domain to frequency domain.



#### 4. EXPERIMENTATION AND RESULTS

In this section, some experiments are carried out to prove the efficiency of the proposed approach. The proposed method has been simulated using the MATLAB 7 program on Windows 7 platform. The results are been compared with results obtained in paper [19].

A set of 8-bit grayscale images of size 1920 × 1200 are used as the cover-image to form the stego-image. Results are shown in below tables and their explanation is described respectively.

**Table1 PSNR values between stego and cover image**

Cover Image	Secret Image	LZW		Huffman Coding	
		Haar	KWT	Haar	KWT
Tiger	secImg1	113.8945	114.2451	97.6029	97.5546
	secimg2	118.7044	119.0849	101.2573	101.2321
	secimg3	115.8789	115.8788	99.9245	99.9178
Lady	secImg1	114.7984	114.8602	101.6321	101.7952
	secimg2	119.2105	119.2744	104.3347	104.5463
	secimg3	116.0976	116.2196	103.1182	103.2345
Wolf	secImg1	104.4612	103.5587	94.3174	94.0167
	secimg2	107.2275	106.4051	97.2298	97.1196
	secimg3	105.4636	104.3666	95.8815	95.6198
<b>Average PSNR</b>		112.859622	112.654822	99.4776	99.448511

Table 1 shows PSNR values between the stego image and cover image where PSNR value is comparatively greater when using Haar Transform for transforming cover image and compressing secret image using LZW.

**Table 2 MSE values between stego and cover image**

Cover Image	Secret Image	LZW		Huffman Coding	
		Haar	KWT	Haar	KWT
Tiger	secImg1	2.6732E-07	2.4659E-07	1.156E-05	1.156E-05
	secimg2	8.8317E-08	8.0907E-08	4.84E-06	4.84E-06
	secimg3	1.6928E-07	1.6928E-07	6.76E-06	6.76E-06
Lady	secImg1	2.1709E-07	2.1402E-07	4.41E-06	4.41E-06
	secimg2	7.8601E-08	7.7454E-08	2.56E-06	2.25E-06
	secimg3	1.6096E-07	1.565E-07	3.24E-06	3.24E-06
Wolf	secImg1	2.3462E-06	2.8881E-06	2.401E-05	0.000025
	secimg2	1.2409E-06	1.4996E-06	1.225E-05	1.296E-05
	secimg3	1.8626E-06	2.3978E-06	1.681E-05	1.764E-05
<b>Average MSE</b>		7.1459E-07	8.5892E-07	9.604E-06	9.851E-06

Table 2 shows MSE values between the stego image and cover image where MSE value is comparatively greater when using Haar Transform for transforming cover image and compressing secret image using LZW.

**Table3 PSNR values between stego and cover image under salt and pepper attack**

Cover Image	Secret Image	LZW		Huffman Coding	
		Haar	KWT	Haar	KWT
Tiger	secImg1	69.7655	69.7479	69.8098	69.7692
	secimg2	69.7215	69.7442	69.7821	69.7746
	secimg3	69.7599	69.7568	69.7387	69.7415
Lady	secImg1	70.2664	70.2259	70.2536	70.2469
	secimg2	70.2594	70.2332	70.2588	70.2328
	secimg3	70.2669	70.2534	70.2302	70.2835
Wolf	secImg1	70.0602	70.0444	70.0535	70.0507
	secimg2	70.0861	70.0807	70.0959	70.1228
	secimg3	70.0682	70.0857	70.0648	70.052
<b>Average PSNR</b>		70.0282333	70.0191333	70.031933	70.030444

Table 3 shows PSNR values between the stego image and cover image where PSNR value is greater when using Haar Transform for transforming cover image and compressing secret image using Huffman Coding under salt and pepper attack.

**Table 4 MSE values between stego and cover image under salt and pepper attack**

Cover Image	Secret Image	LZW		Huffman Coding	
		Haar	KWT	Haar	KWT
Tiger	secImg1	0.0069	0.0069	0.0068	0.0069
	secimg2	0.007	0.007	0.0069	0.0069
	secimg3	0.0069	0.0069	0.0069	0.0069
Lady	secImg1	0.0062	0.0062	0.0061	0.0062
	secimg2	0.0062	0.0062	0.0061	0.0062
	secimg3	0.0061	0.0062	0.0064	0.0062
Wolf	secImg1	0.0065	0.0065	0.0063	0.0064
	secimg2	0.0061	0.0064	0.0065	0.0064
	secimg3	0.0065	0.0064	0.0064	0.0064
<b>Average MSE</b>		0.00648889	0.00652222	0.0064889	0.0065

Table 4 shows MSE values between the stego image and cover image where MSE value is greater when using Haar Transform for transforming cover image and compressing secret image using LZW under salt and pepper attack.

**Table5 PSNR values between stego and cover image under speckle noise attack**

Cover Image	Secret Image	LZW		Huffman Coding	
		Haar	KWT	Haar	KWT
Tiger	secImg1	67.4797	67.4805	67.4711	67.471
	secimg2	67.4777	67.4794	67.4762	67.4689
	secimg3	67.4694	67.4786	67.4667	67.4744
Lady	secImg1	67.1999	67.2062	67.1979	67.2035
	secimg2	67.204	67.2016	67.203	67.2048
	secimg3	67.2033	67.2026	67.2021	67.2084
Wolf	secImg1	71.0493	71.046	71.0369	71.0333
	secimg2	71.0504	71.0518	71.0391	71.0417
	secimg3	71.0488	71.0507	71.0357	71.0386
<b>Average PSNR</b>		68.5758333	68.5774889	68.569856	68.571622

Table 5 shows PSNR values between the stego image and cover image where PSNR value is comparatively greater when using Kekre's Wavelet transform for transforming cover image and compressing secret image using LZW under speckle noise attack.



**Table 6 MSE values between stego and cover image under speckle noise attack**

Cover Image	Secret Image	LZW		Huffman Coding	
		Haar	KWT	Haar	KWT
Tiger	secImg1	0.0117	0.0117	0.0117	0.0117
	secimg2	0.0117	0.0117	0.0117	0.0117
	secimg3	0.0117	0.0117	0.0117	0.0117
Lady	secImg1	0.0125	0.0125	0.0124	0.0125
	secimg2	0.0125	0.0125	0.0125	0.0125
	secimg3	0.0125	0.0125	0.0125	0.0125
Wolf	secImg1	0.0051	0.0052	0.0052	0.0052
	secimg2	0.0051	0.0051	0.0052	0.0052
	secimg3	0.0051	0.0051	0.0052	0.0052
<b>Average MSE</b>		0.00976667	0.00977778	0.0097889	0.0098

Table 6 shows MSE values between the stego and cover image where the results are again very much similar for Kekre

wavelet transform ,Haar transform and LZW under speckle noise attack.

The results states a good improvement over PSNR and MSE values using Haar transform and Kekre Wavelet Transform to convert Cover image from spatial domain to frequency domain without any attacks.







It also shows that the MSE values is lower in case of using Haar transform for transforming cover image and using LZW compression mechanism for secret image.

The MSE values between the stego image and cover image are equal when speckle noise attack is applied on the retrieved image.

Further in figure 3 MSE and PSNR values are shown on respective Cover Image and Stego Image. In the results three different cover images of size 1920X1200 are used to hide three different secret images of size 50X50 one at a time.

SECRET IMAGE	ORIGINAL COVER IMAGE		RETRIEVED IMAGE		
			DCT	Haar Wavelet	Kekre Wavelet
	STEGO IMAGE 	Huffman Encoding	 PSNR = 92.5645 MSE = 0.00003	 PSNR = 101.6321 MSE = 0.0000441	 PSNR = 101.7952 MSE = 0.0000441
		LZW		 PSNR = 114.7984 MSE = 0.0000021709	 PSNR = 114.8602 MSE = 0.0000021402
	STEGO IMAGE WITH SPECKLE NOISE 	Huffman Encoding	 PSNR = 67.1839 MSE = 0.012544	 PSNR = 67.1979 MSE = 0.0124	 PSNR = 67.2035 MSE = 0.0125
		LZW		 PSNR = 67.1999 MSE = 0.0125	 PSNR = 67.2062 MSE = 0.0125

**Fig 4 PSNR and MSE Comparitive results using Kekre wavelet transform ,Haar transform and DCT transformsusing Huffman Encoding and LZW.**

<p>STEGO IMAGE WITH SALT AND PEPPER NOISE</p> 	Huffman Encoding	 PSNR = 70.2247 MSE = 0.0062	 PSNR = 70.2536 MSE = 0.0061	 PSNR = 70.2469 MSE = 0.0062
	LZW	 PSNR = 70.2664 MSE = 0.0062	 PSNR = 70.2259 MSE = 0.0062	

**Fig 5 PSNR and MSE Comparitive results using Kekre wavelet transform ,Haar transform and DCT transformusing Huffman Encoding and LZW.**

Fig 4 and 5 shows the comparative results along with salt and pepper attack and speckle noise attack.the results show the stego images with attacks and without attack along with the retrieved secret image. The results specify the PSNR and MSE values in each case.

## 5. CONCLUSION

In this paper Kekre’s Wavelet Transform (KWT) [4] and Haar Transform[3] are used to convert the cover image into frequency domain. LZW encryption [36] and Huffman Encoding are the compression algorithm used to compress secret image. The encoded bits generated from the compression algorithms are hidden in last coefficient of each transformed 8X8 block of the cover image. In total there will be four combinations used for image steganography such as Kekre’s wavelet Transform of the cover image and Huffman Encoding compression algorithm on secret image, Kekre’s wavelet Transform of the cover image and LZW compression algorithm on secret image, Haar transform of the cover image and Huffman Encoding compression algorithm on secret image and Haar transform of the cover image and LZW compression algorithm on secret image. Moreover PSNR and MSE values are calculated to compare the different techniques of Steganography. The performance of the various techniques is also compared under Speckle noise attack and Gaussian noise attack. The results specify that compression algorithm LZW performs better than Huffman Encoding by using KWT on the cover image. In future other image transforms in combination with different encryption algorithms can be explored.

## 6. REFERENCES

- [1] H.B. Kekre, SudeepThepade, “Image Retrieval using Non- Involutional Orthogonal Kekre’s Transform”, International Journal of Multidisciplinary Research and Advances in Engineering (IJMRAE), Vol. 1, No.1, November 2009. Pp. 189-203.
- [2] M. Sifuzzaman1, M.R. Islaml and M.Z. Ali, “Application of Wavelet Transform and its Advantages Compared to Fourier Transform”, Journal of Physical Sciences, Vol. 13, 2009, pp. 121-134.
- [3] H.B. Kekre, TanujaSarode, SudeepThepade, Sonal Shroff, “Instigation of Orthogonal Wavelet Transforms using Walsh, Cosine, Hartley, Kekre Transforms and Their use in Image Compression” International Journal of Computer Science and Information Security, Vol. 9, No. 6, 2011.
- [4] H.B. Kekre, ArchanaAthawale, DipaliSadavarti, “Algorithm to Generate Kekre’s Wavelet Transform from Kekre’s Transform”, International Journal of Engineering Science and Technology (IJEST), Vol. 2, No. 11, 2010, pp. 756-767.
- [5] Gonzalez, R.C. and Woods, R.E., Digital Image Processing using MATLAB, Pearson Education, India,2006.
- [6] Jayaraman, S., Esakkirajan, S. and Veerakumar, T. Digital Image Processing, Tata McGraw Hill Education Private Limited, India, 2009.
- [7] Chan, C.K. and Cheng. L.M. 2003. Hiding data in image by simple LSB substitution. Pattern Recognition, 37: 469 – 474.
- [8] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar,“A novel technique for image steganography based on Block-DCT and Huffman Encoding”, International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010
- [9] H.B. Kekre, Tanuja Sarode, Prachi Natu “Performance Comparison of Walsh Wavelet,Kekre Wavelet and Slant Wavelet Transform in Image Compression, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013
- [10] Chen, T.S., Chang C.C., and Hwang, M.S. 1998. A virtual image cryptosystem based upon vector quantization. IEEE transactions on Image Processing, 7,10: 1485 – 1488.

- [11] Chung, K.L., Shen, C.H. and Chang, L.C. 2001. A novel SVD- and VQ-based image hiding scheme. *Pattern Recognition Letters*, 22: 1051 – 1058.
- [12] Iwata, M., Miyake, K., and Shiozaki, A. 2004. Digital Steganography Utilizing Features of JPEG Images, *IEICE Transfusion Fundamentals*, E87-A, 4:929 – 936.
- [13] Li, Zhi., Sui, Ai, Fen., and Yang, Yi, Xian. 2003 “A LSB steganography detection algorithm”, *IEEE Proceedings on Personal Indoor and Mobile Radio Communications*: 2780-2783.
- [14] H.B. Kekre, ArchanaAthawale, DipaliSadawarti, “Algorithm to Generate Wavelet Transform from an Orthogonal Transform”, *International Journal of Image Processing (IJIP)*, Vol.4, Issue 4, 2010.
- [15] Moerland, T, “Steganography and Steganalysis”, *Leiden Institute of Advanced Computing Science*, [www.liacs.nl/home/tmoerl/privtech.pdf](http://www.liacs.nl/home/tmoerl/privtech.pdf)
- [16] Ahmed, N., Natarajan T., Rao K. R. “Discrete cosine transform”. In: *IEEE Transactions on Computers*, Vol. 23, 1974, 90-93.
- [17] R.S. Stanković and B.J. Falkowski. “The Haar wavelet transform: its status and achievements”. *Computers and Electrical Engineering*, Vol. 29, No.1, January 2003, pp.25-44
- [18] H. B. Kekre, TanujaSarode, PrachiNatu : “Color Image Compression using Hybrid Wavelet Transform with Haar as Base Transform”,*International Journal of Scientific and Research Publications*, Volume 4, Issue 6, June 2014 1 ISSN 2250-3153.
- [19] DrArchana B. Patankar ,Sana Haji “A Comparative study of Block-DCT, Kekre’s Wavelet and Haar Transform using Huffman Encoding in Image Steganography” *International Conference on Communication Computing and Virtualization 2015*,Vol.1 ,ISBN 978-0-9884925-7-8,pp 119-124