Performance analysis of Image Steganography Schemes based on different Transform Domains

Dr. Sushil Kumar Azad nėe Dr. Sushil Kumar

Department of Mathematics, Rajdhani College, University of Delhi, New Delhi

ABSTRACT

This paper presents the comparative analysis of steganography in gray-scale and color digital images using transform domain approach. A summary on different transforms used in steganographic schemes is included. The performance analysis of image steganography schemes is presented based on the basic characteristics of steganography such as imperceptibility, payload, undetectability, security and robustness. .

Keywords: Image Steganography, DCT, W LT, SLT, CTT, DD DWT, DD DT DWT

INTRODUCTION

Data hiding is a process to embed a useful information or data into a cover object such as such as text, an image file, an audio/video file and a TCP/IP header file. The popularity of digital data hiding has increased in recent years due to the fast advancement of the computer and network technology. The private communications is essential for the organizations such as Banking, Commerce, Diplomacy, Medical profession and others. Usually, the private data is encrypted into some ciphertext that appears totally meaningless before it is sent out through the net. But, the ciphertext can draw hacker's attention and can easily destroy the ciphertexts and make the transmissions fail, even though he/she may not be able to decrypt it. Steganography, a branch of data hiding ensure the security of the secret information travelling on the internet by avoiding any attention and suspicion of the chacker. In fact, steganography scheme have found to be more flexible and robust to variety of image processing operations in conjunction with coding techniques and with the advancement of information theory.

Table 1: Applications of Data Hiding

Application areas	**Purpose**
Defence organizations	For safe circulation of secret data
Medical profession	To assist in transmitting electronic patient records across distances to hospitals and countries through the Internet without worrying about security breaches on the network
Law enforcement fields	Not only the need of hiding and recovery of message required perfectly, but also the recovery of original cover is importorant for the examination.
Military and intelligence agencies	For safe circulation of secret data
E-government	For secrecy of the data
Smart identity card	Safety of personal details embedded
Image authentication	For copyright control of materials
Online voting system	To make the online election secure and robust against a variety of fraudulent behaviours
Mobile banking	To improve security
Tamper proofing	To prevent or detect unauthorized modifications and other numerous applications

There are mainly four requirements of any data hiding or steganographic technique, namely, Impercptibility, Capacity, Security and Robustness. Imperceptibility means that human eyes cannot distinguish the difference between the steg-image and the original image. Capacity refers to the amount of data that can be embedded in the cover object. Security means that an eavesdropper cannot detect the hidden data, and Robustness requires that the hidden data can be recovered within certain acceptable errors even when the stego-image has endured some signal processing or noises. The following diagram depicts the characteristics of the stego-system:

IMPERCEPTIBILITY	SECURITY	CAPACITY	UNDETECTABILITY	ROBUSTNESS
H	**H**	**H**	***H***	***R***

(H= 'High' , R='Reasonable')

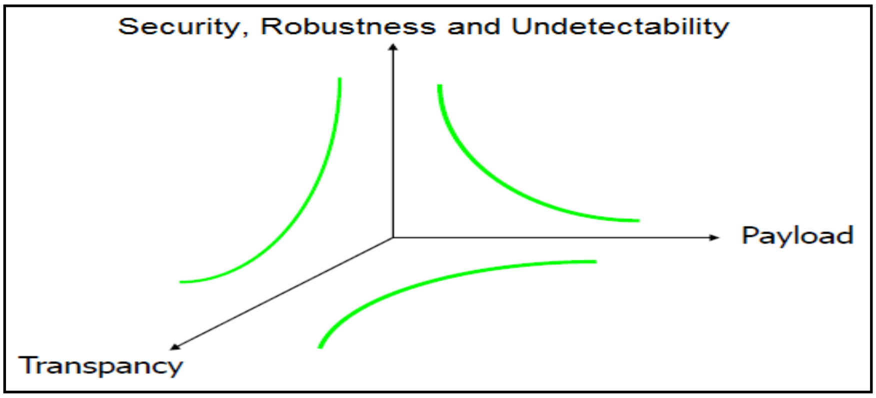


Fig 1:Trade-off among security, robustness, undetectability, transparency and payload (Fridrich [5])

Figure 1 depicts the relationship between the characteristics of steganography. It shows that if we want to embed high payload then, either transparency may be lost or the stego-system may not remain robust to common statistical attacks or the message may become detectable by the eavesdropper.

The main goals of the design of good steganographic algorithms are:

(i) *The choice of accurate covers,*
(ii) *The search for embedding technique which modify the cover as little as possible to make them robust from the accidental distortions (common attacks) and*
(iii) *To make the data hiding secured.*

There are many options of digital media for using as the cover object such as text, audio, video, protocols or images. Image steganography is found to be a better option by researchers due to the following reasons:

1. confined ability of human visual system;

2. availability of high degree of redundancy (i.e., presence of superfluous information which can be easily interpolated [1]);

3. 'innocent' data types to eavesdroppers;

4. *A 1024 x 768 image has a potential to hide a total of 2,359,296 bits (294,912 bytes) of information using 3-LSB insertion method, and in 640 x 480 image of 256 colors (8 bits/pixel), one can hide 300 kB worth of data* [7].

STEGANOGRAPHIC PROCESS

The steganographic process is usually consists of two methods, viz., Embedding method and Extraction method. To define these methods, we first define some basic notations

Notations:

1. C: the set of cover objects

2. M : original message to be embedded in cover objects

3. K: set of keys

4. S: modified cover object, called stego-object.

5. SC: *Steganographic Channel space, that is, the redundant space of the cover object.*

We define the *Steganographic System*, SS as the pair $< SSE_{sc}, SSD_{sc} >$, where

$SSE_{SC}: C \times M \times K \rightarrow C'$ is defined by

$SSE_{sc}(c, m, k) = c^*$ for all $c \in SC, m \in M, k \in K$

and $SSD_{sc}: C' \times K \rightarrow M$ is defined by

$SSD_{sc}(c^*, k) = m$

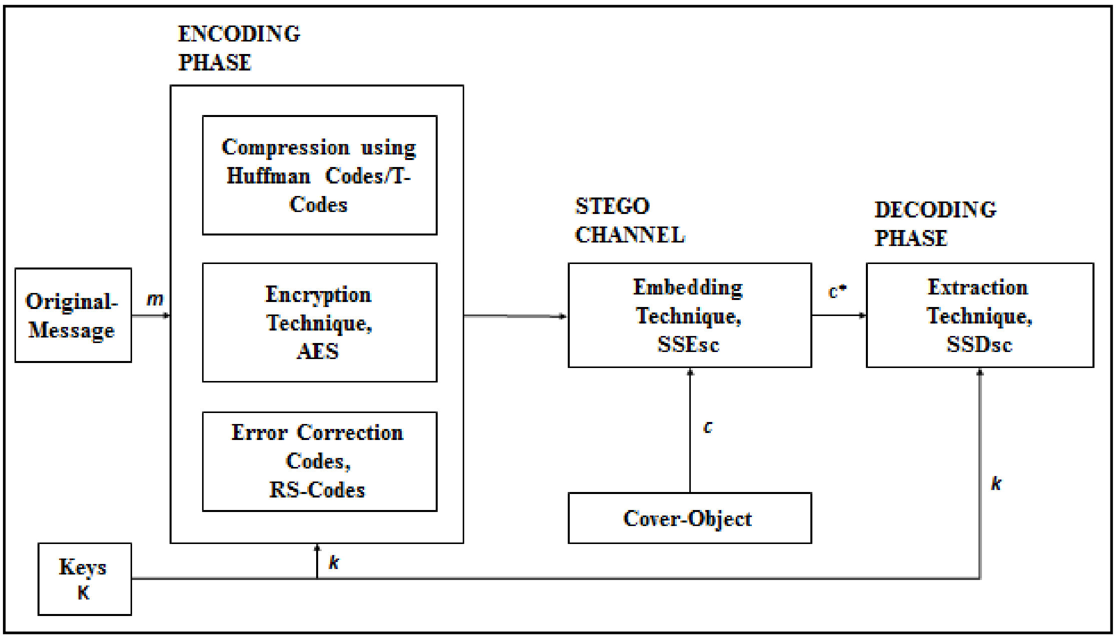


Fig 2: General model for steganographic system [12]

CLASSIFICATION OF STEGANOGRAPHY SCHEMES

Depending on the applications, Steganography methods have been classified in many ways which are summarized as follows:

1. High bit-rate data hiding** and **low bit-rate data hiding

*2. Distortion free or **reversible** steganography and fragile or **irreversible** steganography*

3. Spatial domain** and **Transform domain

4. Protection against detection (i.e., data hiding) and Protection against removal(Watermarking and fingerprinting)

*5. **Pure** stegonagraphy technique, the **secret** stegonagraphy technique and the **public key** stegonagraphy technique.*

6. Text information hiding, Image information hiding, Audio information hiding, Video information hiding and so on

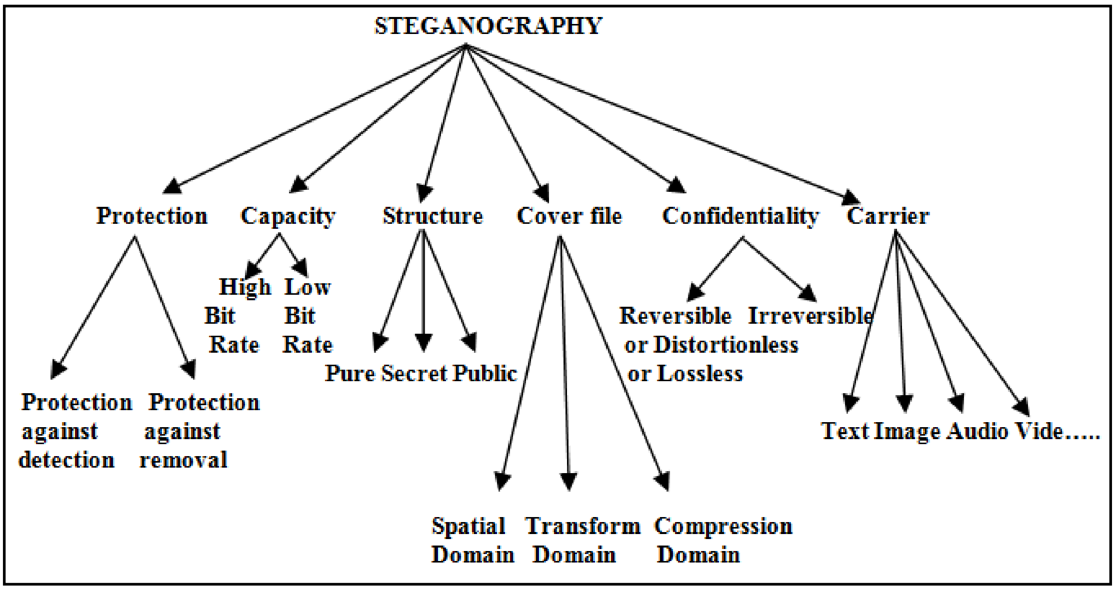


Fig 3: Classification of Steganography[12]

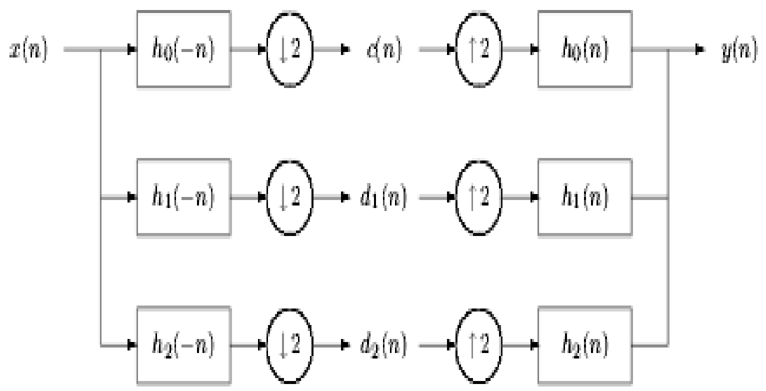
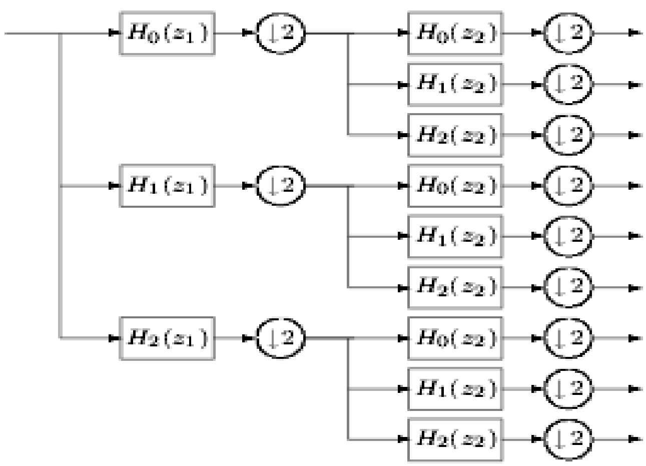
Research in the spatial and transform domains for finding a robust, secure and high payload steganographic technique has attracted many researchers. It has been observed that the spatial domain based steganographic schemes have relatively low-bit capacity and are not resistant enough to lossy image compression and other image processing. On the contrary, frequency domain-based schemes can embed more payload and are more robust to attack. To provide an additional layer of security, Cryptography and Source encoding methods have also been used in conjunction with *Steganography*.

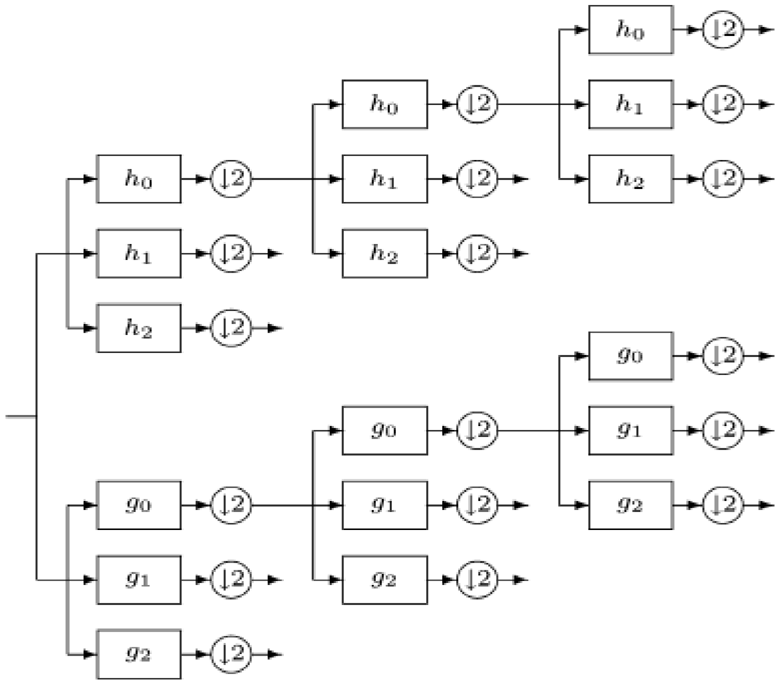
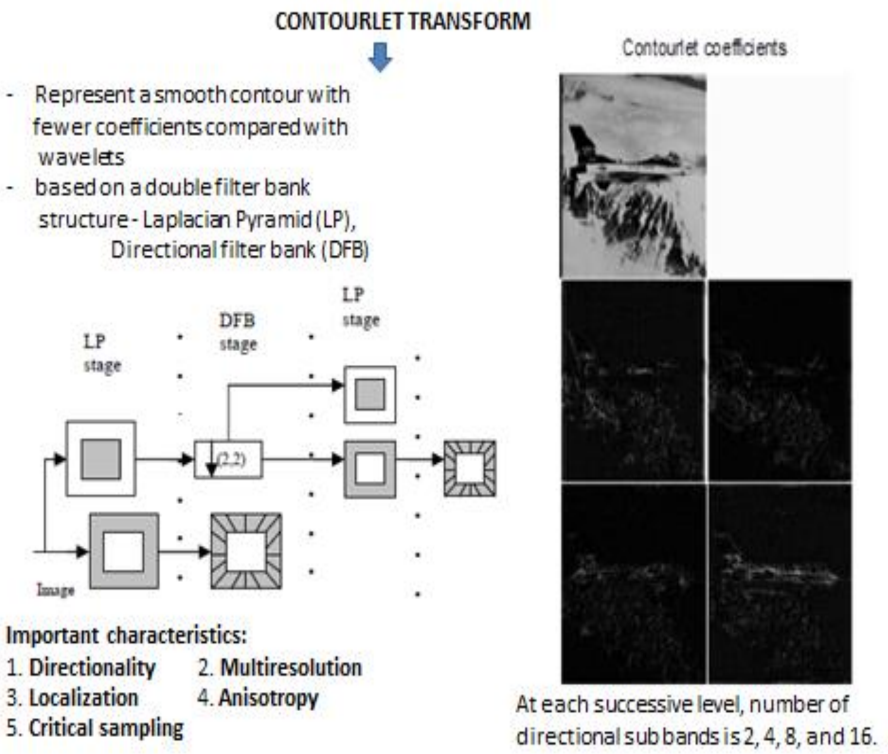
The wavelet transform and wavelet bases are of critical concerns to researchers. Wavelet transforms are most widely-used tool in signal processing due to its inherent mutiresolution representation akin to the operation of the human visual system. The Wavelet transforms provide short windows at high frequencies and long windows at low frequencies but cannot yield a discrete-time basis that is optimal with respect to time localization. The wavelets have poor directional selectivity for diagonal features because the wavelet filters are separable and real. Thus, the wavelet- related research resulted into development of other transforms, known as directional transforms, namely 2-D multiscale transforms Ridgelet, Curvelet and contourlet. These transforms represent edges with different orientations with different subbands more efficiently than the Wavelet transforms. To attains the properties such as shift invariance and directional selectivity ,Kingsbury [6] in 1999 introduced Complex wavelet transform replacing the tree structure of the conventional wavelet transform with a dual tree.

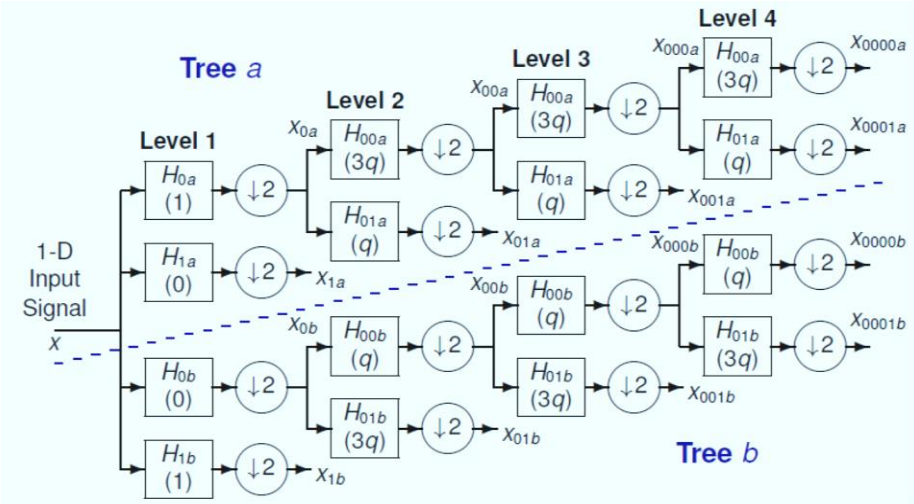
Selesnick [8] have proposed a wavelet- like transform , known as Slantlet transform that can provide better time localization and better signal compression compared to classical Haar-Wavelet transform. He also proposed another complex wavelet transform, namely double-density dual-tree DWT based on double-density DWT and dual-tree DWT. We give a general review of transforms in the Table 2.

Table 2: Basic features of transforms

Transform	Features
DCT	Forward DCT: $F(u,v)=\frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right]$ for $u=0,\ldots,7$ and $v=0,\ldots,7$ where $C(k)=\begin{cases}1/\sqrt{2} & \text{for } k=0\\ 1 & \text{otherwise}\end{cases}$ Inverse DCT : $f(x,y)=\frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}C(u)C(v)F(u,v)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right]$ for $x=0,\ldots,7$ and $y=0,\ldots,7$
WAVELET [2]	**Wavelet Basis** Mother Wavelet $\psi_{j,k}(x)=2^{j/2}\psi(2^{j}x-k).$ Father Wavelet $\psi(x)=\sum_{k\in\mathbb{Z}}g_k\sqrt{2}\phi(2x-k)$ {The set of coefcients $\{g_k\}$ are the high-pass filter coeficients associated with the particular wavelet function being used.} $f(x)=\sum_{k}c_{j_0k}\phi_{j_0,k}(x)+\sum_{k}\sum_{j>j_0}d_{j,k}\psi_{j,k}(x)$ $=c_{0,0}\phi_{0,0}(x)+\sum_{k}\sum_{j>j_0}d_{j,k}\psi_{j,k}(x).$ **Smooth Coeff.=** $c_{j-1,k}=\sum_{n}h_{n-2k}c_{j,n}.$ **Detail Coeff.=** $d_{j-1,k}=\sum_{n}g_{n-2k}c_{j,n}.$ $g_k=(-1)^{k}h_{1-k}.$ *where, j = called dilation or scale parameter, and k= called translation or location*

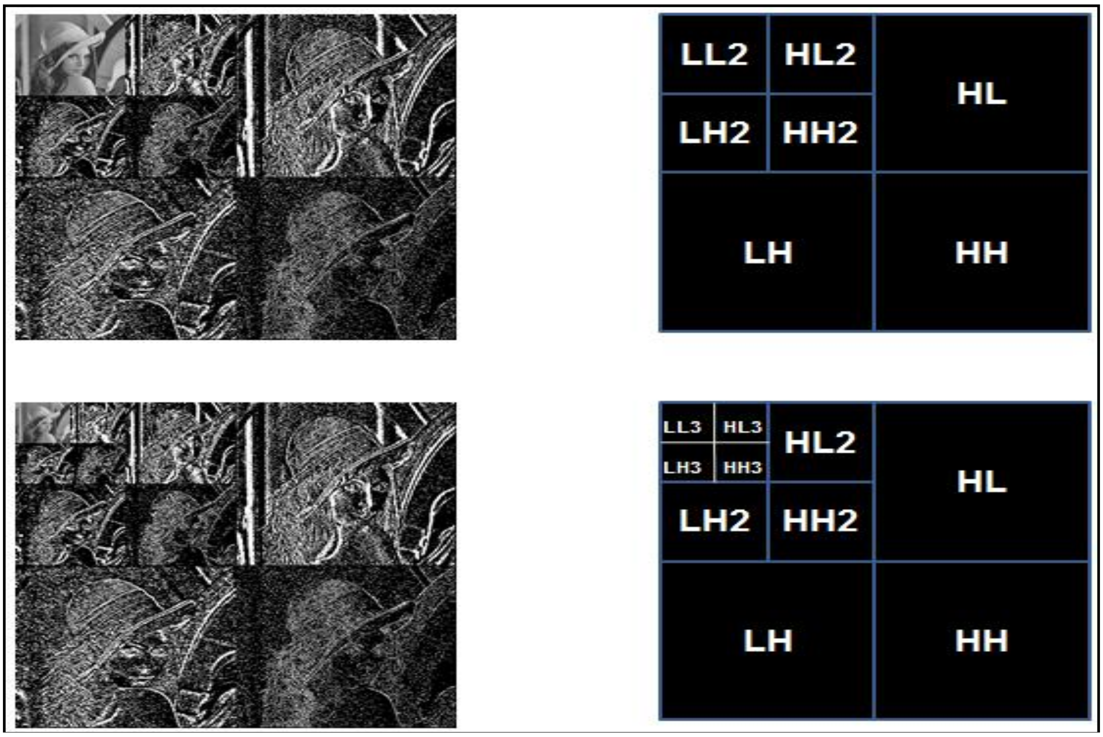
	parameter; h_k are the low-pass wavelet coefficients The **important features of the Real DWT** are **Good compression** of signal energy. **Perfect reconstruction** with short support filters. **No redundancy** – hence orthonormal or bi-orthogonal transforms are possible. **Very low computation** – order-N only. **Demerits:** Severe shift dependence, and Poor directional selectivity in 2-D, 3-D etc.
Slantlet transform (SLT) [8]	**Important Features:** 1. Implemented in form of a parallel structure, employing different filters for each scale 2. Provide exactly a scale dilation factor of 2 and are less frequency selective due to shorter supports of component filters 3. Slantlet filters are of lengths 8 and 4, respectively. 4. Slantlet filters require 2i+1 supports at the ith scale
DD DWT [9]	2-D DD DWT, the cover image is decomposed into nine sub-bands labelled LL, LH1, LH2, H1L, H1H1, H1H2, H2L, H2H1, H2H2, respectively.  
DD DT DWT [10]	There are two types of the 2-D double density dual-tree DWT: 1. The 2-D double density dual-tree real oriented DWT, which is 2 times expansive

<table>
<tr><td></td><td>2. The 2-D double density dual-tree complex oriented DWT, which is 4 times expansive.

</td></tr>
<tr><td>Contourlet transform (CTT) [4]</td><td>The CTT is based on a double filter bank structure by combining the Laplacian Pyramid (LP) with a directional filter bank (DFB).

</td></tr>
<tr><td>Dual Tree</td><td>Features</td></tr>
</table>

Complex Wavelet Transform (DT CWT) [6, 11]	1. Good **shift invariance** = **negligible aliasing**. 2. Good **directional selectivity** in 2-D, 3-D etc. 3. **Perfect reconstruction** with short support filters. 4. **Limited redundancy** –2:1 in 1-D, 4:1 in 2-D The critically decimated 2D DWT outputs three orientational selective sub-bands per level conveying image features oriented at the angles of 90^o , $\pm$ 45^o , and 0^o , the 2D DT-CWT produces six directional subbands per level to reveal the details of an image in $\pm15^o$, $\pm$ 45^o and $\pm$ 75^o directions with 4:1 redundancy 

The Figures 4 to 7 shows the multiresolution decomposition of cover image using different transforms at level 1 and lever 2, respectively.

(a)



(b)

Figure 4:(a) Output of 1-level 2-D decomposition of Lena.jpg, (b) Output of 2-level 2-D decomposition of Lena.jpg

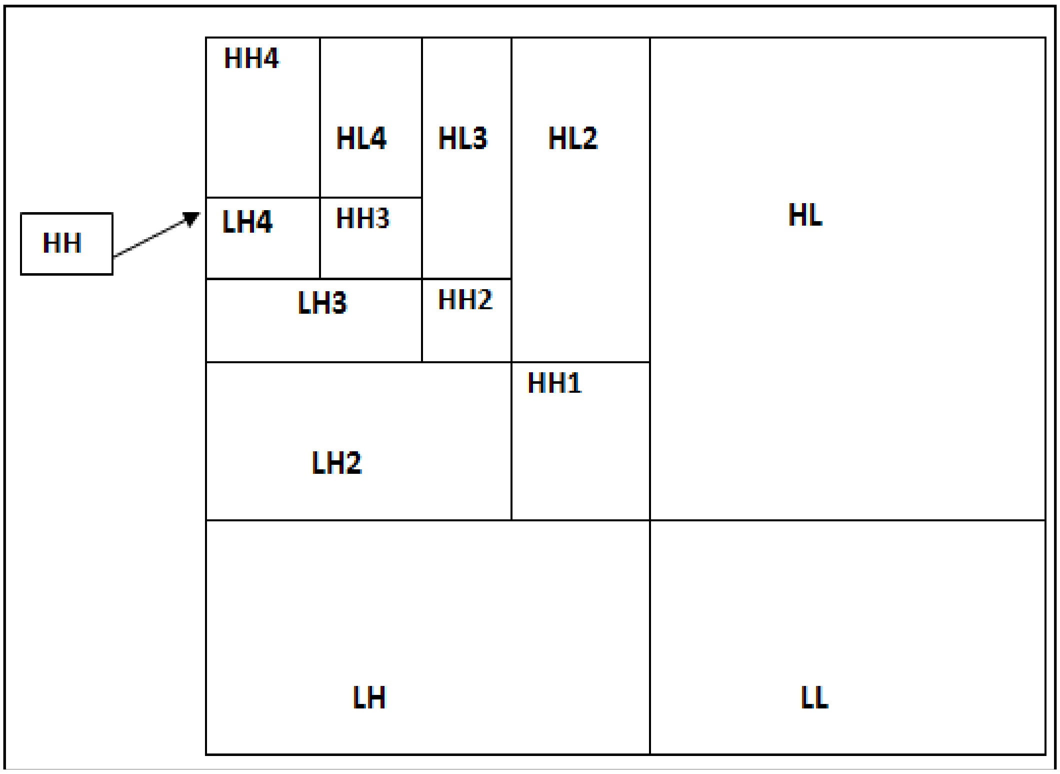


Figure 5: 2-level SLT decomposition of image

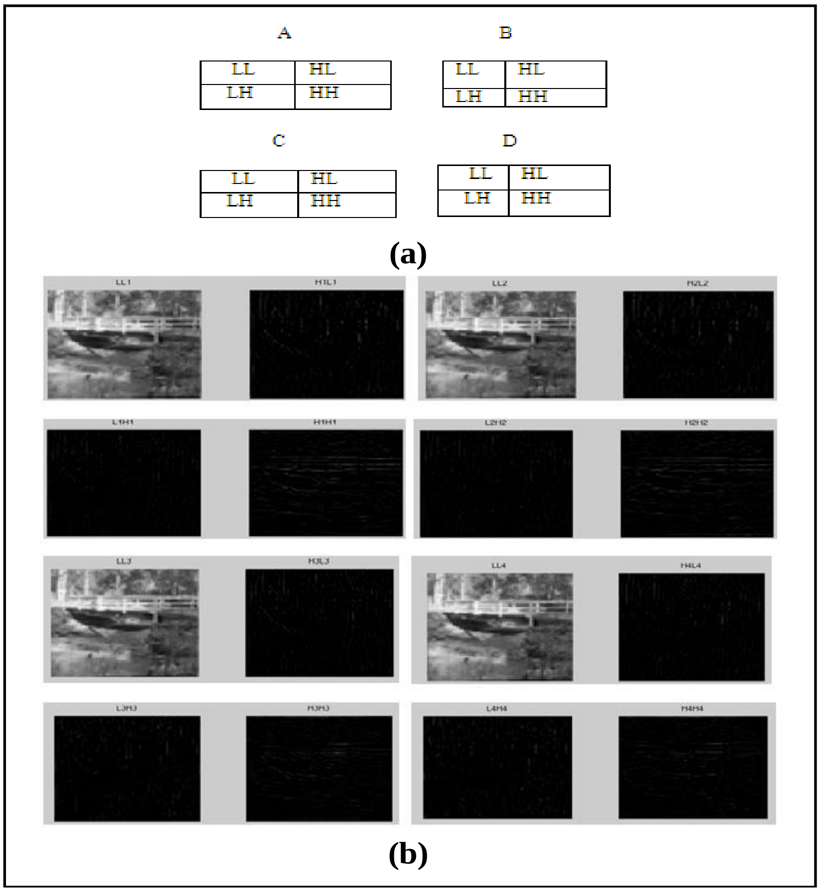


Fig 6: (a) Decomposition types of 2-D DT CWT, (b) 2-D Decomposition of ‘New7.tif’

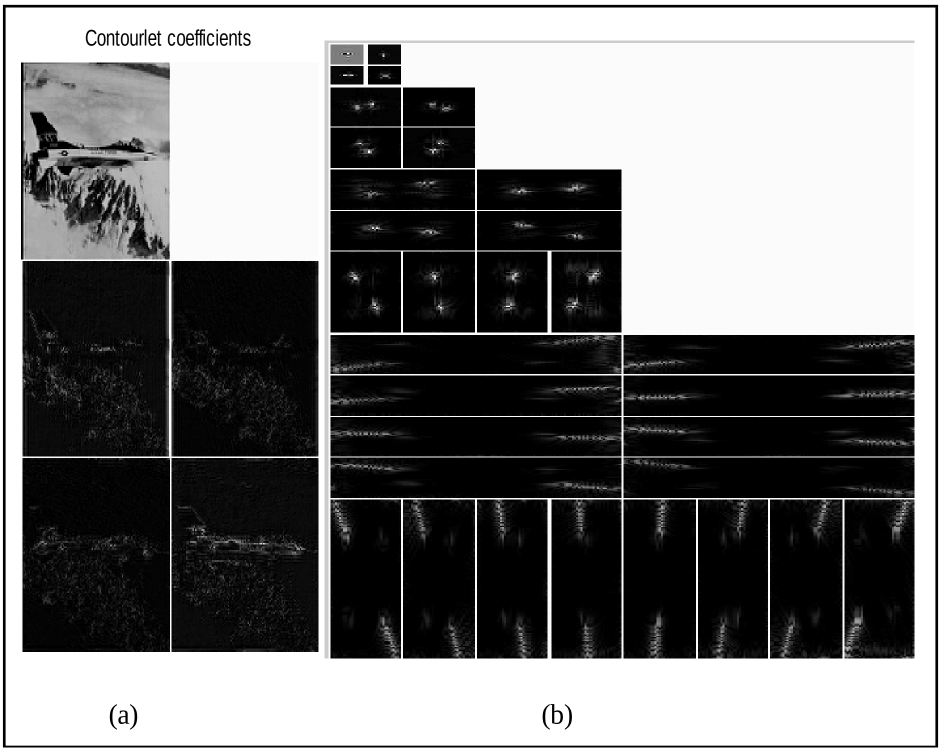


Fig 7: (a) Contourlet decomposition of 1-level, (b) Contourlet basis of level 4, Image: ‘aeroplane.tif’

The characteristics of these transforms are summarized in the Table 3.

Table 3: Characteristics of Transforms

Properties of Transforms	**Wavelet**	**Slantlet**	**Curvelets**	**Contourlet**	**Dual Tree Complex Wavelet**
Multiscale	Yes	Yes	Yes	Yes	Yes
Multi-Resolution	Yes	Yes	Yes	Yes	Yes
Multi-Directional	Contains only fixed number of directional elements-cannot differentiate between opposing diagonal features	It is a wavlet-like transform with two zero moments and better time localization	Yes	Band pass images from the LP are fed into a DFB to capture directional information.	Can have six directional subbands at 15, 75, 45, -15, -75 and -45 and can discriminate between opposing diagonals.
Redundancy Ratio/Facor	O(N) for N level of decomposition	Same as DWT	16J+1, where j is the number of multiscale levels	16J+1, where j is the number of multiscale levels	Little (4:1 for 2-d signals), it is exhibits 2^d (where d is the dimension of the signal being transformed) redundancy compared to a separable (dwt)
Special Feature	Represent images that contain smooth areas separated with edges	Two zero moments and improved time localization	Can detect image activities along curves	Can capture smooth contours in images	Provides shift-invariance and good directional selectivity
Perfect Reconstruction	Yes	Yes	Yes	Yes	Yes
Computing Time	O(n ^{2logn})	Same as Wavelet	O(n)	O(n) for n-pixel images	O(n)
Lacks in Performance	Lacks shift invariance and directionality, fails when edges are smooth curves	Same as DWT	Lacks shift-invariance due to the down-sampling and up-	It is shift-variant. The lack of shift invariance causes pseudo-Gibbs phenomena around	Low redundancy, high computaions

Properties of Transforms	Wavelet	Slantlet	Curvelets	Contourlet	Dual Tree Complex Wavelet
			sampling and could not be implemented in discrrete domain	singularities AND less clear directional geometry/features than Curvelets	
Anisotropicity	Do not describe well highly anisotropic elements	No	Satisfy anisotropy principle	Yes	Yes
Time Localization	Cannot yield discrete-time basis that is optimal with respect to time localization	Provide better time localization	Better than WLT	Improved time localization	Improved time localization
Capacity	Have 3 middle and 1 high frequency subbands at level 2	Same	Higher than WLT	Higher than WLT, 1-stage has 1 low subband and 4 high sub-bands…..	1-stage of 2-D DD DWT has 1 Low subband and 8 High subbands; 1-level of 2-D forward real DD DT DWT has 12 high subbands…..
Compression	Remarkable with small threshold value	Better than DWT	Good for smooth and edge contour objects	Same as Curvelets	Higher rate of compression and lower RMS error as compared with DWT, DCT and others

EMBEDDING SCHEMES

It is generally considered that grayscale images are more suitable than color images for hiding data because the disturbance of correlations between color components may easily reveal the trace of embedding. But the steganographic using color images has attracted researches as the color image provides three times embedding capacity than the grayscale image. Some of the well-known steganographic schemes for gray images are *Modified LSB fixed Mode/ Varying*

Mode [3] and *Reversible Companding technique* [17], and for color images, one of the high bit rate data hiding *scheme known as Wavelet Fusion method* [16] are widely used.

Table 4 : (b: message bit; x: the rightmost bits of pixel value)

Steganographic Schemes	**Embedding/Extraction process**
LSB	$x' = x - x \bmod 2^k + b; b = x \bmod 2^k$ where k is the number of LSBs to be substituted;
Modified (or randomized) LSB (*MLSB*)	Randomized permutation function used to permute the coefficients of detail sub-bands obtained from the cover image before embedding the secret message using LSB technique
MLSB varying mode (MLSB-VM)	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 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.
Reversible companding method	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). If the equation E[C(x)] = x is satisfied, then this kind of Companding could be applied into reversible data hiding.
Wavelet fusion method	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 from 0.0 to 1.0.

PERFORMANCE ANALYSIS

In this section we shall present the analysis of the steganographic techniques in spatial domain and transform domain. The results based on the image steganographic algorithms for the following different schemes are analyzed:

Irreversible schemes in grayscale image using Modified (or randomized) LSB and LSB varying mode,

(i) Irreversible schemes in color image using Fusion technique and

Reversible scheme in grayscale image using thresholding technique.

The performance of these techniques are evaluated according to the widely used metrics: PSNR/WPSNR, CQM, SSIM, KLDiv and Embedding efficiency. The summary of the characteristics of these schemes, for details see [12-15], based on experimental results are given in Table 5.

Table 5:Characteristics of different steganographic schemes (SSIS='Self-Synchronizing Image Steganography')[10]

(*L= 'Low', B='Better than previous schemes', , A='Acceptable for low capacity', LP='Polynomial order of n', QP= 'Polynomial of order n^2' and HP= 'Polynomial of order n^a, $a > 2$', EX='Exponential order', P='Poor', VG= 'Very Good'*

STEGANOGR-APHIC SCHEMES	CHARACTERISTICS					
	PERCEPTI-LITY	*SECUR-ITY*	*CAPAC-ITY*	*UNDETE-CTABI-LITY*	*ROBUST-NESS*	*COMPLXITY*
(M1). Jpeg-jsteg/OutGuess	H	G	L	P	G	QP
(M2).4-bit XOR based on DCT	R	G	R	P	P	QP
(M3).MLSB-FM based on HWLT	G	G	R	P	P	QP
(M4).MLSB-FM based on SLT	G	G	R	P	P	HP
(M5).MLSB-FM based on CTT	G	G	B	P	P	LP
(M6).MLSB-FM based on DD DWT/ DD DT DWT	VG	G	H	G	P	HP
(M7).MLSB-VM based on HWLT	G	G	R	B	P	QP
(M8).MLSB-VM based on SLT	R	G	R	P	B	HP
(M9).MLSB-VM based on CTT	G	G	B	R	P	LP
(M10).MLSB-VM based on DD DWT/	VG	G	H	P	P	HP

DD DT DWT						
(M11).Fusion based on HWLT	G	H	H	P	A	QP
(M12).Fusion based on SLT	R	H	H	P	P	HP
(M13).Fusion based on CTT	H	H	B	P	R	LP
(M14).Fusion based on DD DWT/DD DT DWT	VG	H	H	P	R	HP
(M15).P-RDH based on SLT	R	G	R	R	A	HP
(M16).P-RDH based on CTT	H	G	B	R	A	LP
(M17).P-RDH based on DD DWT/DD DT DWT	R	G	H	R	A	HP
(M18).R-RDH based on SLT	R	G	R	R	A	HP
(M19).R-RDH based on DD DWT/ DD DT DWT	R	G	H	R	A	HP
(M20).Matrix Encoding based on improved Error-Map Technique	H	H	R	G	R	EX
(M21). SSIS based on RS-codes	H	H	R	G	R	HP

We know that the running time of Huffman method is fairly O(n log(n)). The worst case time complexity of 2-D DCT is $O(N^2)$, of 2-D DWT is $O(N^{2\log(N)})$, of SLT is same as of DWT, of CTT is O(N) on N pixels and of CWT, it is double the time taken by DWT, i.e. $O(2N^{2\log(N)})$ Since all the algorithms discussed in the paper are deterministic, we find their complexities as of polynomial order or of exponential order.

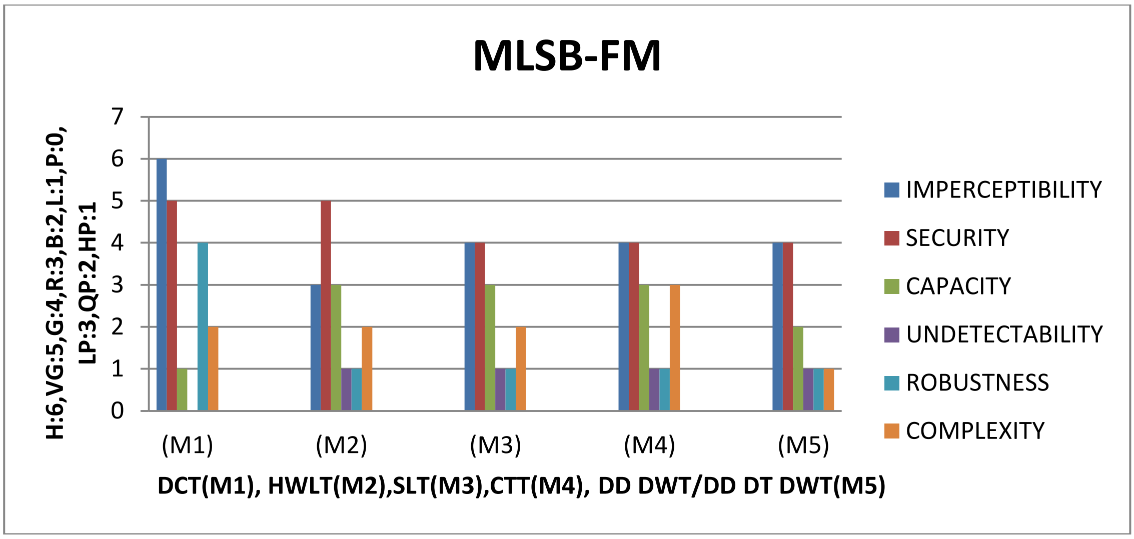


Fig 8: Performance analysis of steganography using the MLSB-FM method

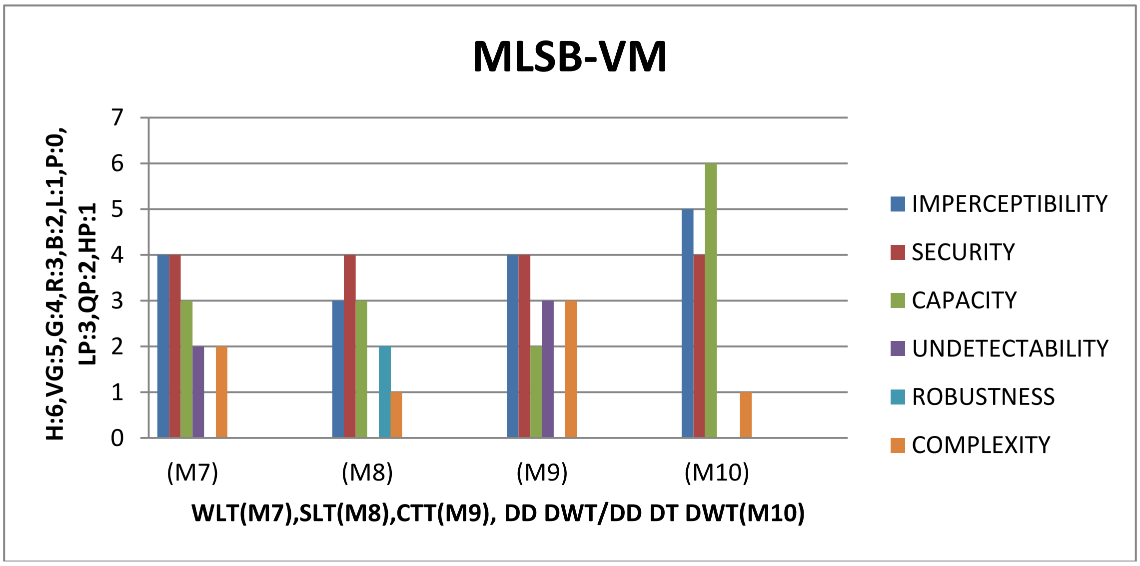


Figure 6.2: Performance analysis of steganography using the MLSB-VM method

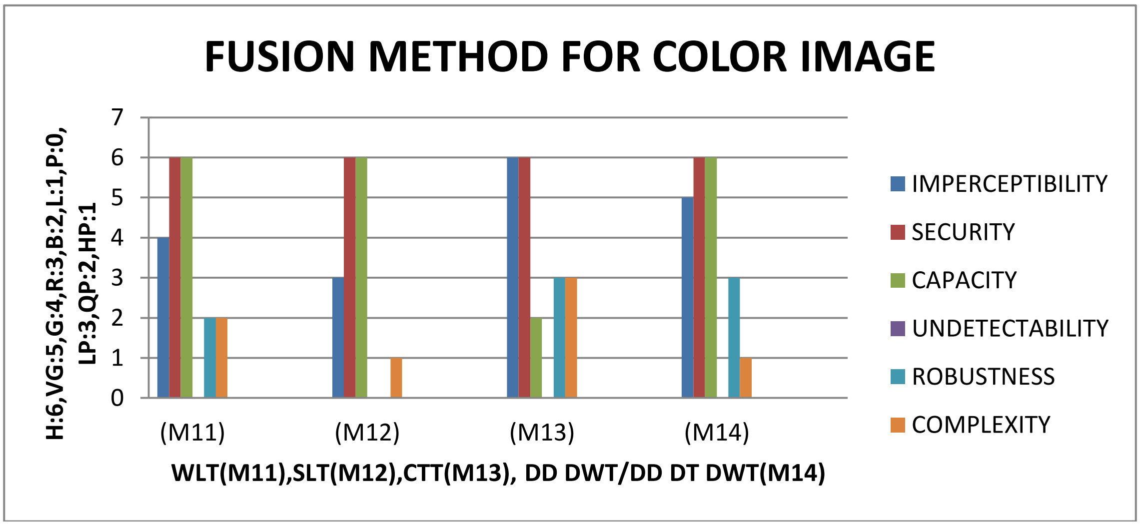


Fig 9: Performance analysis of steganography using the Fusion method

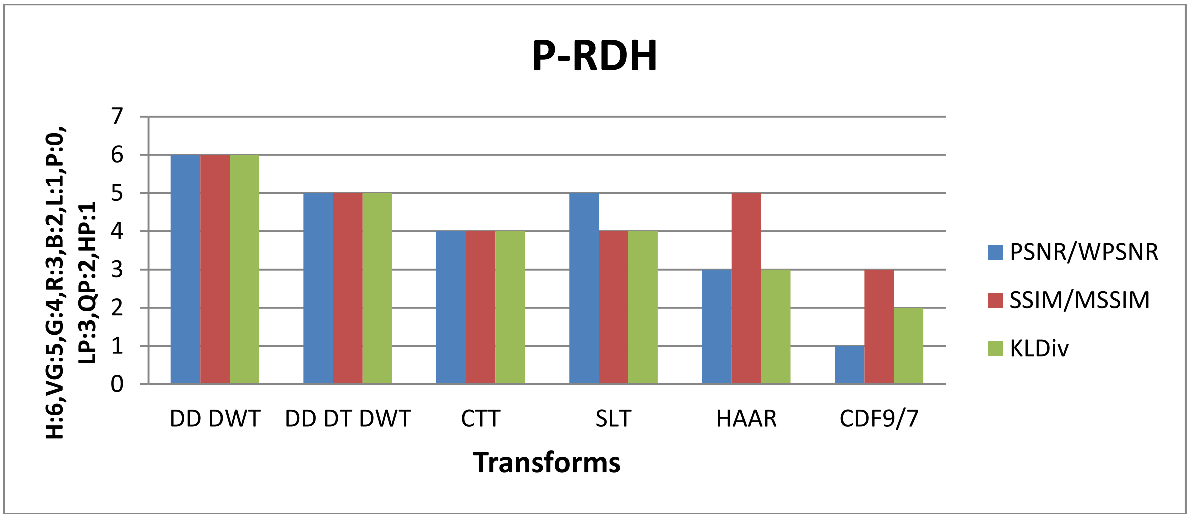


Fig 10: Performance analysis of steganography using the Perceptible-RDH method

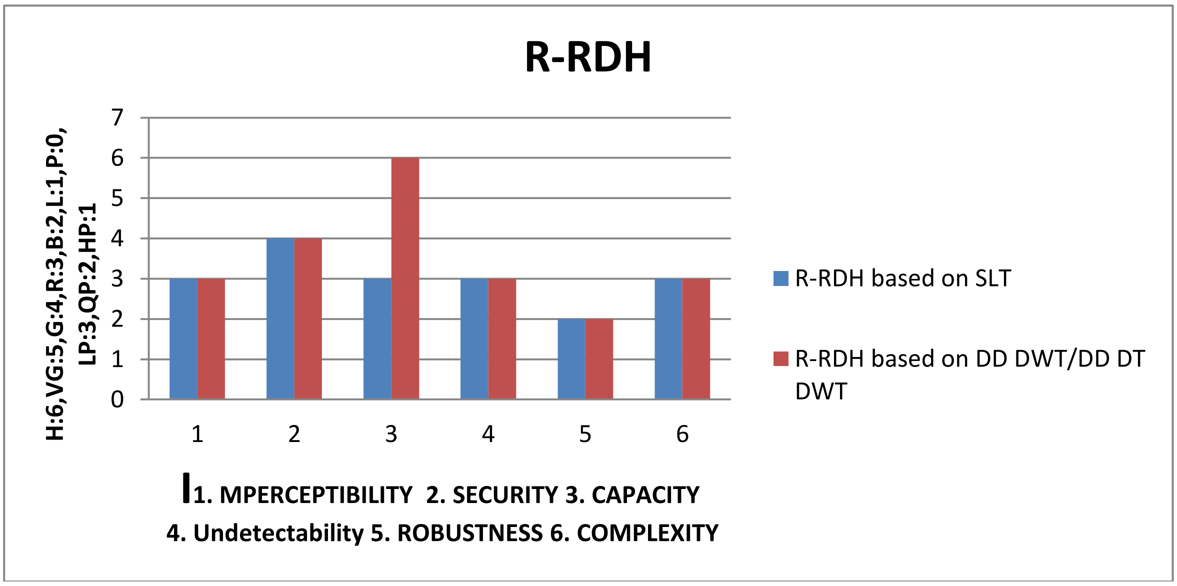


Fig 11: Performance analysis of steganography using the Robust-RDH method

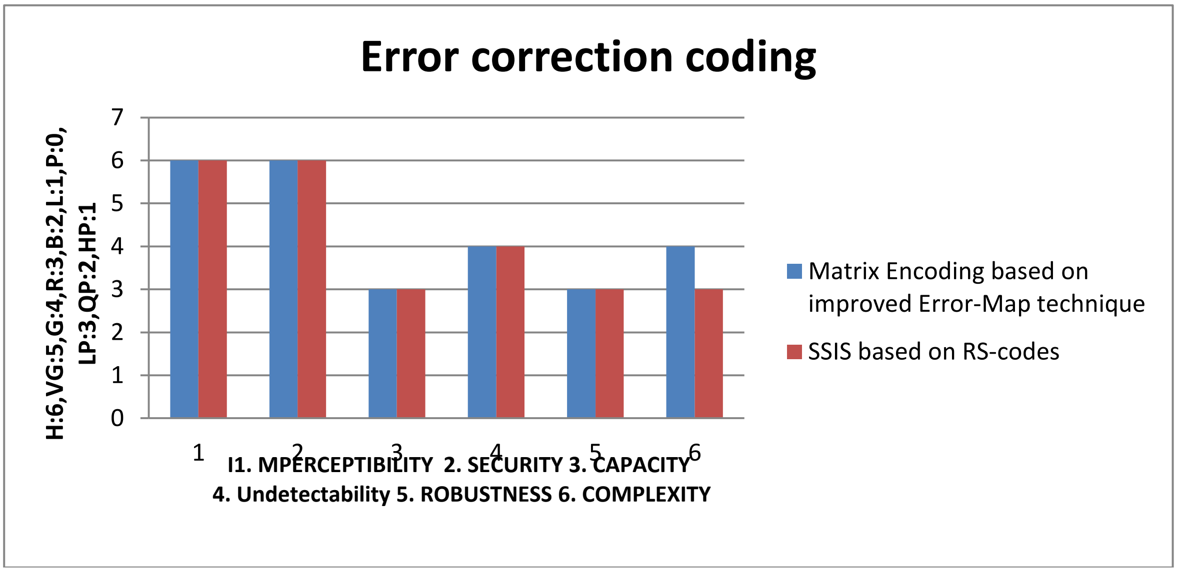


Fig 12: Steganography schemes based on Error correction coding

CONCLUSION

Based on the different techniques discussed in the paper and the performance analysis discussed in the preceding section, we draw the following conclusions:

1. DD-DWT based MLSB-FM method provides much better imperceptibility than other transforms and hence is better option for achieving good image quality. Also, DD DWT and DD DT DWT based MLSB-FM algorithms shows excellent result of structural similarity of images.

2. DD DWT outperforms to other transforms in terms of imperceptibility

The order in which different transforms performs in terms of imperceptiblity is

SLT < CTT < Haar < DD DT DWT < DD DWT

3. For DD DWT based MLSB-VM method, the maximum/median of KLDiv is obtained as almost zero for the bpp upto 0.17 and then it slightly increases but remains in the range (0, 4.5 $x10^{-4}$). The same observation is see for other transforms also, i.e., the maximum values of KLDiv remains constant till the bpp is ≈ 0.17 and then increases as bpp increases.

4. DD DT DWT and DD-DWT give better imperceptibility for alpha = 0.05. As the value of alpha is lowered, higher imperceptibility observed at the loss of embedding rate. DD DWT and DD DT DWT also provide higher payload for embedding than other transforms at the cost of complexity.

5. The imperceptibility is found to be better in the SLT based reversible thresholding algorithm than DWT based reversible thresholding method.

6. The DD DT DWT is a better option than DWT for the steganography system as it provides not only better imperceptibility but also provides more embedding capacity.

7. Image steganography based on RS-codes satisfy the criteria of imperceptibility.

8. Robust and Secure image steganography based on Matrix Encoding shows better security than the existing methods. RS-codes make our technique robust against channel errors. The application of RS-codes enables us recover burst errors, which is very beneficial in steganography, in which the media object may undergo some changes while in transit.

REFERENCES

[1] Amirtharajan R. Qin J. and Rayappan J. B. B., 2012. Random Image Steganography and Steganalysis: Present Status and Future Directions, Information Technology Journal*, 11: 566-576.*

[2] Calderbank A. R., Daubechies I., Sweldens W. and Yeo. B. ,1998. Wavelet transforms that map integers to integers, Applied and Computational Harmonic Analysis, Vol.5, no. 1, 332-369.

[3] Chen Po-Yuch and Lin Hung-Ju , 2006. A DWT Based approach for Image Steganography, International Journal of Applied Science and Engineering, Vol. 4, no. 3: 275-290.

[4] Do M.N. and Vetterli M., 2005. The Contourlet transform: An efficient directional multiresolution image representation, IEEE Trans. On Image Processing, 14(12), 2091-2106.

[5] Fridrich J., 1998. Applications of Data Hiding in Digital Images, Tutorial for the ISPACS 1998 Conference in Melburne, Australia.

[6] Kingsbury N.G., 2000, September. The dual-tree complex wavelet transform with improved orthogonality and symmetry properties, International Conference on Image Processing Vol. 2, 10-13, 375-378.

[7] Ortiz John A. (2012). An introduction to more advanced steganography, bh-as-11-ortiz-Steganography WP.pdf, Black hat USA.

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

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

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

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

[12] Sushil Kumar, 2013, December. Data Hiding in Digital Images using Steganography, Ph.D. Thesis, University of Delhi, Delhi.

[13] Sushil Kumar, 2014. A comparative study of transform based secure image steganography, International Conference on Communication and Network Security(ICCNC 2014), Milan, Italy, Published in IJCCE, San Bernardino, CA 92405.

[14] Sushil Kumar, 2017. Fusion based Image Steganography for Digital Colour Image, National Conference on Challenges and Opportunities in Computer Engineering (NCCOCE'17), Christ University, Bengaluru, India.

[15] Sushil Kumar, 2017. Data Hiding using Slantlet Fusion method and T-codes, Journal of Information, Communication and Intelligence Systems (JICIS).

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

[17] Xuan G.,.Shi Y.Q., Yang C., Zhang Y., Zou D. and Chai P., 2002, Dec. 9-11, Lossless Data Hiding using integer wavelet transform and threshold embedding technique, in Proceeding of IEEE International Workshop on Mutimedia Signal Processing, Marriott Beach Resort ST. Thomas, US Virgin Islands.