# Curvelet Transform Based Data Hiding Approach for Color Images

**V.Perathuselvi ,**
Assistant professor,
Dept of Computer Science Engineering,
Francis Xavier Engineering College,
Tirunelveli,Tamil Nadu,India.

**M.Santhana Arumuga Sankari ,**
M.E., Computer Science Engineering,
Francis Xavier Engineering College,
Tirunelveli,Tamil Nadu,India.
msankarishree@gmail.com

*Abstract*— **The main objective of this project is to develop a novel approach for hiding the data through Steganography. Steganography is a one of the method which is used for information hiding. In Steganography, the secret message is to embedded into the image and then this embedded image is used for further sending purpose. This Steganography technique is used to protect the secret message from the eavesdroppers. To do Steganography this project a novel approach. First the cover image is divided into blocks and then the prediction algorithm is applied to each block to find the blocks which contains the texture information. The prediction error helps to find out the texture blocks. These blocks only used to embed the secret message for providing high visual perception. Not only that in this paper multilayer security is also included. Before embed the secret message the encryption technique is applied and then the encrypted message is collapsed for avoiding attacks. In this paper the embedding process is done on the curvelet transform. It increases the payload and the quality of the embedded image. The curvelet transform is applied on the detected blocks and then normalization process is applied and then the collapsed secret image bit is fused with the curvelet normalized curvelet coefficients. Finally the inverse curvelet transform and denormalization is applied to get the embedded image. In extracting these process is done in reverse manner. This novel scheme provides the high embedding capacity. Not only that this process provides high recovery rate also. So the recovered image is exactly same as the original source texture. From the experimental results it is shown that the proposed approach performs better than the existing approaches.**

***Keywords—Block Dividing; Prediction;Prediction Error;Curvelet Transform; Embedding Process;Extraction Process;Fusion;Stego Image***

## I. INTRODUCTION

In the last decade the development in technology and networking has created serious threats to obtain secured data communication. This has motivated the interest among computer security researchers to overcome the serious threats for secured data transmission. One method of providing more security to data is information hiding. Steganography is a singular method of information hiding techniques. Steganography is a technique to hide information in ways that prevent the detection of hidden messages. It uses digital media as carriers for secret communication. It embeds messages into a host medium in order to conceal secret messages so as not to arouse suspicion by an eavesdropper. Cryptography and Steganography are not one and the same. While Cryptography scrambles a message so that it cannot be understood, Steganography hides the messages so that it cannot be seen. Un-detectability, Robustness and capacity of the hidden data are the main features that differentiate steganography from cryptography. In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, cipher text or images etc. The steganography method provides embedded data in an imperceptible manner with high payload capacity. Encrypting data provides data confidentiality, authentication, and data integrity.

An Many research works have been carried out on LSB based Steganography. Different researchers employed different techniques for the purpose of hiding secret data in a cover image. Following are the few related works carried out by various research groups. Some of the major techniques used in the field of Image Steganography are mentioned below. Some trivial algorithms utilizing the techniques are also listed. Neil F. Johnson and sushil jajodia et al., [1] have provided several characteristics in information hiding methods to identify the existence of a hidden messages and also identify the hidden information. The images are reviewed manually for hidden messages and steganographic tool to automate the process. The developed tool is to test robustness of information hiding techniques in images such as warping, cropping rotating and blurring. Lisa M. Marvel and Charles T. Retter [2] have presented a method of embedding information within digital images, called Spread Spectrum Image Steganography (SSIS). SSIS conceals a message of substantial length with in digital images while maintaining the original image size and dynamic range. A hidden message can be recovered using the appropriate keys without any knowledge of the original image.

Giuseppe Mastronardi et al., [3] have studied the effects of Steganography in different image formats (BMP, GIF, JPEG and DWT) and proposed two different approaches for lossless and lossy image. They are based on the creation of an "adhoc" palette for BMP and GIF images. LUI Tong and QIU Zheng-ding [4] have proposed a Quantization-based Steganography scheme. In this method the secret message is hidden in every chrominance component of a color image and the hiding capacity is higher than that of the popular Steganography software. Since the Quantization-based hiding method is free from the interference and simulation results the hidden message can be extracted at low BER and our scheme is robust to common attacks. M. Mahdavi et al., [9] presented a steganalysis method for the LSB replacement. The method is based on the changes that occur in histogram of an image after the embedding of data. It is less complex and more accurate than the RS steganalytic method for the images which are acquired directly from scanner without any compression.

The RS method needs to count the number of regular and singular groups twice and also require LSB flipping for the whole image. This method has better average and variance of error comparing to RS steganalytic method. Shilpa p. Hivrale et al., [10] have presented various statistical measures and PMF based method of detection. It uses the frequency count of the pixel intensities in the image to test for the detection of stego image or not. Here LSB embedding technique is used. K. B. Raja et al., [11] have proposed a novel image adaptive stegnographic technique in the integer wavelet transform domain called as the Robust Image Adaptive Steganography using Integer Wavelet Transform. According to information theoretic prescriptions for parallel Gaussian models of images, data should be hidden in low and mid frequencies ranges of the host image, which have large energies. Jan Kodovsky and Jessica Fridrich [12] worked out the specific design principles and elements of steganographic schemes for the JPEG format and their security. The detect ability is evaluated experimentally using a state of art blind steganalyser. L.Y. Por et al., [13] have proposed a combination of three different LSB insertion algorithms on GIF image through stegcure system. The unique feature about the stegcure is being able to integrate three algorithms in one Steganography system. By implementing public key infrastructure, unauthorized user is forbidden from intercepting the transmission of the covert data during a communication because the stegokey is only known by the sender and the receiver.

Gaetan Le Guelvoit [14] proposed a work which deals with public- key Steganography in presence of passive warden. The main aim is to hide the secret information within cover documents without giving the warden any clue and without any preliminary secret key sharing. This work explores the use of trellis coded quantization technique to design more efficient public key scheme. Mohammad Ali Bani Younes and Aman Jantan [15] have proposed a steganographic approach for data hiding. This approach uses the least significant bits (LSB) insertion to hide data within encrypted image data. The binary representation of the data is used to overwrite the LSB of each byte within the encrypted image randomly. The hidden data will be used to enable the receiver to reconstruct the same secret transformation table after extracting it and hence the original image can be reproduced by the inverse of the transformation and encryption processes.

Chang-Chu Chen and Chin-Chen Chang [16] have proposed that data hiding scheme is a modification of the LSB-based steganography using the rule of reflected gray code. The embedding ability and distortion level of our novel method are similar to those of the simple LSB substitution scheme. The difference is that the LSBs of stego-image are not always the same as the secret bits while the simple LSB substitution keeps them equally. Babita Ahuja and, Manpreet Kaur [17] have presented LSB based steganography algorithm with high data hiding capacity, as four LSB's are used to hide data, high confidentiality as distortions which can cause suspicions for the intruders, are removed through filtering techniques and two level high security is applied. Debnath Bhattacharyya et al., [18] a security model is proposed which imposes the concept of secrecy over privacy for text messages. The proposed model combines cryptography, steganography and along with an extra layer of security has been imposed in between them. Chin-Chen Chang et al.,[19] proposed a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on wet paper coding

In this paper first the cover image is divided into blocks and then the prediction algorithm is applied to each block to find the blocks which contains the texture information. The prediction error helps to find out the texture blocks. These blocks only used to embed the secret message for providing high visual perception. Not only that in this paper multilayer security is also included. Before embed the secret message the encryption technique is applied and then the encrypted message is collapsed for avoiding attacks. In this paper the embedding process is done on the curvelet transform. It increases the payload and the quality of the embedded image. The curvelet transform is applied on the detected blocks and then normalization process is applied and then the collapsed secret image bit is fused with the curvelet normalized curvelet coefficients. Finally the inverse curvelet transform and denormalization is applied to get the embedded image. In extracting these process is done in reverse manner.

The remainder of this paper is organized as follows. The embedding and extraction process are discussed in Section II. Section III describes the experimental results and performance evaluation of the proposed method. Finally, Section VI concludes the paper.

## II. Proposed Method

The proposed method contains two main modules. They are embedding and extraction. The overall block diagram of the proposed method is shown in Fig.1. In embedding process the cover image and the secret message is given as the input. And the stego image is produced as the output. In extraction process the stego image is given as the input image and the secret message is produced as the output. This process is explained in very detailed manner in Fig.2 and Fig.3.

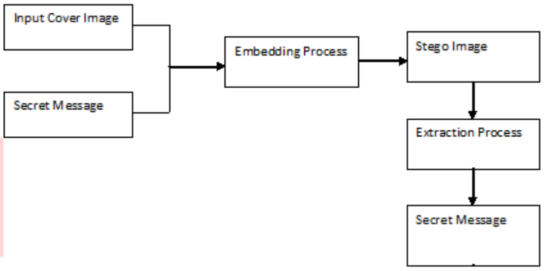


Fig.1. Overall Block Diagram

### A. *Embedding Procedure*

The embedding process is used to produce the stego image. To do this first the cover image is divided into blocks and then the prediction algorithm is applied to each block to find the blocks which contains the texture information. The prediction error helps to find out the texture blocks. These blocks only used to embed the secret message for providing high visual perception. Then these blocks are collapsed for providing additional security. And then the secret message is encrypted using the  encryption technique is applied to produce multilayer security and then the encrypted message is collapsed for avoiding attacks. After that the curvelet transform is applied on the detected blocks and then normalization process is applied and then the collapsed secret image bit is fused with the curvelet normalized curvelet coefficients. Finally the inverse curvelet transform and denormalization is applied. And then the blocks are combined to get the stego image.

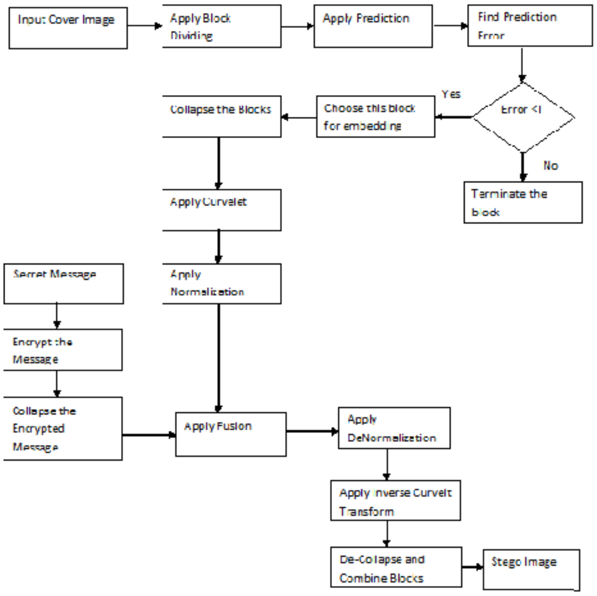


Fig. 2. Process Flow Diagram of Embedding

*1. Block Dividing*

This is the first step of the embedding process. The original cover image sized $M \times N$ as **I**, and it is divided into the non-overlapping $n \times n$ blocks. For simplicity, assume that $M$ and $N$ can be divided by $n$ with no remainder. Denote all $k$ divided blocks in raster scanning order as $\mathbf{B}i, j$, where $k = M \times N/ n2$, $i = 1, 2, \ldots, M/n$, and $j = 1, 2, \ldots, N/n$.

*2. Prediction and Prediction Error*

After block dividing the next step is to find the texture information block. To identify this the interpolation method is used. For do this take the current processing block as Bx,y and its left blocks are Bx,y−1 and upper blocks Bx−1,y, respectively. To find the average value of these two blocks and calculate the difference value of interpolated blocks and the current processing blocks. Then compare the difference value with the threshold value. If the difference value is greater than the threshold value the block contains the structure information so eliminate these blocks. Otherwise the block contains the texture information. These blocks are considered as the embedding blocks.

*3. Multilayer Security*

In this paper the multilayer security is provided. To do this the blocks which are used detected as the embedding blocks are collapsed. And the secret image is also encrypted and it also collapsed to provide more security.

*4. Embedding on Curvelet Transform*

After collapse the blocks then apply the curvelet transform on it. Before apply the curvelet transform the normalization process is applied. After applying the curvelet transform and then the encrypted secret bit is fused with the curvelet transform. Finally the inverse curvelet transform to get the stego image.

*B. Extraction Procedure*

The extraction process is used to get the original secret message from the stego image. To do this first the stego image is divided into blocks and then the prediction algorithm is applied to each block to find the blocks which contains the texture information. The prediction error helps to find out the texture blocks. These blocks only used to extract the secret message for providing high visual perception. Then these blocks are collapsed for providing additional security. After that the curvelet transform is applied on the detected blocks and then normalization process is applied and then extract the secret image bit. Finally these message bit is decrypted to get the original secret message. The overall algorithm of the proposed method is shown below.

*5. Proposed Algorithm*

The overall algorithm of the proposed method is described below.

1. First get the cover image as input
2. And then divide the image into non overlapping blocks
3. Apply the prediction on to each block
4. And then calculate the prediction error from the original and predicted blocks
5. Compare these error value with the threshold to find out the texture information of these blocks
6. If the error value is greater than the threshold the block is terminated because it contains structure information.
7. Otherwise the block is considered as the embedding blocks because it contains the texture information.
8. And then these blocks are collapsed to provide the additional security.
9. And then get the secret message which is to be embedded.
10. Apply the encryption on to the secret message to provide the multilayer security.
11. And then these encrypted message are collapsed
12. Finally apply the curvelet transform on to the selected blocks and then apply the fusion.

13. Apply the inverse curvelet transform and block combining to produce the stego image
14. In stego image apply the step 2-8 steps
15. And then apply the steps curvelet transform and perform defusion to extract the secret message
16. Finally apply the decryption and decollapse to get the original secret message.

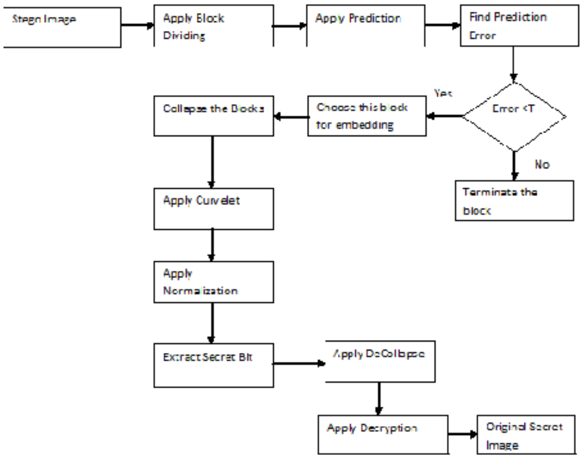


Fig. 3. Process Flow Diagram of Extraction

## III. EXPRIMENTAL RESULTS

### A. *Expiremental Images*

Experiments were conducted on a group of color images to verify the effectiveness of the proposed scheme. For the experimental purpose several standard, 512 × 512 cover images are taken. Some of these images , i.e., Lena, Barbara, Babbon, Peppers, Sailboat, and Tiffany, are shown in Figure 4. The sizes of the divided non-overlapping image blocks are set to 4 × 4, i.e., n = 4 for the experiments.

Lena Barbra

Babbon Peppers

Boat Building

Fig. 4. Expiremental Images

### B. Performance Analysis

To evaluate the performance of the steganography techniques several performance metrics are available. This paper uses the PSNR,SSIM, MSE and RMSE to analyses the performance.

*1. Peak Signal-to-Noise-Ratio*

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between the stego image and the original image. The PSNR formula is defined as follows:

$$PSNR = 10 \times \log 10 \frac{255 \times 255}{\frac{1}{H \times W} \sum_{x=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2} dB$$

where H and W are the height and width of the image, respectively; and f(x,y) and g(x,y) are the grey levels located at coordinate (x,y) of the original image and attacked image, respectively.

*2. Structural Similarity Index*

The structural similarity index is a method for measuring the similarity between the stego image and the original image.

$$SSIM\ (y, \hat{y}) = \frac{\left(2_{\mu_y \mu_{\hat{y}}} + c_1\right)(2\sigma_{y\hat{y}} + c_2)}{\left(\mu_y^2 + \mu_{\hat{y}}^2 + c_1\right)(\sigma_y^2 + \sigma_{\hat{y}}^2 + c_2)}$$

where, $\hat{Y}$ is the stego image, the Y is the original image, μ is the mean and the is the variance.

*3. Mean Square Error*

The mean square error (MSE) is used to evaluate the difference between a stego image and the original image. The MSE can be calculated by,

$$MSE = \frac{1}{n} \sum_{i=1}^{n} (\hat{Y}_i - Y_i)^2$$

where, $\hat{Y}$ is the stego image and the Y is the original image.

*4. Root Mean Square Error*

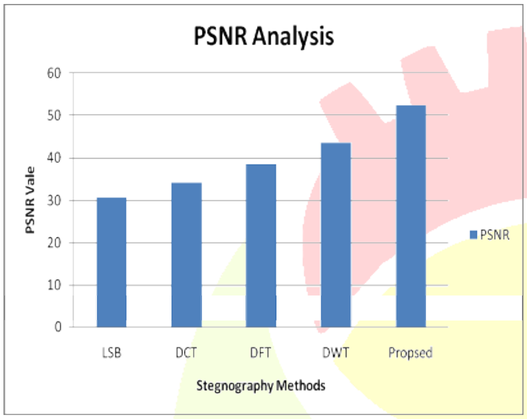
The Root Mean Square Error (RMSE) is a frequently used measure of the difference between stego image values and the original image values.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n} (\hat{Y}_i - Y_i)^2}{n}}$$

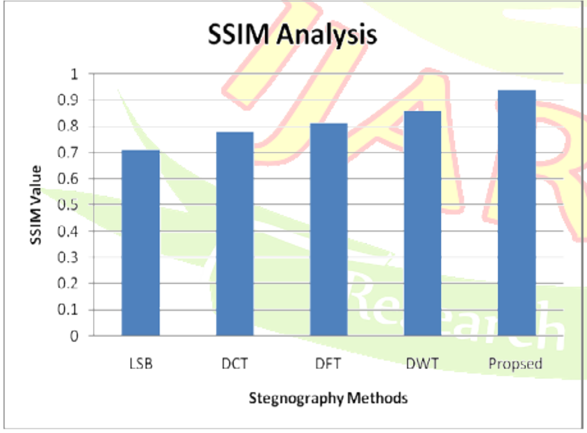
where $\hat{Y}$ is stego image and Y is original image.

To analysis the performance of the proposed system, it is compared with various techniques by using the performance metrics which are mentioned above. This is shown in the below tables and graphs.

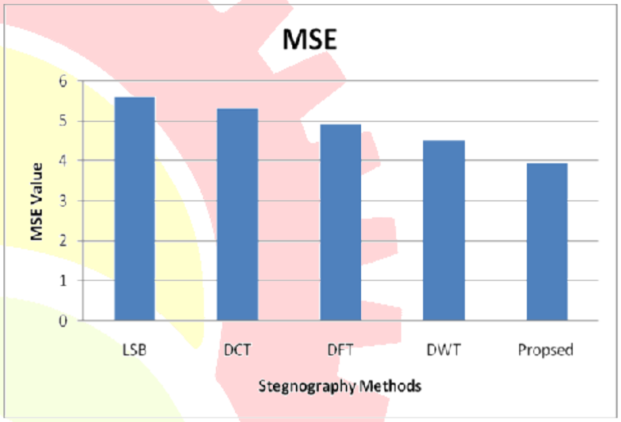
| ***Methods*** | ***PSNR*** |
|---|---|
| LSB | 30.58 |
| DCT | 34.24 |
| DFT | 38.56 |
| DWT | 43.64 |
| Propsed | 52.42 |



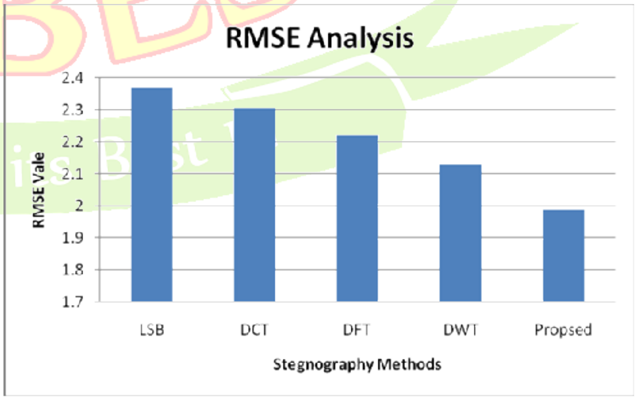
| *Methods* | *SSIM* |
|---|---|
| LSB | 0.71 |
| DCT | 0.78 |
| DFT | 0.81 |
| DWT | 0.86 |
| Propsed | 0.94 |



| *Methods* | *MSE* |
|---|---|
| LSB | 5.61 |
| DCT | 5.32 |
| DFT | 4.93 |
| DWT | 4.53 |
| Propsed | 3.95 |



| *Methods* | *RMSE* |
|---|---|
| LSB | 2.36854386 |
| DCT | 2.30651252 |
| DFT | 2.22036033 |
| DWT | 2.12837967 |
| Propsed | 1.98746069 |



## IV. CONCLUSION

In this paper a novel approach for hiding is proposed. In the novel approach the prediction algorithm is applied to find the texture information. The prediction error is also applied to find out the texture blocks. In this paper multilayer security is also included. Before embed the secret message the encryption technique is applied and then the encrypted message is collapsed for avoiding attacks. In this paper the embedding process is done on the curvelet transform. It increases the payload and the quality of the embedded image. The curvelet transform is applied on the detected blocks and then normalization process is applied and then the collapsed secret image bit is fused with the curvelet normalized curvelet coefficients. Experimental results shows that the proposed method performs better than the existing approaches.

## REFERENCES

[1] Neil F. Johnson and Sushil Jajodia, "Steganalysis: The Investigation of Hidden Information," IEEE conference on Information Technology, pp. 113-116, 1998.

[2] Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," IEEE conference on Military communication, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.

[3] Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, "Steganography Effects in Various Formats of Images. A Preliminary Study," International Workshop on Intelligent data Acquisition and Advanced Computing Systems: Technology and Applications, pp. 116-119, 2001.

[4] LIU Tong, QIU Zheng-ding "A DWT-based color Images Steganography Scheme" IEEE International Conference on Signal Processing, vol. 2, pp.1568-1571, 2002.

[5] Jessica Fridrich, Miroslav Goijan and David Soukal, "Higher-order statistical steganalysis of palette images" Proceeding of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia ContentsV, vol. 5020, pp. 178-190, 2003.

[6] Jessica Fridrich and David Soukal, "Matrix Embedding for Large Payloads" SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents , vol. 6072, pp. 727-738. 2006.

[7] Yuan-Yu Tsai, Chung-Ming Wang "A novel data hiding scheme for color images using a BSP tree" Journal of systems and software, vol.80, pp. 429-437, 2007.

[8] Jun Zhang, Ingemar J. Cox and Gwenael Doerr.G "Steganalysis for LSB Matching in Images With High-frequency Noise" IEEE Workshop on Multimedia Signal Processing, issue 1-3, pp.385- 388, 2007.

[9] M. Mahdavi, Sh. Samavi, N. Zaker and M. Modarres-Hashemi, "Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram," Journal of Electrical and Electronic Engineering, vol. 4, no. 3, pp. 59-70, 2008.

[10]Shilpa P. Hivrale, S. D. Sawarkar, Vijay Bhosale, and Seema Koregaonkar "Statistical Method for Hiding Detection in LSB of Digital Images: An Overview World Academy of Science, Engineering and Technology, vol. 32, pp. 658-661, 2008.

[11]K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal, L. M. Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets" International conference on Communication Systems Software, pp. 614-621, 2008.

[12]Jan Kodovsky, Jessica Fridrich "Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain" Proceedings of SPIE, the International Society for Optical Engineering, vol. 6819, pp. 681902.1-681902.13, 2008.

[13] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, B. Delina, "StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme," Journal of WSEAS Transctions on Computers, vol. 8, pp. 1309-1318, 2008.

[14]Gaetan Le Guelvouit, "Trellis-Coded Quantization for Public-Key Steganography," IEEE International conference on Acostics, Speech and Signal Processing, pp.108-116, 2008.

[15]Mohammed Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion," International Journal of Computer Science and Network Security, vol. 8, no. 6, pp.247-257, 2008.

[16]Chang-Chu Chen, and Chin-Chen Chang, "LSB-Based Steganography Using Reflected Grey Code," The Institute of Electronics, Information and communication Engineers Transaction on Information and System,", vol. E91-D (4), pp. 1110-1116, 2008.

[17]Babita Ahuja and, Manpreet Kaur, "High Capacity Filter Based Steganography," International Journal of Recent Trends in Engineering, vol. 1, no. 1, pp.672-674, May 2009.

[18]Debnath Bhattacharyya, Poulami Das, Samir kumar Bandyopadhyay and Tai-hoon Kim, "Text Steganography: A Novel Approach," International Journal of Advanced Science and Technology, vol.3, pp.79-85, February2009.

[19]Chin- Chen Chang, Yung- Chen Chou and Chia- Chen Lin, "A steganography scheme based on wet paper codes suitable for uniformly distributed wet pixels," IEEE International Symposium on circuits and Systems, pp. 501-504, 2009.