A review paper on Cryptography and Image steganography

Preeti Barot[1], Vikas Sharma[2], Ashish Kulshrestha[3]
Assistant professor ,Department of Electronics & Communication
Jaipur Engineering College & Research Centre, Jaipur

{ preetibarot.ece@jecrc.ac.in[1]| Vikassharma.ece@jecrc.ac.in[2],
|ashishulshrestha.ece@jecrc.ac.in[3]**}**

***Abstract*— Invisible Image Steganography is secret embedding scheme for hiding of secret image into cover image file and the purpose of invisible steganography is secret data communication and copyrights protection. Image Steganography have research challenges for increasing robustness against visual attacks and statistical attacks. Wavelet transformation based Image Steganography techniques provide better robustness for statistical attacks in comparison to Discrete Cosine Transform domain and Spatial Domain based Image Steganography. The combined technique of DWT and DCT provides advantages of both techniques. We have proposed 4x4 block based dwt-dct transformation steganography scheme which provide better imperceptibility for gray scale and colored images both.**

Keywords—Block, DWT, DCT, Steganography, Hiding

I. INTRODUCTION

Invisible steganography is useful for secret communication and copyrights. A secret data hiding in a medium so that no one will guess its existence into this medium; is called invisible steganography [1]. The research issues of invisible steganography system are increasing the imperceptibility and robustness. There are many technique proposed by researchers for increasing the strength of steganography system. To sustain antipiracy technologies, Firm anti-piracy legal laws are needed for support of all these applications because no extra system and mechanism is incorporated in these devices when a person can be caught making illegal use of it [2]. The conscious concealment of data within other image is called image Steganography. Another way is to storing and transmitting data in a particular form in order to make it secure from unintended recipients or use is called cryptography [3] but cryptography does not hide the doubt of secret hiding. Invisible steganography approach is classified into spatial domain steganography and frequency domain steganography.

Frequency domain steganography shows better robustness than spatial domain steganography. Makbol Nasrin et. al. have suggested block level dwt image steganography system and analyzed the performance of robustness [4]. In a digital image, information is imbedded into noisy area of image for hiding secret watermark in less perceptible parts of image and for this varying block level image steganography scheme is suggested and analyzed [5]. Discrete wavelet transform decomposes image into 4 different frequency bands which is called LL, LH, HL and HH where LL sub band represents characteristics of image while HH sub band represents Noise in image [6]. In Discrete cosine transformation, image is converted from space domain to frequency domain where low frequency components are top left corner of DCT coefficient matrix and frequency range increases diagonally from top left corner to bottom right corner of DCT coefficient matrix[7]. El. Safy et. al. suggested a scheme of hiding based on Integer wavelet transformation which shows better imperceptibility
[8]. Integer Wavelet Transform technique and genetic algorithm based image steganography have better results for robustness against visual attacks [9] compared to discrete wavelet transform. Vijay and Vivek proposed a scheme of combined dwt-dct based steganography approach [10].

We have analyzed that hiding of secret datat in LL and LH sub band of DWT transform based steganography distort more than HH domain based DWT steganograpy and degrading visual quality of stego image. In this paper we have proposed a combined steganography technique scheme using 4x4 bloack based DWT-DCT for increasing the imperceptibility of invisible steganography compared to other DWT+DCT based steganography.

II. PROPOSED WORK

It is concluded from the research that many embedding image are embed in the LL,LH, HL sub band and HH sub band of the detail coefficients of wavelet transform for maximize robustness against statistical attacks and robustness against visual attacks or imperceptibility. Coefficients of HH sub band of a level of DWT are selected for embedding image embedding for achieving better the robustness against attacks. After this, on the set of determined HH coefficients of wavelet transform, Discrete Cosine Transform is applied and embedding image is embedded using interchanging of Mid-band coefficients. The LL sub bands signify the characteristics of image while HH sub bands signify the noise level in image. For invisible image hiding, HH frequency sub bands are selected for hiding compared to Low frequency bands because embedding in HH does not change the key characteristics of image. The detailed embedding procedure of proposed technique is explained as following.

Step 1. Cover image is read and transformed using Discreate Wavelet Transformation which decomposes image into 4 different frequency bands.

Step 2. Discrete Wavelet Transformation is applied again on all above sub-bands for decomposing into 16 sub-bands and four HH2 (HH sub-bands at level 2) sub-bands is selected.

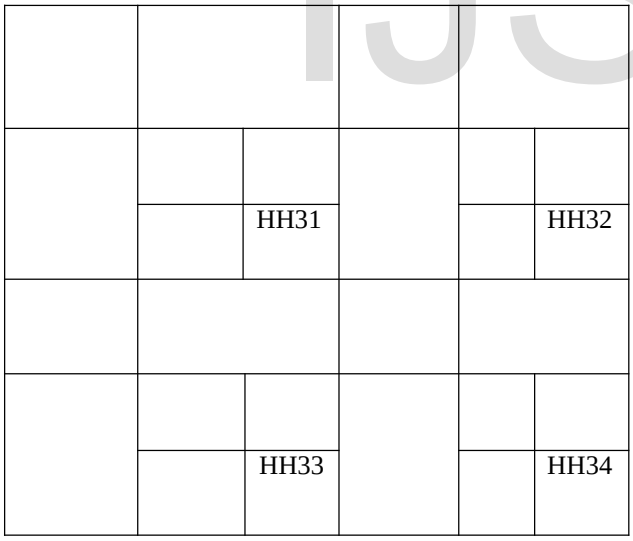

Figure 1: Four selected HH sub bands for embedding

Step 3. Discreate Wavelet Transformation is applied again on selected four HH2 sub-bands for decomposing into 16 sub-bands and four HH3 (HH sub-bands at level 3 i.e. HH31, HH32, HH33 and HH34) sub-bands are selected. These diagonal coefficients (HH sub-bands) are selected achieving better imperceptibility and robustness in order to achieve least distortion in cover image in embedding of secret Image. Selected 4 HH sub bands for embedding are shown in figure 1.

Step 4.Perform Discrete Cosine Transform at 4x4 block level on all above selected HH3 sub-bands and 4x4 blocks of DWT-DCT domain is achieved.

Step 5. Watermark image is read and each pixel converted into binary.

Step 6. A bit of watermark is embedded in DCT block matrix. If watermark bit is 0 then coefficient value P (4, 4) must be greater than or equal to P (3, 3) otherwise swap the values. If watermark bit is 1 then coefficient value P(4,4) must be less than P(3,3) as shown in figure 0 otherwise swap the values.

Step 7.Apply inverse Discrete Cosine Transform on each embedded block.

Step 8. Apply inverse Discrete Wavelet Transform to get watermarked image in space domain.

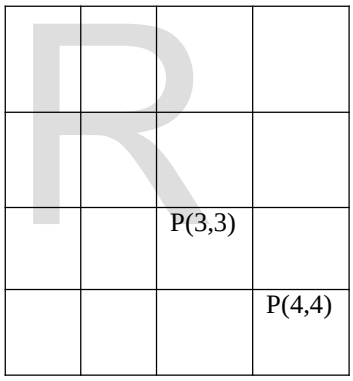

Figure 2: A block of 4x4 DCT Coefficient Matrix

III. EXPERIMENTS & RESULTS

The Proposed Technique is implemented on MATLAB. The Experiments of Proposed IWT-DCT image Steganography technique is performed on host images of Lena.jpeg, baboon.bmp, url.gif etc images of size of 512x512 pixels each. A secret image of size of 32x32 binary images is embedded as secret image in above host images. Pixel values of Cover image is changed slightly due to embedding of secret data but quality of stego image is more robust for visual attacks. It is measured in term of PSNR (Peak Signal to Noise Ratio) and higher imperceptible stego image should show higher PSNR value.

Table 1: PSNR and WPSNR on different cover image using DWT-DCT

Sno	Cover image	Water Mark Image	PSNR	WPSNR
1	Lena.jpeg (Gray Scale)	AB	39. 2654	60.18
2	Baboon. jpeg (Gray Scale)	AB	40.32	56.44
3	barbara. jpeg (Gray Scale)	AB	40.19	56.8622
4	Peppers.jpeg	AB	45.05	62.13
5	fruit_lumi.jpeg (Gray Scale)	AB	44.23	60.33

Table 2: PSNR and WPSNR on different cover image using proposed DWT-DCT method

Sno	Cover image	Secret Image	PSNR	WPSNR
1	Lena.jpeg (Gray Scale)	AB	43.9	59.71
2	Lena.jpeg (colored Scale)	AB	50.30	59.25
3	Baboon.jpeg (gray scale image)	AB	47.77	66.21
4	Baboon.jpeg (colored image)	AB	46.18	70.54
5	barbara.jpeg (gray scale image)	AB	40.6	66.65
6	barbara.jpeg (colored image)	AB	47.83	63.18
7	fruit_lumi.jpeg (gray scale image)	AB	45.13	61.74
8	fruit_lumi.jpeg (colored image)	AB	49.77	62.80
9	Peppers.jpeg (gray scale)	AB	51.33	57.96
10	Peppers.jpeg (colored image)	AB	51.53	58.06

Table 3: Comparison of proposed work with other techniques

S no.	Image Name	Secret Image	PSNR of Vijay's DWT+DCT method [10]	PSNR proposed(DWT+DCT)
1	Leena.jpg	AB	39. 2654	43.9

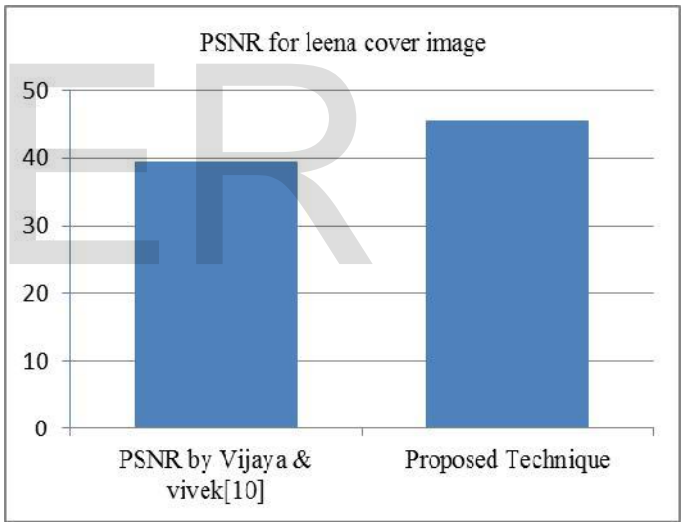

Fig.3: Comparative analysis of proposed technique with other technique for performance of PSNR value for gray scale.

IV. Conclusion

Results are shown in Table 1, 2 and 3 and figure 3and it is derived that proposed technique achieved PSNR value 43.9, 50.30 for gray scale and colored leena image while Vijaya's & Vivek's method provide PSNR 39.2654 on leena gray scale. So proposed method achieved PSNR more than Vijaya's method and other exiting method of DWT+DCT 8x8 block

technique. We have tested the proposed technique on different textured gray scale and colored images and results that 4x4 block based dwt + dct is much better than 8x8 block based dwt+ dct technique. PSNR signify robustness against visual and statistical attacks for invisible steganography. So 4x4 based DWT-DCT based steganography process is more imperceptible and robust for visual attacks. In the proposed work, watermark is embedded in high frequency band or edge and noise information not in characteristics and shapes information of cover image. Further proposed technique may be verified for robustness of statistical attacks in future.

REFERENCES

[1] Abbas Cheddad A., Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", International Journal of Signal Processing, Elsevier pp:727-752, 2010.

[2] Kumar, Vijay, and Dinesh Kumar, "Performance evaluation of dwt based image Watermarking", In *IEEE 2nd International Advance Computing Conference (IACC)*, pp. 223-228, IEEE, 2010.

[3] Yong, Xie, Wu-yang Shan, Xiao-long Cao, and Qi-qin Feng. "Analysis and comparison of holographic and traditional digital image watermarking in DWT domain", In *7th IEEE International Conference on Computer Science & Education (ICCSE)*, pp. 790-793, IEEE, 2012.

[4] Makbol, Nasrin M., Bee Ee Khoo, and Taha H. Rassem. "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics." *IET Image Processing , Vol.*10, no. 1 pp. 34-52, 2016.

[5] Joshi, Amit M., Monica Bapna, and Manisha Meena, "Blind Image Watermarking of Variable Block Size for Copyright Protection", In *Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing*, pp. 853-859, Springer, India, 2016.

[6] Soni, Karuna, Sandeep K. Gupta, Umesh Kumar, and Shubh L. Agrwal, "A new Gabor wavelet transform feature extraction technique for ear biometric recognition", In *6th IEEE Power India International Conference (PIICON)*, pp. 1-3, IEEE, 2014.

[7] Dosodia, Priya, Amarjeet Poonia, Sandeep K. Gupta, and Shubh Lakshmi Agrwal, "New Gabor-DCT feature extraction technique for facial expression recognition", In *Fifth IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 546-549, 2015.

[8] El Safy, R. O., H. H. Zayed, and A. El Dessouki "An adaptive steganographic technique based on integer wavelet transform", In IEEE *International Conference on Networking and Media Convergence, (ICNM 2009).*, pp. 111-117, IEEE, 2009.

[9] Ghasemi, Elham, Jamshid Shanbehzadeh, and Bahram ZahirAzami. "A steganographic method based on Integer Wavelet Transform and Genetic Algorithm", In IEEE *International Conference on Communications and Signal Processing (ICCSP)*, pp. 42-45, IEEE, 2011.

[10] Ahire, Vijaya K., and Vivek Kshirsagar. "Robust watermarking scheme based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) for copyright protection of digital images." *IJCSNS International Journal of Computer Science and Network Security, Vol.* 11, no. 8, pp. 208-213, 2011.