IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 12, December 2018

User Interface Based High Payload Double Image Steganography

Priya R Sankpal[1], Anuradha MR[2]

Assistant Professor, Dept. of ECE, BNMIT, Bangalore, India[1]

Graduate Student, Dept. of ECE, BNMIT, Bangalore, India[2]

Abstract: Digital data, since its invasion has become an integral part of everyday life aspects. Digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital data can be stored efficiently with a very high quality, and it can be manipulated very easily using computers. Watermarking techniques have been developed to protect the digital data from such manipulations. In watermarking, the most challenging task is the embedding capacity in an image. The strength of watermarking can be changed for the improvement of resolution of the images in order to make the image indistinguishable from the original images. The proposed method suggests an effective and easily implementable way to secure the confidential information with a high payload capacity. Also a User Interface (UI) was developed, which makes the watermarking process user friendly. The UI provides the sender with the freedom of opting cover image and watermark image in which actual data is stored. Confidential data can also be entered dynamically by the user. This is then made secure by symmetric key encryption technique and transmitted over the media. The transformation that is employed is the 3 level DWT process. The PSNR and MSE are also calculated to verify the robustness of the algorithm.

Keywords: Double image, PSNR, Payload, Encryption

I. INTRODUCTION

Digital image watermarking is used to embed the useful information in the image that is hidden from the outside world while transferred over internet or any other media. Digital image processing attains several computer operations over digitized image for different purposes like filtration of images from noise, improvising quality of image[2]. It is the process of embedding any secret information (copyrights, digital signatures) as a pattern of bits in the media such as video, image, audio etc in order to secure the data. Watermarking results are so reliable that the final embedded image is indistinguishable from the original information. Digital watermarking can achieve security by embedding a copyright's signal into host signal. A good image watermarking needs to satisfy imperceptibility and robustness [3].There is several techniques which can be imbibed to carry on the process of watermarking. Transformation of an image from spatial domain to frequency domain has many advantages and gives the transmitter or the user to make use of various operations on images.

DFT is one of the trivial methods used in the investigation of the signal coefficients. It is used to perform Fourier analysis in many applications. DCT has additional capabilities compared to DFT with respect to even symmetry and periodicity. They are majorly used in JPEG related applications, solving partial differential equations etc. The versatile transform which has ability to capture both frequency and location(in time) is Discrete wavelet transform. The important factor of DWT is its temporal resolution which is not seen in other Fourier transforms.

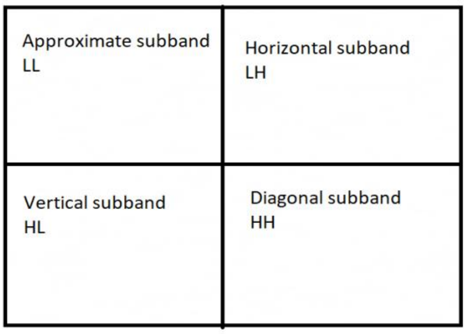


Fig 1: DWT decomposition

DOI 10.17148/IJARCCE.2018.71220

DWT has many bases whereas the Fourier bases use only sine's and cosines. The domain of watermarking is two types such as frequency domain and spatial domain. The frequency domain techniques are tougher and more hidden to general image processing operations like JPEG compression, blurring and adding noise[4].

Wavelet transform of the image results in four different sub images termed as Approximate, Horizontal ,Vertical , Diagonal components. The important details and the basic information of the image are found in the approximate component. These four components are also represented as LL, LH, HL and HH frequency bands respectively, where L denotes low frequency components and H represents high frequency components. The image when transformed results in four sub bands which depict important details of the image with respect to their components. Digital watermarking has some benefits in transmitting confidential information over the media and channel. The performance characteristics of this technique are listed, Robustness: The watermark must be able to withstand alterations in normal signal processing operations such as image cropping, transformation, compression etc.

Imperceptibility: The watermarked image should look same as the cover image to the human eye. The attacker will not be able to detect that watermark is embedded in it.
Security: An unauthorized person cannot detect, retrieve or modify the embedded watermark. This can be achieved by specifying many security related algorithms.
PSNR: The ratio between maximum signal extractions to noise attacks that can be obtained at higher rates.
In this paper, the methodology explains double image steganography, to securely transfer maximum amount of data. The next section of this paper is as follows. In section II, the related work is briefly discussed. Section III describes the double image high payload watermarking algorithm. Section IV depicts the experimental results and comparison with other methodologies. Section V draws the conclusion of this technique.

II. RELATED WORK

There is a need to protect the patented copyright information and other secret data. This can be done solely by the digital watermarking method which uses various algorithms or techniques to overcome the acts of forgery, cyber theft etc. J un Yu, Shu-min Dong state a novel digital image multi watermarking which is based on DWT and ICA (Independent Component Analysis). The host image is decomposed into two layer multi-resolution to get middle-frequency sub-band named HL2, LH2, and the coefficients of HL2, LH2 is marked as matrix IHL2' hH2 using Arnold transformation [4].Authors in [3] describe the method CDMA-based watermarking where informed embedding is generalized by taking into account more detailed host information as well as possible pre-processing operations on the watermark at the embedder and the extractor. The model and embedding method can achieve a payload of more than 200 bps. The technique in [1], a blind digital watermarking algorithm is provided using DWT and DCT. HL coefficient is puzzled first before embedding the scrambled image into a HL coefficient of the cover image. This ensures additional security to the watermark entrenched image. J un Yu, Shu-min Dong explain the watermarking procedure using OFDM and CDMA technologies. OFDM-CDMA method is a combination of OFDM and CDMA methods. In this method, the watermark is converted to parallel streams and multiplexed to streamline the bandwidth so it can provide a high data payload. Then, each sequence of the parallel watermark is multiplied by spreading codes to reinforce the orthogonality of each sequence, so it can minimize the error between the sequences [2].

III. WATERMARKING METHODOLOGY

The method demonstrated here makes use of 3 level wavelet transform to hide an image in another image. Watermark image contains the information which is securely stored in cover image. This is known as double image steganography. A standard 256*256 image is considered for this purpose. To ensure that the information is secure, symmetric key encryption and Caesar cipher techniques are employed to retain the robustness of this cryptographic methodology. A unified approach seen here is the user friendly interface and embedding capacity of the algorithm.

The watermarking approach utilized here has 3 main portions.
1. Data hiding followed by image hiding in the cover image using wavelet decomposition method.
2. Symmetric key password is used for authentication purpose which is a simplified approach in terms of security.
3. Caesar encryption is used to generate the required input sequence by specifying the shift value in the algorithm.

The method describes the steps in which the data can be concealed in the image. The User Interface makes the watermarking process user friendly because it provides the sender with the freedom of opting cover image and watermark image in which actual data is stored. Confidential data can also be entered dynamically by the user. This is then made secure by symmetric key encryption technique and transmitted over the media. The transformation that is employed is the 3 level DWT process. The PSNR and MSE are also calculated to verify the robustness of the algorithm.

DOI 10.17148/IJARCCE.2018.71220

User Interface Dialog Box: A user interface (UI) is an interface that provides menu of choices for user input. The operation of each block is such that it waits for the user to provide appropriate input in order to go ahead with the further operations. It exhibits a modal menu dialog box containing the various options designed as per the requirement. It returns the number of selected menu items and ceases the operation if the user selects the exit button in the menu window. The operations for each menu dialog box are specified to carry out their respective functions, which display results provided the user responds with correct input values. The user interface can also be specified with the main title which denotes the brief action of the approach.

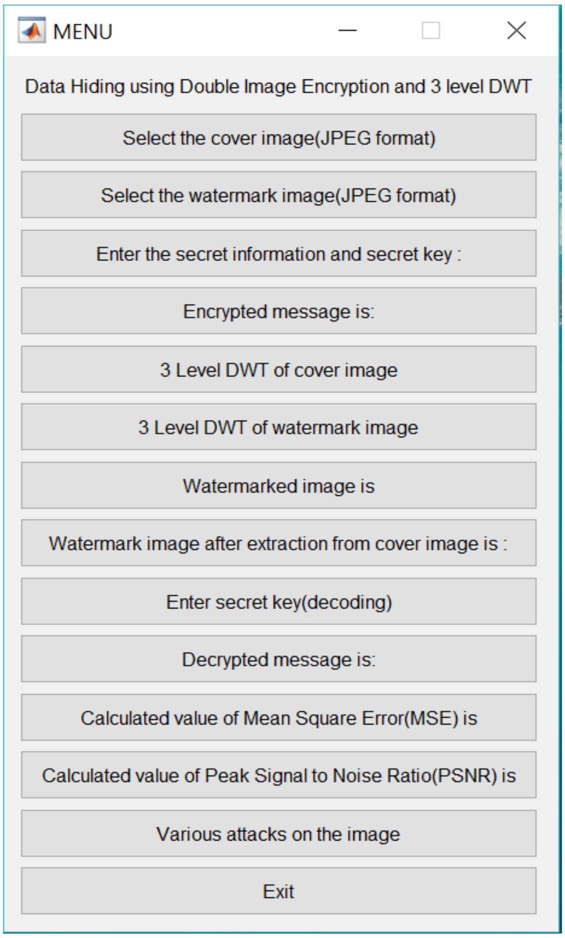

MENU
Data Hiding using Double Image Encryption and 3 level DWT
Select the cover image(JPEG format)
Select the watermark image(JPEG format)
Enter the secret information and secret key :
Encrypted message is:
3 Level DWT of cover image
3 Level DWT of watermark image
Watermarked image is
Watermark image after extraction from cover image is :
Enter secret key(decoding)
Decrypted message is:
Calculated value of Mean Square Error(MSE) is
Calculated value of Peak Signal to Noise Ratio(PSNR) is
Various attacks on the image
Exit

Fig 3: User Interface employed in this method

The cover image contains the watermarked hidden information. After the user chooses the desired base media, the interface menu next takes the user to enter the information along with the secret key to generate the watermarked image. At the receiver end, the watermarked image is decoded using the secret key. This is again subjected to deduction of information from the extracted image. The PSNR and MSE values are the two essential factors that make the algorithm sturdy.

A. Watermark embedding and extraction

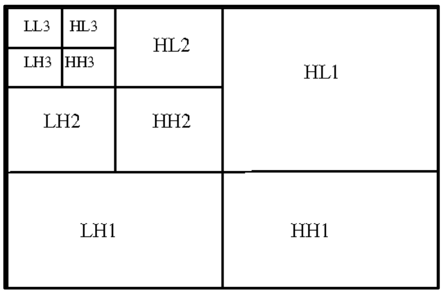


Fig 4: 3 level DWT process

This section describes the wavelet transformation technique that enables the image pixels to undergo several operations for watermarking process. Normally we have come across one level wavelet transformations. The decomposition is done using either a wavelet or wavelet decomposition filters. The sub band of frequency used for the watermarking process in this paper is the LL component. The wavelets employed in this method are the Haar wavelet.The Haar wavelet is also the simplest possible wavelet. The normalized values of message bits are used to append to the watermark image. Normalized values are calculated by dividing each bit by the maximum value of the entire message.

3 level DWT is an efficient way to embed the information in the most secure way. Initially the LL component of the cover image is subjected to wavelet decomposition. Here the image size also reduces, which is further subjected to another level of wavelet decomposition. In the second level, the LL1 component obtained is put through one more level of decomposition process. Now, the information is appended to the watermark image, after that it is saved in the cover image. These watermark image pixels are added to the cover image along with the watermarking factor, w. The output results change as and when the watermarking strength co-efficient changes.

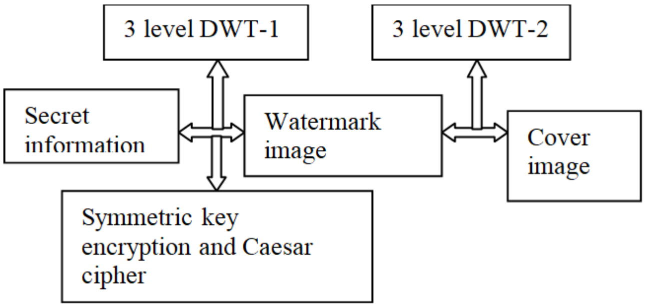


Fig 5: Watermarking embedding process

The watermarking embedding algorithm is discussed in the following steps:

1. Load the cover image and perform 3 level DWT on the LL component of it which gives rise to LL2, the 3rd level sub band
2. Load the watermark image and perform 3 level DWT on LL component of it which gives L_L2, the 3rd level sub band
3. Enter the secret information and secret key for encoding process.
4. The message is normalized and then appended to the watermark image

$$msg\_norm = \frac{msg\_bit}{msg\_bit_{max}} \qquad (1)$$

$$L\_L2=L\_L2+msg\_norm \qquad (2)$$

5. Caesar cipher substitution method encrypts the data
6. Watermarked image is added to the cover image

Watermarked image final = LL2 + (w*L_L2) (3)

Where w is the watermarking coefficient

7. 3 level Inverse DWT(IDWT) is performed on the final watermarked image

Watermark Extraction: The inverse 3 level wavelet decomposition of the cover image is carried out(IDWT) to extract the watermark image. This watermark image is further decomposed by 3 levels to extricate the concealed information.

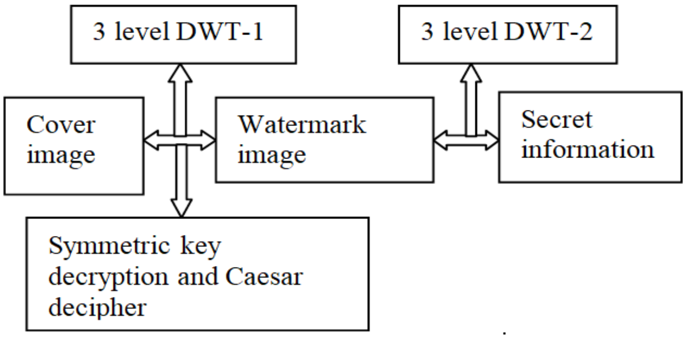


Fig 6: Watermark extraction process

DOI 10.17148/IJARCCE.2018.71220

The reverse algorithm is used to extract the watermark image from cover image.

1. 3 level DWT of the LL sub band of the final watermarked image which results in the AA2
2. 3 level DWT of LL sub band of the watermark image resulting in A_A2 component
3. User enters the symmetric key for the decoding process at the receiver end
4. Watermark image is extracted from the cover image

A_A2= AA2 - (w*L_L2) (4)

5. The normalized message values are obtained from the A_A2 component

msg_norm1=A_A2-L_L2 (5)

6. The secret data is acquired from normalized values and decrypted using Caesar algorithm.

msg bit=msg_norm1*msg$_{max}$ (6)

B. Encryption Algorithm

Caesar Cipher technique:

Caesar cipher is a primitive method yet the simplest and lucid cryptographic technique. However, there are other ways of encrypting the data whereas this forms a lucid way of performing cryptography. It is a type of substitution technique wherein each element of the confidential data is rearranged according to the specified number of shifts. It is one of the first and the oldest cryptographic algorithms.

Caesar encryption:

Cn(i)=(i+n)mod 26 (7)

where, Cn(i) = cipher text and n=number of shifts

Caesar decryption:

Dn(i)=(i-n)mod 26 (8)

where, Dn(i) = plain text

Symmetric key password: Symmetric key encryption, a trivial yet the a straight forward technique is used in this method. It makes use of a secret key which can be a number, a word, or just a string of random letters that makes the information secure. Usually the secret key is applied to the confidential information to change the pattern of the message, but in this mechanism it is used as the key to carry put the watermarking process. The symmetric key is used to encrypt a message and the same key is also used to decrypt it at the receiver end. In Symmetric Encryption there's only one key. Until the sender and receiver enter the common secret key, the process cannot be carried out.

C. Payload measurements and other parameters

In watermarking, the most challenging task is the embedding capacity in an image. The strength of watermarking can be changed for the improvement of resolution of the images in order to make the image indistinguishable from the original images. The payload capacity achieved in this methodology is 256 characters. The watermark image can hold up to 256 characters which are further stored in a cover image. Other aspect is the bit per pixel rate(bpp). The watermark image has capacity to assimilate 1.0268 bpp to 1.018 bpp. The 256 characters can contain any message elements from the keyboard of a computer which can include numbers, alphabets, special characters and even spaces.

Mean Squared Error (MSE): The MSE indicates the cumulative squared error between the watermark image and compressed image and PSNR represents a measure of the peak error. The lower the value of MSE, better the result.

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (9)$$

Where M and N are the rows and columns of the image

Peak Signal to Noise Ratio (PSNR): The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are used to compare image compression quality. The psnr is used to find out the peak signal to noise ratio for the given image. This ratio is a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed image or the recovered image.

PSNR = 10*log(255*255/MSE) (10)

Table 1: Payload capacity (in terms of Total number of bits and bits per pixel), PSNR, MSE for different embedding strengths

Images	Watermarking strength (w)	PSNR	MSE	Payload	
				Bits	Bpp
Cover image-leg	0.002	58.3102	0.2410	256	1.018
xray (grayscale)	0.001	53.4097	0.2378	256	1.028
Watermark image-dis located ankle bone (grayscale)	0.01	52.8031	0.2561	256	1.026
Color Images	0.01	56.5671	0.2213	256	7.689

IV. EXPERIMENTAL RESULTS

For the demonstration of watermarking process, x-ray of the leg is chosen as cover image and fractured foot is chosen as watermark image. The text information can contain any string, word, number or special character. This is embedded into the watermark image using DWT. The images that are considered are of the standard size 256*256.Color image and grayscale image can be given as the input which will be converted to grayscale image for watermarking process.

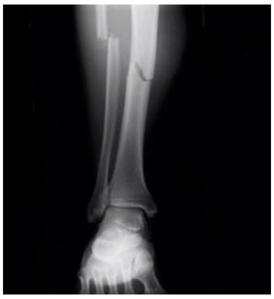


Fig 7: cover image(xray of right leg)

Patient name: Natasha
Admitted date : 2/3/1996
Result : right foot ankle bone dislocation
Status: under observation

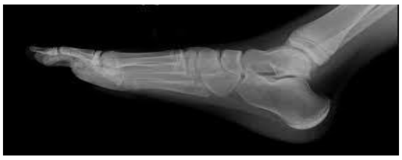


Fig 7: cover image(x-ray of right leg)

The secret information is entered by the user in the command window. The window waits for the user to enter valid information and displays the length of the information. The next step is that the user must enter the secret key password to proceed further. Before embedding the secret information onto the image, the message is encrypted using Caesar cipher technique where the message bit positions are shifted by the standard value of 3. This information and watermark image is then stored in the cover image. Now the double image containing data are transmitted over the media channel for secure transmission. The 3 level DWT of the image makes the watermarking process more secure and accurate. This precise method conceals the information in the third level decomposed image which also retains the information till the extraction process. There is very less distortion and very less difference between the final watermarked image and the cover image.

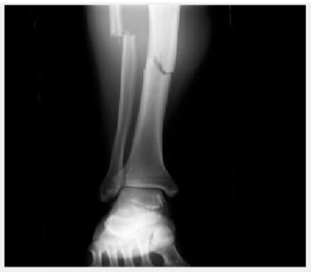


Fig 9: 3 level DWT of cover image

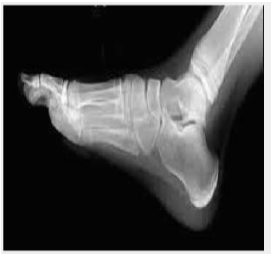


Fig 10: 3 level DWT of watermark image

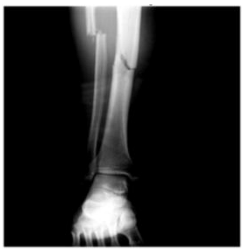


Fig 11: Watermarked image

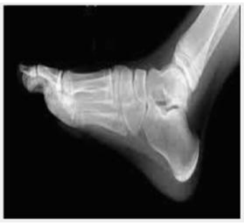


Fig 12: Extracted watermark image

The watermark image which is extracted from cover image is almost similar to the host image. In this method, when the watermarking strength is varied, there is no noticeable or distinguishable difference between host image and extracted image. This ensures that the watermarking process is secure enough to carry the secret information. Embedding strength is mainly concerned with the resolution or clarity with which final watermarked image can be obtained without any noise. At the receiver, the secret key is cross verified before the decoding process could be carried out. The watermark image is extracted from the cover image by deducing to the 3 level DWT. Again the 3 level IDWT is performed on the extracted image to extract the information.

Various attacks on the watermarked image: The final watermarked image is prone to various attacks while it is transferred over the channel. The watermark image will be subjected to different types of modifications wherein the opponent might try to pull out the information. While trying to do this, there may be many operations that are performed on the cover image. The images must not be affected by such additions, filtering, compression etc.

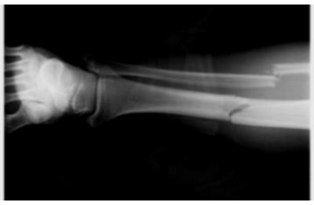


Fig 13: Rotation of the cover image

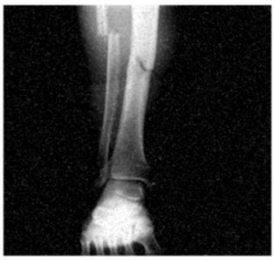


Fig 14: salt and pepper noise of cover image

DOI 10.17148/IJARCCE.2018.71220

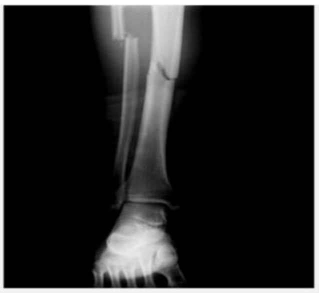


Fig 15: Poisson noise of cover image

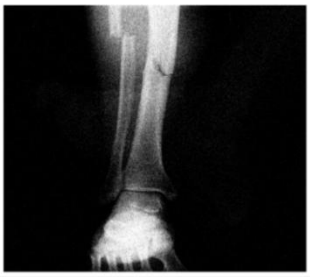


Fig 16: White Gaussian noise of cover image

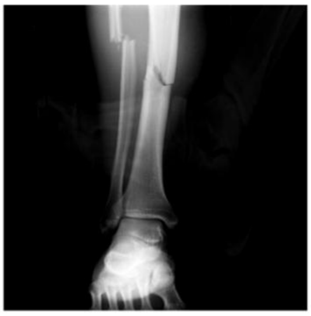
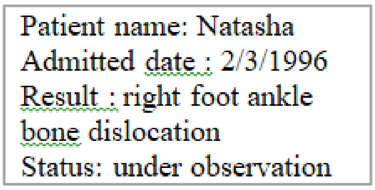


Fig 17: Median filtering of cover image



Patient name: Natasha
Admitted date : 2/3/1996
Result : right foot ankle
bone dislocation
Status: under observation

Fig 18: Received secret message

Observations: The values that are obtained out of the watermarking process are compared with the other techniques. It is seen that the payload capacity varies directly with the image dimensions. For the payload of 256 characters and 1.0179 bpp here for grayscale images, and 7 to 7.689 bpp for colour images, the PSNR and MSE values are found to be quite satisfactory. The data which is retrieved at the receiver's end is exactly the same message that was generated at the other end. The suggested method uses the simple yet robust algorithm to transform the data and make it secure.

Table 2: Comparison of the parameters with existing methods

Methods	**Payload**	**PSNR(dB)**	**MSE**
[4]	0.3 bpp to 8 bpp	50.86	-
[7]	-	51.14	0.1386
[6]	-	52.23 to 77.97	-
[2]	0.97 bpp to 0.156 bpp	43.7	-
[1]	-	47.27	-
Proposed method	256 bits and1.018 bpp(Grayscale image) 7 bpp to 7.689 bpp (Color image)	58 (Grayscale) 56 (Color)	0.2410

CONCLUSION

The proposed method suggests an effective and easily implementable way to secure the confidential information. The payload capacity is directly proportional to the size of the image. Here in this case the standard size of the image is 256*256 for which the PSNR, MSE and payload are 58 dB, 0.2410, 256 characters and 1-7 bpp. For further processing, the multilevel wavelet decomposition is used, which gives information regarding frequency components present in the signal and enhances the information about the signal. Watermarking in DICOM (Digital Imaging and Communications in Medicine) images forms an important application to safely transfer crucial patient related data. There are also benefits of watermarking in defence, currency security, protecting patented work and images.

ACKNOWLEDGMENT

The authors would like to thank all the earlier works on steganography, which kindled enthusiasm to carry out the work done in this paper. All work done, images shown in this paper are for educational purpose and not for commercial purpose.

REFERENCES

[1]. M.Veni and T.Meyyappan, "DWT DCT based New Image Watermarking Algorithm to Improve the Imperceptibility and Robustness 2017 International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE2017), 10.1109/ICEICE.2017.8192444, April 2017, pp. 1-6

[2]. Rahmawati Hasanah ; Mohammad Sigit Arifianto, "A high payload reversible watermarking scheme based-on OFDM-CDMA," 10th International Conference on Telecommunication Systems Services and Applications (TSSA), Denpasar, Indonesia, 6 October 2016, pp. 1-6

[3]. Peng Zhang, Member, IEEE, Ye Li, Jingsai Jiang, Xiaofeng Ma, Yanhong Fan, and Qiuyun Hao, "Informed Embedding with Selective Host Rejection for CDMA-Based High-Payload and Robust Watermarking," Sixth International Conference on Advanced Computational Intelligence, Hangzhou, China, October 19-21,2013, pp. 228-232

[4]. J un Yu, Shu-min Dong, "A Multi-watermarking Based on DWT and ICA**,"** 2nd International Conference on Image, Vision and Computing, 1 June 2017, pp. 616-619

[5]. Prerna Gupta and Girish Parmar, "Image Watermarking using IWT-SVD and its Comparative Analysis with DWT-SVD," International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017, pp. 527-531

[6]. Priyanka Bharti and Roshan "High PSNR based Image Watermarking by DWT CZT-SVD algorithm," 8th International Conference on Computational Intelligence and Communication Networks, 2016, DOI 10.1109/CICN.2016.86, pp. 404-407

[7]. Zhang Na-na, Yin Jing, Mao Jia-fa and Su Gui-Lian, "Research on the Watermarking Payload for Spatial-domain Image under Transparent Conditions," IEEE 14th International Conference on Communication Technology 2012, pp. 615-621

BIOGRAPHIES

Priya R Sankpal is pursuing her PHD in image processing. Her subjects of interests are network security, image processing and embedded systems. She is an Assistant Professor in Department of ECE at BNMIT, Bangalore, India.

Anuradha MR is a graduate in ECE from BNMIT. Some of her subjects of interests include image processing, networking and embedded systems.

DOI 10.17148/IJARCCE.2018.71220