A Novel Technique for Digital Watermarking using DWT and Neural Network

Mrs.Nirupma Tiwari Dr. Naveen Hemrajani Dr. Dinesh Goyal

Abstract— Digital watermarking (DW) is a technology that hides information in image to provide authentication. Information hiding is done by the tampering content of the image. In this research, self image embedding using two level discrete wavelet transform (2DWT) with singular value decomposition (SVD),and probabilistic neural network (PNN) classifier method. Firstly, take cover image and create watermark image using bi-cubic interpolation method.Secondly, encrypt watermark image using stream cipher (SC) method. Thirdly, the watermarking embedding region is directed with 2DWT and the low frequency DWT coefficient is isolated into non-covering pieces; SVD is connected to each block. A bit of the watermark is inserted through slight alterations of the singular quality (SV) framework in every block. The resulting analysis shows that proposed algorithm offers better image quality and more robustness under geometrical attack (GA), compression attack (CA) and noise attack (NA). Lastly, classify the watermarked image using PNN classifier.The resulting analysis shows that proposed algorithm offers better image quality and more robustness under copy move forgery attack. Peak Signal to Noise Ratio (PSNR) and L2 Normalization (L2Norm) are evaluated to find image quality and robustness. Finally, a comparative study is made against the previous technique.

Index Terms— DWT; SVD; Bi-Cubic; PNN; Stream Cipher; PSNR; MSE;L2Norm; Attcaks

1 INTRODUCTION

The growth of internet and web technology, digital data are transmitted must be authenticated, secured and copyright protected, so various information protection methods are developing day by day. Copy of digital data is more and more easy, digital watermarking has been proposed a solution to copy of multimedia data in a networked environment. To provide security two techniques have been used such as encryption and watermarking. In the process of encryption, it used to protect digital data during transmission. In watermarking secrete imperceptible signal is embedded in original data. DW(Digital Watermarking) has certain characteristic; the most important is robustness, imperceptibility and invisibility. DW is divided into two categories special domain watermarking and frequency domain watermarking. Zhen Li,proposed a blind watermarking scheme. In which watermark is embedded into a high frequency band of SVD DCT block [1].

A variety of schemes have been proposed for copyright protection. DW has picked up a great deal of prominence for its productivity. The human eye can't watch the subtle element. Small bit of changes in the color estimations of a picture is corrected by the eye, so that the distinction is un-recognizable. DW makes utilization of this limitation [2]. In the processing step of DWT,it divides the signal into high and low frequency parts. The low frequency part contains coarse data of sign while high frequency part contains data about the edge segments. The high frequency segments are generally utilized for watermarking subsequent to the human eye is less touchy to changes in edges [3].

SVD:Another approach used for watermarking is based on a SVD method which provides robustness and security [4] and which is used for watermark casting and detection. SVD is a method in which a given image represented as a matrix 'A' is decomposed into a product of two orthogonal matrices 'U' and 'V' and 'S' matrix as –

$$A = USV^T$$

Where matrix 'S' is a diagonal matrix which consists all nonnegative Eigenvalues of matrix A. Matrix 'U' and 'V' are orthogonal because the product of matrix 'U' and transpose of 'V' is Identity matrix.

PNN chooses a learning classification and evaluations the probability of the example by utilizing the spiral premise capacity. PNN can work in parallel and requires no criticism from individual neurons in the data; along these lines, PNN training is quick and simpler to learn than other neural systems, for example, back-propoagation systems. The PNN comprises of four layers of hubs, to be specific, the information, example, summation, and yield layers. At the point when a data is exhibited, the principal layer registers the separations from the info vector to the preparation information vectors and after that delivers a vector with components that show how shut the information is to a training input. The summation layer entireties these commitments for every class of inputs to deliver a vector of probabilities as its net yield.

Finally, a competitive transfer function on the output of the summation layer selects the maximum of these probabilities and produces a 1 for that class and a 0 for the other classes to obtain the watermark binary image.The training of PNN is conducted by generating a pattern node, connecting it to the summation node of the target class, and assigning the input vector as the weight vector. The values of the three wavelet coefficients (cH3, cD3, and cV3) are combined to form a feature of the training vector with a size of 128 * 128. This feature is used as input to 128 PNN, for training and extraction.[5]

Stream cipher encryption: A SC is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).The processing of SC for every plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of every digit is reliant on the present condition of the figure, it is otherwise called state cipher. Practically speaking, a digit is normally a

bit and the joining operation an exclusive or (XOR). Be that as it may, SC can be susceptible to genuine security issues if utilized erroneously (see stream figure assaults); specifically, the same beginning state (seed) should never be utilized twice [6].
Bicubic interpolation- It is able through either cubic splines, or cubic convolution algorithm [7].

2 Literature Review

Takwa Chi haoui (2014)[8] it presented a technique that consequently distinguishes copied areas in the same picture. Copied identification is performed by distinguishing the nearby attributes of the pictures (purposes of enthusiasm) utilizing the SIFT strategy and by coordinating between indistinguishable components utilizing the SVD technique. The precision is bad for this framework.
Ramesh Chand Pandey (2014) [9]-It used SURF and SIFT, which make it very fast and robust in detecting copy-moved regions. Experimental results demonstrate commendable performance in image copy- move forgery detection. It is mainly dedicated to investigating how to improve the detection phase for multiple cloned objects with respect to the cloned image patch and for patches with highly uniform texture where salient keypoints are not recovered by SURF and SIFT like techniques.
A technique proposed by Bashar Noda [10], utilizes DWT and Kernel Principal Component (KPCA) for copy move fraud notice. They utilized these routines in light of their strong block coordinating featured. They isolated the picture into a few little measured pieces. They figured KPCA based vectors and DWT vectors for each square. At that point they put these vectors in a network and sorted it lexicographically. They utilized the sorted squares to locate the comparative focuses and figured their counterbalance frequencies. To stay away from false location, they put limit esteem for offset frequency.They built up another calculation to distinguish flip and turn kind of forgeries utilizing marking strategy and geometric change. This calculation indicated promising upgrades contrasted with ordinary PCA-approach. It also recognizes forgeries which have an added substance noise and lossy JPEG conversation.
Kayvan.Ghaderi (2013) [11] et al present a novel semi-blind watermarking scheme for image copyright protection, which is developed in the Lifting Wavelet Transform (LWT) and is based on SVD. It has been used fractal decoding to make a very compact representation of watermark image. In the embedding stage of watermarking method, at first; furthermore perform breaking down of the host picture with 2D-LWT change, then SVD is connected to sub-groups of changed picture, and install the watermark by altering the singular qualities. In the watermark extraction stage, the embedded codes are extracted from the watermarked picture. At that point the watermark picture is rendered by running the extracted code.
Song Huang (2011) [12] et al present that this technique presented hides a scrambled watermark into an image, and thinks about HVS attributes amid the watermark embedding process, then uses a bach propagation NN system to take in the qualities of the inserted watermark identified with the watermarked picture.

3 Proposed Methodology

In this algorithm, firstly take a color cover image and create watermark image using bi-cubic interpolation method. Bi-Cubic Interpolation finds the pixel value of the weighted average of the 16 closest pixels of the defined input coordinates, and allocates that value to the output coordinates. The one-dimensional interpolation function is applied in both directions for two-dimensional interpolation. Secondly, the XOR is performed between watermark image and pseudo random bits. These bits are behaved like an encryption key. The same key is required for decrypting the watermark image.In the third step, embed the watermark image into cover image using 2-DWT and SVD.

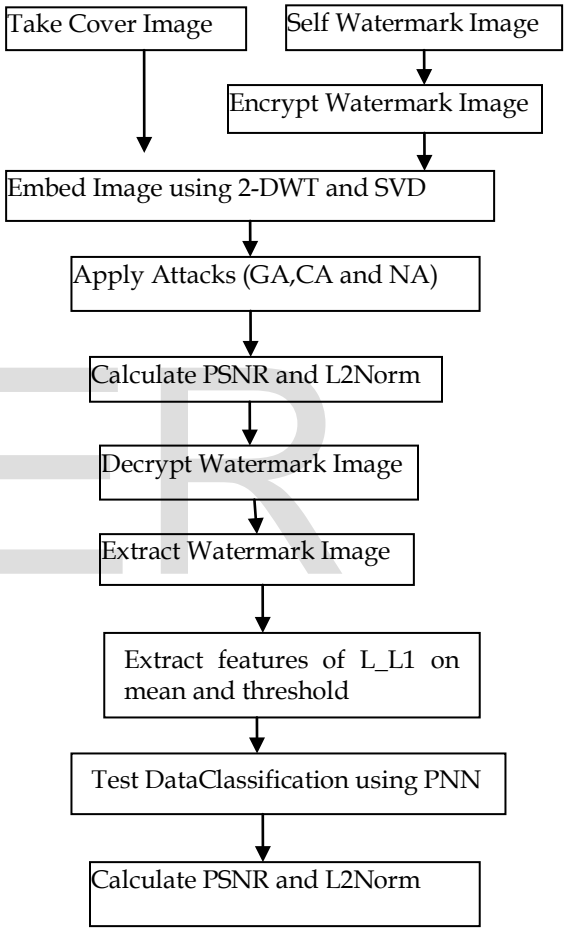


Figure1. Proposed System Block Diagram

In the fourth step,apply different types of attack on watermarked image. In the extraction process, extract watermark image from embedded image. Encryption of watermark image ensures the security of watermark from unauthorized attacks. Without the key information watermark cannot be decrypted. In the last step,we construct a three-layer PNN with 3, 10 and 2 neurons in the input, hidden and output layer respectively. And the activation function in the hidden layer is a sigmoid function, but the output neuron uses the linear activation function. Note that the train goal should be set suitably during training samples, because whether a bigger or smaller train

goal does harm to the generalization ability of PNN.Proposed model shown in figure 1.

3.1 Proposed Algorithm

Embedding Algorithm
Input: Cover Image
Output: Watermarked Image

1) Read cover image and separate the cover image I (N×N×3) to three color RGB planes.
2) Choose cover image as a watermark image. We use Cubic interpolation to scale these matrices and used it as a watermark. The size of scaling which is determined by certain rules from the watermarking information. In order ensure image quality, we will choose an appropriate rate, this rate is 0.25.
3) Apply Bicubic interpolation with scaling factor 0.25. This is our watermark information.
4) h_LL1,h_LH1,h_HL1,h_HH1 and w_LL1, w_LH1, w_HL1, w_HH1
5) Apply SVD on three levels preceded by stationary wavelet transform on both the images.
6) Perform SVD on the h_LL1 coefficient of the cover image.
$$[U_i, S_i, V_i] = svd(h\_LL1) \quad (1)$$
Where Ui,Vi are orthogonal matrices of an image and Si is singular matrix and i indicate a level of SVD.
7) Perform SVD on the w_LL1 coefficient of the watermark image.
$$[U_j, S_j, V_j] = svd(w\_LL1) \quad (2)$$
8) Modify the singular value of Si by embedding the singular value of watermark image such that
$S_m = S_i + \text{alpha} * S_j$
Where □m is modified singular matrix of Siand alpha denotes the scaling factor, is used to have power over the power of watermark signal
9) Embed signular matrices with orthogonal matrices for final watermark image as W with below formula
$$W = U_i * S_m * V_i' \quad (4)$$
10) Perform the two level inverse DWT (IDWT) on the DWT transformed image, to obtain the watermarked image on four coefficients: newhost_LL,h_LH1,h_HL1,h_HH1

Input: Watermarked Image
Output: Tampered Image

11) Apply large and small tampering on watermarked image for security and robustness

Input: Cover Image and Tampered Image
Output: Detect Tampering Location

12) Calculate SIFT key descriptor for both images using this formula:
$$des = \frac{des}{\sqrt{sum(des)^2}} \quad (5)$$
Where des is key descriptor and des initialize to 128 unit length
13) Find key point location using scale orientation.
14) For each descriptor in the original image, select its match to tampered image.
15) Detect the ratio of angles (acos of dot products of unit vectors) ,the ratio of Euclidean distances for small angles near about close approximation.
16) Find matches between original image and tampered image and also create matchtable.

Extraction Algorithm
Input: Watermarked Image
Output: Extracted Watermark Image

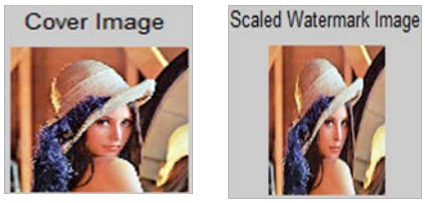
17) Apply two level DWT transform to decompose the watermarked image W into four overlapping sub-bands (wm_LL1,wm_LH1,wm_HL1,wm_HH1).
18) Apply SVD to wm_LL3 sub band i.e.,
$$[U_m, S_m, V_m] = svd(wm\_LL1) \quad (6)$$
19) Modify the singular value of Si by extracting the singular value of watermarked image such that
$$S_j = (S_m - S_i)/\text{alpha} \quad (7)$$
20) Extract signular matrices with orthogonal matrices for final extracted watermark image as W with below formula:
$$W = U_m * S_i * V_m' \quad (8)$$
21) Decrypt watermark image using stream cipher.
22) Classify data using PNN on cover image and watermarked image on the basis of image features.
23) Calculate PSNR and MSE value of watermarked and cover image.
$$MSE(x) = \frac{1}{m} \|x - x\hat{}\|^2 = \frac{1}{m} \sum_{i=1}^{N} (x - x\hat{})^2 \quad (9)$$
Where x is cover image, x^ is watermarked image, N is the size of thecover image

$$PSNR(x) = \frac{10 * \log((\text{double}(m).\hat{}2))}{MSE(x)} \quad (10)$$
Where m is the maximum value of the cover image
24) Calculate normalized cross-correlation between cover image and watermarked image.
$$\text{L2nrom} = \frac{sum(sum(O\_img * w\_img))}{sum(sum(O\_img * w\_img))} \quad (11)$$
Where L2norm is normalized cross-correlation, O_img is cover image and w_img is a watermarked image.

4 PERFORMANCE ANALYSIS

In this paper, several color images of size 512 X 512 are used as the cover image. The watermark is a scaled image and the size of the watermark is same as the cover image.

A. Read Cover Image and Generate Watermark Image using bi-cubic



(a) (b)

Figure 2. (a) Show Cover Image (b) Scaled Watermark Image

B. Encrypt Watermark Image

Figure.3. Show Encrypted Watermark Image

C. Embedding Process

Figure.4. Show Embedded Image

D. Attacks:

Figure 5. Show Attacked Image

E. Decrypt Watermark Image

Figure 6. Show Decrypted Image

F. Extract Watermark Image

Figure.7. Show Extracted Image

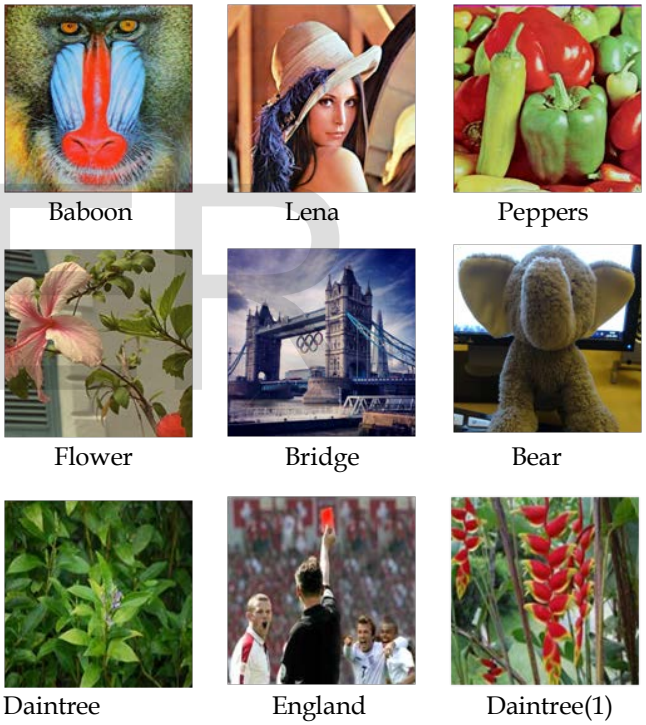


Figure 8 Experimental Images

The original lena image is shown in Fig. 2(a) and Fig. 2(b) shows the scaled watermark image. After embedding the watermark using the proposed scheme, watermarked image is obtained which is shown in Fig.4. Finally, the extracted watermark is shown in Figure.7 which is same as the embedded one.

TABLE1
PSNR AND L 2NORM COMPARISON BETWEEN BASE [2] AND PRO POSED SYSTEM

Image	PSNR		L2Norm	
	Base	Proposed	Base	Proposed

Baboon	26.78	36.37	0.0282	1.00
Lena	26.24	36.39	0.0255	1.00
Peppers	26.13	36.39	0.0236	1.0313
Flower	26.62	36.37	0.0253	1.0316
Bridge	28.17	36.38	0.0244	1.0287
Bear	27.55	36.39	0.0255	1.0334
Daintree	28.09	36.39	0.0219	1.0607
England	27.54	36.39	0.0255	1.0326
Daintree(1)	26.71	36.41	0.0246	1.0364

In this research, two performance parameters have been used to demonstrate the performance of the proposed method. The two parameters are- PSNR and L2Norm.
It can be seen from the Table1 that the high value of PSNR and L2Norm are evaluated from the proposed method compared to the existing methods for all images.

TABLE 2.
SHOWS TIME VALUE BETWEEN ENCRYPTED IMAGE AND DECRYPTED IMAGE

Image	Encryption Time	Decryption Time
Baboon	0.5873	0.5718
Lena	0.6227	0.8507
Peppers	0.5821	0.5727
Flower	0.6084	0.5677
Bridge	0.6285	0.5720
Bear	0.5898	0.5727
Daintree	0.5691	0.5614
England	0.5681	0.5566
Daintree(1)	0.5640	0.5625

TABLE 3
SHOWS PSNR AND L2NORM VALUE BETWEEN COVER IMAGE AND GA IMAGE

Image	Proposed PSNR	Proposed L2Norm
Baboon	7.89	0.4770
Lena	6.98	0.4403
Peppers	7.69	0.4266
Flower	8.96	0.5020
Bridge	7.74	0.4418
Bear	7.59	0.3115

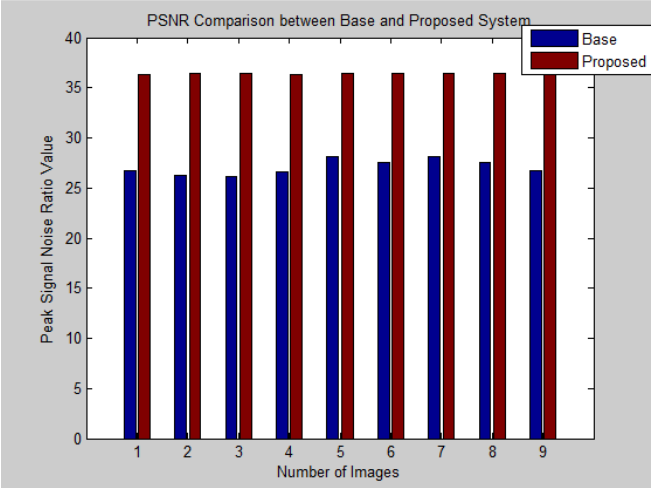
TABLE 4.
SHOWS PSNR AND L2NORM VALUE BETWEEN COVER IMAGE AND CA IMAGE

Image	Proposed PSNR	Proposed L2Norm
Baboon	26.86	1.015
Lena	29.90	1.018
Peppers	31.72	1.023
Flower	31.10	1.024
Bridge	27.56	1.014
Bear	30.05	1.011

TABLE 5.
SHOWS PSNR AND L2NORM VALUE BETWEEN COVER IMAGE AND NA IMAGE

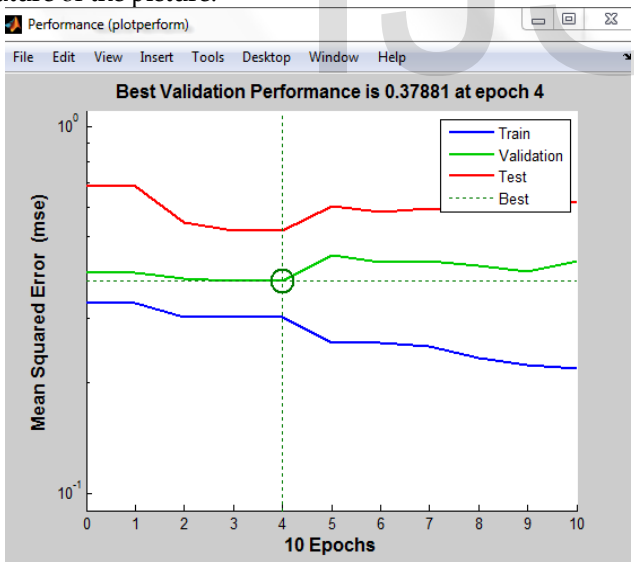
Image	Proposed PSNR	Proposed L2Norm
Baboon	24.78	1.0263
Lena	24.52	1.0249
Peppers	24.70	1.0305
Flower	25.02	1.0309

Bridge	24.59	1.0270
Bear	24.35	1.0179

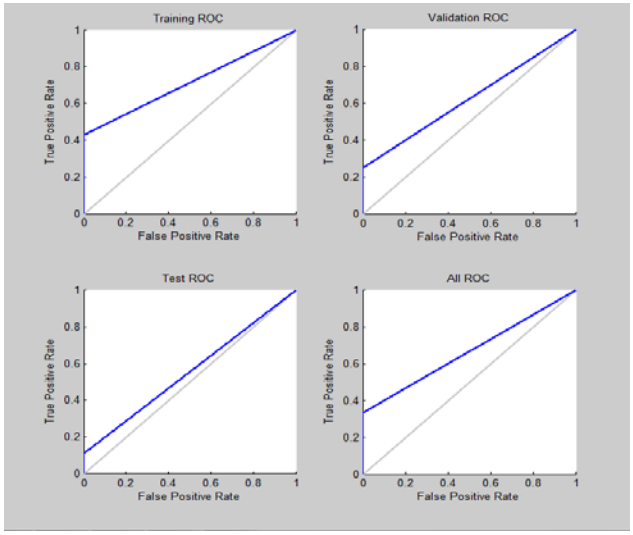


Graph 1. PSNR Comparison between Base[2] and Proposed System

Graph1 has demonstrated the quantized examination of the PSNR of various pictures utilizing Base framework (blue color) and by Proposed Approach (red color). It is clear from the plot that there is an increase in the PSNR estimation of pictures with the utilization of the proposed strategy over existing systems. This diminishing speaks to change in the target nature of the picture.



Graph 2. Shows MSE value between Cover image and Watermarked Image



Graph 3. Shows Receiver Operating Characteristics (ROC)

5 CONCLUSION

In this research, self embedding and tampering detection using two level discrete wavelet transform (2DWT) with singular value decomposition (SVD), and Probabilistic Neural Network (PNN) method. This property proves the robustness of the proposed method. The proposed method is also capable of locating the tampered areas when the image is attacked by the third parties.The combination of both feature-based and block-based different techniques can help and improve the expected results. Acceptable results are found. The results confirm the excellent invisibility of the watermarked image (PSNR = 52.67dB), as well as the satisfactory watermarked image (MSE = 0.3513) using PNN classifier. The proposed algorithm is superior to other existing techniques reported in the literature in terms of invisibility. In our future work, we plan to improve the method by reducing the false matching rate. D
Different tests will conduct to verify the robustness of the watermarked image. The test involved the use of various common attacks such as JPEG compression, rotation, Gaussian noise, cropping, and median filter against the watermark.

ACKNOWLEDGMENT

We would like to present our gratitude to Professor Naveen Hemrajani, HOD CSE (JECRC) Dr. Dinesh Goyal principal Gyanvihar University Jaipur for their guidance and support.We would like to thanks for precious or valuable information they provided us.We would like to thanks our family members for love and care.

REFERENCES

[1] Nirupma Tiwari and Dr.Naveen Hemrajani, "A Novel Frequency Domain Based Watermarking", International Journal of Innovations in Engineering and Technology (IJIET)2013, pp: 187-191.

[2] Nirupma Tiwari1, Monika Sharma2 , Manoj Kumar Ramaiya3,Naveen Hemrajani," DWT based Self-Embedding watermarking", UACEE International Journal of Advances in Computer Science and its Applications – IJCSIA 2013 , pp: 116 119.

[3] Pratibha Sharma and Shanti Swami," Digital Image Watermarking Using 3 level Discrete Wavelet Transform", Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013), pp: 129-133.

[4] Pooja Kulkarni, shraddha bhise and sidhana khot," Review of Digital Watermarking Techniques", International Journal of Computer Applications January 2015(0975 – 8887) Volume 109 – No. 16, , pp: 40-44.

[5] Yahya AL-Nabhani, Hamid A. Jalab *, Ainuddin Wahid, Rafidah Md Noor," Robust watermarking algorithm for digital imagesusing discrete wavelet and probabilistic neural network",1319-1578 , The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University,2015.

[6] https://en.wikipedia.org/wiki/Stream_cipher

[7] https://en.wikipedia.org/wiki/Bicubic_interpolation

[8] Takwa Chihaoui, Sami Bourouis, and Kamel Hamrouni, COPY-MOVE IMAGE FORGERY DETECTION BASED ON SIFT DESCRIPTORS AND SVD- IVP-107, ATSIP', Sousse, Tunisia, pp 125-129,March 2014.

[9] Ramesh Chand Pandey, Sanjay Kumar Singh, K. K. Shukla and Rishabh Agrawal, Fast and Robust Passive Copy-Move Forgery Detection Using SURF and SIFT Image Features,10.1109@ICIINFS.2014.7036519

[10] Bashar, M., Noda, K., Ohnishi, N., & Mori, K. (2010). Exploring duplicated regions in natural images. IEEE Transactions on Image Processing,(99), 1,2010.

[11] Kayvan. Ghaderi*, Fardin. Akhlaghian**, and Parham. Moradi*,"A New Robust Semi-Blind Digital Image Watermarking Approach Based on LWT-SVD and Fractal images",2013 IEEE.

[12] Song Huang and Wei Zhang, Wei Feng and Huaqian Yang," Blind Watermarking Scheme Based on Neural Network", 978-1-4244-2114-5/08/ IEEE,pp 5985- 5989,2008.

ACKNOWLEDGMENT

First Author- Nirupma Tiwari is currently pursuing Phd* degree program in Computer Science & engineering in Suresh Gyanvihar University, Jaipur India. E-mail: girishniru@gmail.com.

Sceond Author- Dr.naveen hemrajani, Phd* Email id- navin_h@yahoo.com.

Third Author- Dr. Dinesh Goyal, Principal of School of Engineering Suresh Gyanvihar university jaipur Phd* **Email id dinesh.goyal@mygyanvihar.com**