IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. II (May.-June. 2017), PP 23-29
www.iosrjournals.org

A Robust Technique For Digital Watermarking using 3-DWT-SVD and Pattern Recognition Neural Network

Yamini Gupta, Nirupma Tiwari
Dept. of CSE/IT SRCEM College Gwalior, India
Dept. of CSE/IT SRCEM College Gwalior, India

Abstract: *Digital image watermarking (DIW) is the way which is resilient to many attacks on digital media based on image where data authentication is full by embedding a watermark in image characteristics. This work incorporates a novel method for DIW using three level discrete wavelet transform (3DWT)-Singular value decomposition (SVD) and PNN classifier with various attacks. Extensive experiments present that proposed watermarking algorithms have high robustness and a good imperceptibility to numerous usual image processing attacks, such as Gaussian blurring, noise attack, Swirl Attack and Negative Attack. To estimate the algorithm efficacy and extracted quality of image watermarking, we used extensively known measurements of image quality function, for example SNR and L2 normalization (L2Norm). Results indicate the excellent invisibility of the extracted watermark image (SNR = 45.68dB), as well as exceptional watermark extraction (L2Norm = 3.0329).*

Keywords: *DWT, SVD, SNR, Attacks, L2Norm, PNN, Accuracy, FAR, FRR.*

I. Introduction

Digital image watermarking is a technology which is complete to protect digital data for example images, video & audio from prohibited manipulations. The common characteristics of digital watermarking are: insensitivity, secrecy, and robustness. Therefore, it must withstand the attacks like JPEG compression, noise in the channel (during transmission) and common image processing operations and shall be secure to any attempt made through unauthorized user to watermark tamper [1].

DWT

Embedding the watermark into an image is a difficult task, as it alters the information in the original image and hence the appearance. Using DWT, an image is decomposed into four unique frequency sub bands (LL, LH, HL, HH). The HL frequency sub-band is selected, which covers mid frequencies. It is robust against different filtering noises and geometric noises. Only fine information of the image is present in it. Hence insertion of the watermark into the HL sub-band does not alter the original image information and it retains its appearance to an optimum level.

SVD

Insertion of the watermark into the frequency sub-band of an image results in little distortion in the watermarked image. SVD of an image gives three singular matrices (U,S, V). Where U and V are orthogonal matrices and S is the diagonal matrix. The watermark data will be inserted into the original image singular values in S matrix. The modification of the singular values does not lead to distortion in the original image. Hence SVD is used to embed the watermark in original image [2].

II. Literature survey

Reema Jain (2015) et al present that provides Digital Image Watermarking based on Hybrid DWT-FFT with different malicious attacks (JPEG compression, Salt & Peppers Noise, Gaussian Noise, Blurring and Blurring & Noise). PSNR is computed to measure quality of image for proposed method for improved results as compared to previous information hiding methods [3].

Shabir A. Parah (2015) et al presents that present scenario huge amount of information is being shared as digital content. Digital content, copy without apparent loss in value is not a complex task. Because of this, there are additional digital information copying chances. Thus, there is a great prohibiting requirement like illegal digital media copying. DWM is a powerful solution to this problem [4].

Yahya AL-Nabhani (2015) et al presents that develop an improved method for creating watermarked images with high invisibility. At the time of extraction, watermarks can be effectively removed without the required for the original image. Developed DWT with the Haar filter to embed a binary watermark image in particular coefficient blocks. A probabilistic NN is used to the watermark image extract. To estimate the algorithm efficiency and the watermark images extracted quality, we used extensively known quality of image function measurements, for example PSNR and NCC [5]. Chunlei Li (2015) et al presented that embedding alterations are then distributed to important coefficients which preserve huge perceptual capacity through SAD quantizing. Meanwhile, the either modulation approach is employed to control quantization artifacts and robustness growth. In such a framework, the blind watermark extraction can be straightforwardly attained with the watermarking secret keys which only shared by the embedder and extractor for advanced security [6].

D.Vaishnavi (2015) et al presented that two discrete approaches for robust and invisible watermarking image are proposed in RGB color space. First method, watermark gray scale is embedded on elements of blue color channel and in another method, the blue color channel watermark elements are embedded on the blue color channel elements of host image [7].

III. Proposed work

In this algorithm, firstly take a color cover image and watermark image. Applying 3-DWT, decompose the cover image and watermark image into four different bands. In the second step, take LH band and apply SVD on this band to determine the singular values. Embed the watermark image into cover image with scaling factor. Extract the feature of cover image and database which contain 34 images- 17 cover image, 17 watermarked image on first moment and thresholding of LH and HL band. In the fourth step, apply different types of attack on watermarked image. In the classification process, store all features of image in .mat file for classification, PNN take 5 inputs, 10 hidden layer and one output layer. In the extraction process, extract watermark image from embedded image. 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 aim should be set appropriately at the time of training samples, because whether a smaller and bigger train aim does harm to the generalization PNN ability.

Embedding Algorithm
Input: Cover Image
Output: Watermarked Image

1) Read cover image 'CI' and watermark image 'WI' with NXN size.
2) Apply 3-DWT on the CI and WI to split into four groups: L_L11,L_H11,H_L11,H_H11 and w_LL11,w_LH11,w_HL11,w_HH11
3) Apply SVD on three levels preceded by DWT on both the images.
4) Perform SVD on the L_H11coefficient of the cover image.

$$[U_i, S_i, V_i] = svd(\text{L\_H11})(1)$$

Where U_i,V_i are orthogonal matrices of an image and S_i is singular matrix and i indicate a level of SVD

5) Perform SVD on the w_LH11coefficient of the watermark image.

$$\left[U_j, S_j, V_j\right] = svd(\text{w\_LH11})(2)$$

Modify the singular value of S_i by embedding the singular value of watermark image such that

$$\mathrm{S_m} = \mathrm{S_i} + \mathrm{alpha} * \mathrm{S_j}(3)$$

Where S_{m} is modified singular matrix of $S_i$and alpha denotes the scaling factor, is used to have power over the power of watermark signal

6) Embed singular matrices with orthogonal matrices for final watermark image as W with below formula:

$W = U_i * S_m * V_i{}'(4)$

7) Perform the three level inverse DWT (IDWT) on the DWT transformed image, to obtain the watermarked image on four coefficients: L_L11,newhost_LH,H_L11,H_H11

Input: Watermarked Image
Output: Attacked Image

8) Apply Gaussian blur (GB), Noise attack (NA), Swirl Attack (SA) and Negative attack (NGA) on watermarked image for security and robustness.

Extraction Algorithm
Input: Watermarked Image
Output: Extracted Watermark Image

9) Apply three level DWT transform to decompose the watermarked image W into four overlapping sub-bands (e_LL11,e_LH11,e_HL11,e_HH11).
10) A Apply SVD to e_LH11sub band i.e.,

$$[U_m, S_m, V_m] = svd(\text{e\_LH11})(5)$$

11) Modify the singular value of S_i by extracting the singular value of watermarked image such that

$$\mathrm{S_j} = \frac{(\mathrm{S_m} - \mathrm{S_i})}{\mathrm{alpha}}(6)$$

12) Extract singular matrices with orthogonal matrices for final extracted watermark image as W with below formula:

$$W = U_m * S_j * V_m{}'(7)$$

13) Perform the three level inverse DWT (IDWT) on the DWT transformed image, to obtain the extracted watermark image on four coefficients w_LL11,newwatermark_LH,w_HL11,w_HH11.
14) Classify data using CFBN on CI, W and attack images on the basis of image features.
15) Calculate Signal Noise Ratio (SNR) and Mean Square Error (MSE) value of watermarked and cover image.
$MSE(x) = \frac{1}{N}||x - x^{\wedge}||^2 = \frac{1}{N}\sum_{i=1}^{N}(x - x^{\wedge})^2$ (8)
Where x is cover image, x^ is watermarked image, N is the size of the cover image
$SNR(x) = \frac{10\ X\log\left((double(m).^{\wedge}2)\right)}{MSE(x)}$(9)
Where m is the maximum value of the cover image
16) Calculate normalized cross-correlation between cover image and watermarked image.

$$L2Norm = \frac{sum(sum(O\_imgXw\_img))}{sum(sum(O\_imgXw\_img))}(10)$$

Where L2norm is normalized cross-correlation, O_img is cover image and w_img is a watermarked image.

Classification Algorithm
Input: Dataset Features and Labels
Output: PSNR and MSE
17) Extract color feature and store feature vector of mean value using the formula:

$$M = \sum_{N}^{i=1}\sum_{N}^{j=1}\frac{1}{N} \times CI \qquad (11)$$

Where CI= L_H11 and H_L11 is cover image bands, N is number of pixels
18) Extract shape features using thresholding on CI.
19) Repeat Step 18 to step 19 until all dataset images (First 17 are cover images and other are watermarked images).
20) Classify the data using Pattern network with 5 input neurons, 10 hidden neurons and 1 output neuron.
21) Calculate PSNR and Accuracy using below formula:

$$PSNR(x) = \frac{10\ X\log\left((255.^2)\right)/log10}{MSE(x)} \qquad (12)$$

$$Accuracy = \frac{(TP+TN)}{(TP+FP+FN+TN)}(13)$$

Where Confusion matrix consists of four variables namely:
1. True positive (TP): The percentage of total number of genuine images taken as genuine, closer to 1 is better.
2. True negative (TN): The percentage of total number of genuine images taken as forged, closer to 1 is better.
3. False positive (FP): The percentage of forged images taken as genuine, closer to 0 is better.
4. False negative (FN): the percentage of forged images taken as forged, closer to 0 is better.

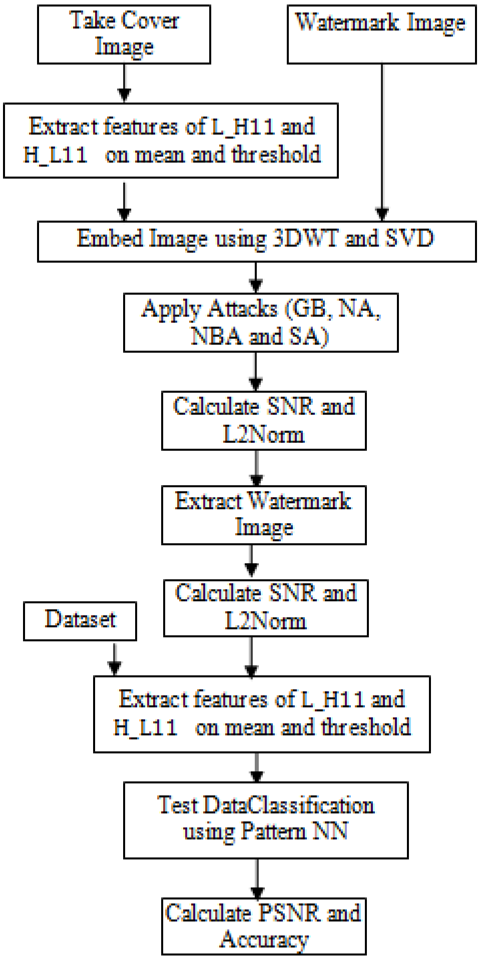

Take Cover Image
Watermark Image
Extract features of L_H11 and H_L11 on mean and threshold
Embed Image using 3DWT and SVD
Apply Attacks (GB, NA, NBA and SA)
Calculate SNR and L2Norm
Extract Watermark Image
Calculate SNR and L2Norm
Dataset
Extract features of L_H11 and H_L11 on mean and threshold
Test DataClassification using Pattern NN
Calculate PSNR and Accuracy

Fig1. Block diagram of My Approach

IV. Result simulation

In this paper, several color images of size 512 X 512 are used as the cover image. It is performed on MATLAB platform using Image Processing and Neural Network Toolbox. In this research, two performance parameters have been used to demonstrate the performance of the proposed method. The two parameters are- SNR and L2Norm.

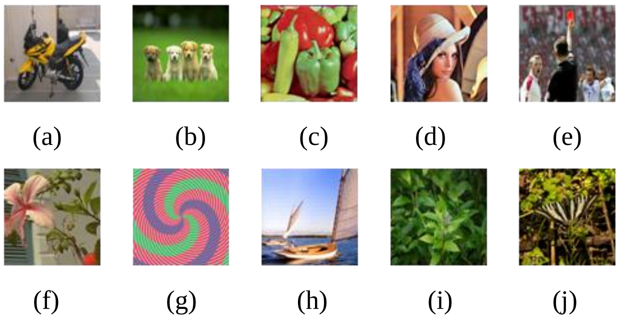


Fig2. Experimental Dataset

TABLE 1: Snr Comparison Between Previous Approachand My Approach On Blurring Attack For Watermarked Image

Image	Previous Approach SNR [3]	My Approach SNR
(a)	32.96	45.52
(b)	38.04	45.64
(c)	36.33	45.37
(d)	32.19	45.39
(e)	37.00	45.55

(f)	36.05	45.43
(g)	24.76	45.38
(h)	31.36	45.68
(i)	41.43	45.62
(j)	27.50	45.47

Table 2: Snr Comparison Between Previous Approachand My Approach On Noisy Attack On Watermarked Images

Image	Previous Approach SNR [3]	My Approach SNR
(a)	20.01	45.53
(b)	19.59	45.63
(c)	19.72	45.39
(d)	19.63	45.40
(e)	19.78	45.55
(f)	20.16	45.44
(g)	19.40	45.45
(h)	19.32	45.67
(i)	19.26	45.61
(j)	18.92	45.48

Table 3: Snr Comparison Between Previous Approach And My Approach On Noisy Attack On Watermarked Images

Image	My Approach Watermarked L2Norm	My Approach Extracted L2Norm
(a)	0.9882	1.5537
(b)	0.9914	1.9285
(c)	0.9888	1.7088
(d)	0.9856	1.4960
(e)	0.9892	1.7934
(f)	0.9902	1.7496
(g)	0.9471	1.2616
(h)	0.9915	1.1466
(i)	0.9849	3.0329
(j)	0.9067	1.9599

Table 4: Snr Comparison Between Previous Approachand My Approach

Image	Extracted SNR	
	Previous Approach	***My Approach***
(a)	11.54	46.68
(b)	8.85	46.59
(c)	10.61	46.65
(d)	10.77	46.28
(e)	9.72	46.65
(f)	10.81	46.57
(g)	11.36	45.95
(h)	14.04	46.04
(i)	7.86	47.34
(j)	7.91	46.84

TABLE I. COMPARISON BETWEEN NBA, SA, GA AND NA

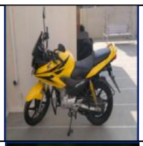
Negative Attack	Swirl Attack	Blur attack	Noise attack
			

TABLE II. PSNR, ACCURACY AND MSE USING PNN METHOD

Performance	**Average PSNR**	**Average MSE**	**Average Accuracy (%)**
Proposed System	58.012	0.1028	80

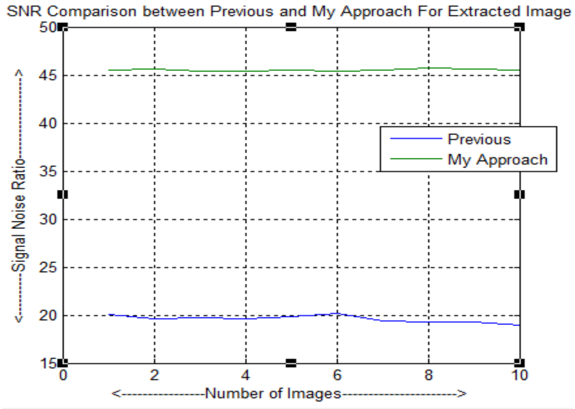
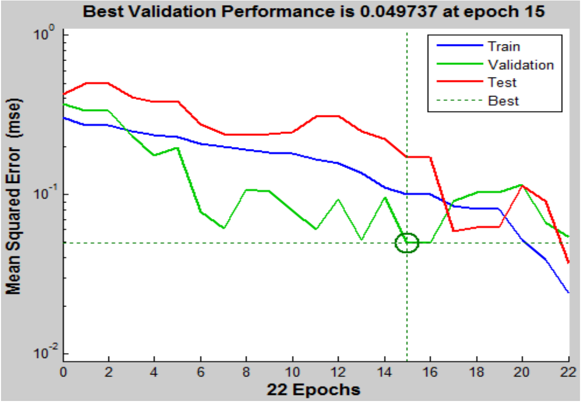
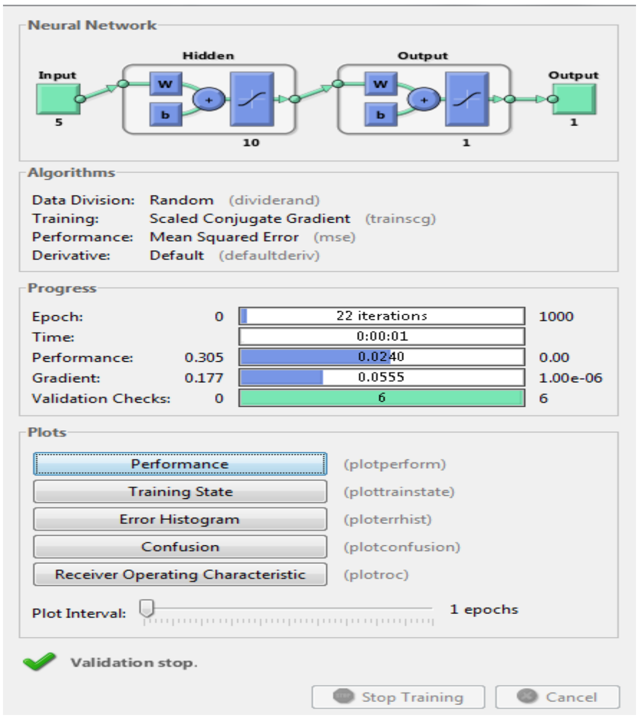


Fig 3.




Neural Network
Input
5
Hidden
W
b
+
10
Output
W
b
+
1
Output
1

Algorithms

Data Division: Random (dividerand)
Training: Scaled Conjugate Gradient (trainscg)
Performance: Mean Squared Error (mse)
Derivative: Default (defaultderiv)

Progress

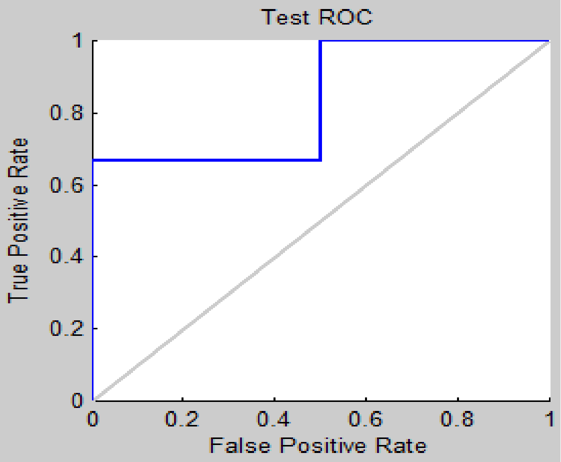
Epoch:	0	22 iterations	1000
Time:		0:00:01	
Performance:	0.305	0.0240	0.00
Gradient:	0.177	0.0555	1.00e-06
Validation Checks:	0	6	6

Plots

Performance (plotperform)
Training State (plottrainstate)
Error Histogram (ploterrhist)
Confusion (plotconfusion)
Receiver Operating Characteristic (plotroc)

Plot Interval: 1 epochs

✓ Validation stop.



V. Conclusion

This work incorporates a novel technique for DIW using three level DWT-SVD and PNN with different malicious attacks (NBA, SA, GA AND NA). Table 1 and Table 2 shows the effectiveness of the proposed method in terms of SNR of watermarked image & extracted watermark. The proposed algorithm is superior to previous methods reported in the literature in invisibility terms. In our future work, we plan to improve the method by reducing the false positive rate.

References

[1] Purnima K. Sharma, Paresh Chandra Sau and Dinesh Sharma,” Digital Image Watermarking: An Approach by Different Transforms using Level Indicator”, 2015 International Conference on Communication, Control and Intelligent Systems (CCIS) 2015 IEEE.

[2] Niteesh Shrinivas Naik, Naveena N and K. Manikantan,” Robust Digital Image Watermarking using DWT+SVD approach” 2015 IEEE International Conference on Computational Intelligence and Computing Research.

[3] Reema Jain, Mahendra Kumar, Arihant Kumar Jain, and Manish Jain,” Digital Image Watermarking using Hybrid DWT-FFT Technique with Different Attacks”, This full-text paper was peer-reviewed and accepted to be presented at the IEEE ICCSP 2015 conference2015 IEEE.

[4] Shabir A. Parah, Shazia Ashraf and Ayash Asharf,” Robustness Analysis of a Digital Image Watermarking Technique for Various Frequency Bands in DCT Domain”, 2015 IEEE.

[5] Yahya AL-Nabhani, Hamid A. Jalab, Ainuddin Wahid, Rafidah Md Noor,” Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network”, Journal of King Saud University – Computer and Information Sciences (2015) 27, 393–401.

[6] Chunlei Li, Zhaoxiang Zhang , Yunhong Wang , Bin Ma and Di Huang,” Dither Modulation of Significant Amplitude Difference for Wavelet Based Robust Watermarking”, Preprint submitted to Neurocomputing March 27, 2015.

[7] D.Vaishnavia and T.S.Subashini,” Robust and Invisible Image Watermarking in RGB Color space using SVD”, International Conference on Information and Communication Technologies (ICICT 2014) Procedia Computer Science 46 (2015) 1770 – 1777.