Comparative Analysis of Digital Image Watermarking Techniques - SVD based Algorithms in Different Wavelet Domains

Anu Bajaj
M.Tech,
Dept. of Computer Science and Engineering
G.J.U. S & T, Hisar, Haryana, India
er.anubajaj@gmail.com

Abstract—**The aim of digital watermarking is to hide some secret information or logo into the multimedia content for protecting the content from unauthorized access or illegal use. Digital image watermarking is a promising domain for various applications, for example, ownership identification, copy protection, authentication, broadcast monitoring, tamper detection etc. In this paper we are going to discuss two different techniques with our proposed one which all are based on SVD but in different wavelet domains that is RDWT, DWT and IWT. Comparison between these techniques is performed on the basis of their computation time, watermarked image and extracted watermark fidelity, and the most important robustness against attacks on the basis of PSNR and correlation coefficient. The graphical representation shows that the proposed algorithm based on IWT-SVD works well than the other two.**

Keywords-Digital Watermarking, DCT, DWT, IWT, RDWT, SVD, PSNR, NCC

I. Introduction

Commercialization of the multimedia content increases day by day due to the use of Internet at a rapid rate, so is the cyber forgery. To protect the contents of the owner, the technique named digital watermarking emerged. It hides secret information/image in such a way that it is imperceptible to human eye and also robust against common signal processing operations and attack. At the same time it can positively identify the owner by comparing with the original content/key, if required. The watermarking system consists of two functions, viz. embedding function, and extracting/detecting function. The embedding function embeds the secret message called watermark into the original image and then the watermarked image is passed onto the internet where it may be passed through general processing functions or attacked by an attacker either to remove or destroy the watermark. The extracting/ detecting function is used to extract the watermark for verification purposes or to check the presence of watermark for monitoring purposes. The general watermarking system is shown in Fig 1.

The different watermarking algorithms have to fulfill different requirements as per the required applications. The three basic requirements as defined by Cox et al. [1] are:

1) *Imperceptibility:*The watermarked image and the original image should be perceptually indifferent to human eye.

2) *Robustness:*The watermark should not be removed or destroyed at least by common signaling operations.

3) *Capacity/Payload:*The watermark should carry enough information to represent uniqueness and meaningful information.

The imperceptibility and robustness are conflicting requirements. So there should be trade-off between the requirements which entirely depends on application need e.g. the watermark may be perceptible or imperceptible, it may be fragile or robust according to the application requirement.

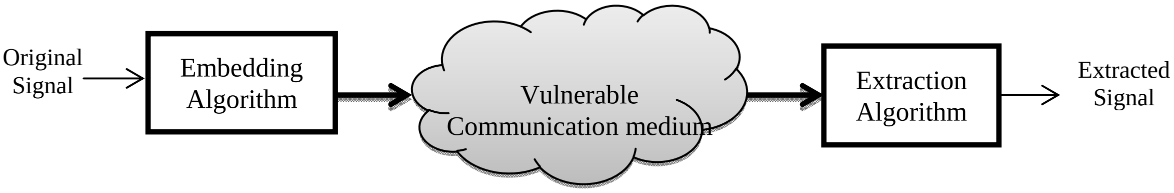


Figure 1. General Framework of Watermarking System

II. DWT-DCT-SVD Watermarking

This watermarking algorithm is generated by using DWT, DCT and SVD. As DCT based algorithms are more robust against JPEG Compression attack and DWT compression offers scalability. SVD based techniques are used as singular values provide robustness against many attacks. So, it takes the advantage of all these techniques in order to give a more robust watermarking algorithm as given by Navas et al. [2].

A. Embedding Process

1. Apply DWT to the original image A, and the watermark image W, to decompose the image into four sub-bands LL, LH, HL, and HH.
2. Apply DCT to all bands of original and watermark.
3. Apply SVD to the DCT transformed images, say S_o and S_w.
4. Modify the singular values S_o with the singular values of S_w. i.e. $S_{wmi} = S_{oi} + \alpha * S_{wi}$, , such that the value of scaling factor (α) is more in LL band and less for other three bands, here i=LL, LH, HL, and HH.
5. Apply inverse DCT then inverse DWT to get the watermarked image.

B. Extraction Process

1. Apply DWT to the watermarked image A’ and the original image A to decompose the image into four sub-bands LL, LH, HL, and HH.
2. Then apply DCT to all bands of the watermarked and original image.
3. Apply SVD to the DCT transformed images, say S'_{wm} and S_o.
4. Obtain the singular values of watermark by subtracting the SVs of original image from SVs of watermarked image i.e. $S'_{wi} = (S'_{wmi} - S_{oi})/\alpha$, where i=LL, LH, HL and HH.
5. Apply inverse DCT and then inverse DWT to get the watermark image.

III. RDWT-SVD WATERMARKING

A watermarking algorithm based on RDWT and SVD is generated. As RDWT is redundant discrete wavelet transform so, it provides complete frame expansion, and hence more robust than DWT against affine transform. And also it does not down-sample the band as it makes redundant wavelets of same size. SVD is applied then for more robustness against attacks and due to its unique property that small variation in singular values does not affect the signal energy a lot [3].

A. Embedding Process

1. Apply RDWT to the original and watermarked images to decompose into four sub-bands LL, LH, HL, and HH.
2. Apply SVD to the LL band of the transformed images.
3. Modify the singular values of original image with the singular values of watermark image i.e. $S_{wm} = S_o + \alpha * S_w$.
4. Apply inverse RDWT to get the watermarked image.

B. Extraction Process

1. Apply RDWT to the watermarked image to decompose into four sub-bands LL, LH, HL, and HH.
2. Apply SVD to the LL band of the transformed images.
3. Obtain the singular values of watermark by subtracting the SVs of original image form SVs of watermarked image. i.e. $S'_w = (S_{wm} - S_o)/\alpha$.
4. Apply inverse RDWT to get the watermark image.

IV. PROPOSED WATERMARKING-IWT SVD

Here we use IWT (Integer Wavelet Transform) with SVD. IWT has better computational efficiency than DWT. Multimedia contents store as integer values [2]. DWT does floating point transformation and hence inverse DWT truncates the floating point values to integer values [5]. But IWT performs lossless decomposition and hence it can be used for lossless data hiding. SVD is then performed on the transformed image, as SVD is more robust against attacks then traditional methods [4]. It has the unique property that even large variations in the singular values do not affect the signal energy a lot. It is reversible non-blind watermarking scheme.

A. Embedding Process

1. Apply IWT to the original and the watermark image to decompose it into four sub-bands LL, LH, HL, and HH.
2. Apply SVD to LH, HL (diagonal) bands of the images.
3. Modify the singular values of original image with that of watermark image i.e. $S_{wmi} = S_{oi} + \alpha * S_{wi}$, where i=LH, and HL.
4. Apply inverse IWT to get the watermarked image.

B. *Extraction Process*

1. Apply IWT to the watermarked and original image.
2. Apply SVD to LH, and HL (diagonal) bands of the images.
3. Obtain the SVs of the watermark by subtracting the original SVs from the watermarked image i.e. S_w'= $(S'_{wm} – S_o)/\alpha$.
4. Apply inverse IWT to get the watermark image.

V. PERFORMANCE MEASUREMENT

To check the quality of the watermarked image w.r.t the original image, PSNR (Peak Signal to Noise Ratio) is used. It can be calculated as:

$$PSNR = 10 \log_{10} \frac{N \times N}{MSE} \qquad (1)$$

Where, NxN is the size of the image, and MSE is the Mean Square Error between the original A (i, j) and the watermarked image A' (i, j), can be written as:

$$MSE = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{(A(i,j) - A'(i,j))^2}{N \times N} \qquad (2)$$

To find out the similarity between the original and extracted watermark, normalized correlation coefficient (NCC) is calculated. Its formula is:

$$NCC = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{(W(i,j) \times W'(i,j))}{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (W(i,j) \times W(i,j))} \qquad (3)$$

Where, W (i, j), W' (i, j) are the original watermark image and the extracted watermark image respectively. NCC is a value between 0 and 1. The larger the NCC value, the higher the watermark robustness.

VI. EXPERIMENTS

We used standard Lena image (Fig. 2a) of size 512x512 and a watermark of recycle logo of size 512x512. The value of scaling factor is kept constant for comparison i.e. α=0.025. The experiments are performed for different format Lena images viz. BMP, JPG, GIF, and PNG; and also the watermarks used are of different intensity pixels, e.g. more white pixeled (Fig. 2b), black and white pixeled (Fig. 2c), and more black pixeled images (Fig. 2d). Due to lack of space we are not showing all the cases, so here only png format Lena and more black pixeled watermarks are used for comparison. Different attacks are performed on the watermarked images; watermarks are then extracted from them. Some attacks are shown in Table1 rests are represented on the graphs for detailed analysis. Here, Watermarked images are compared on the basis of PSNR and extracted watermarks with the NCC. Correlation based detection is performed. The tolerance level, (τ) is set to 0.8 i.e. if the NCC is greater than τ then the algorithm is robust against that particular attack else not.

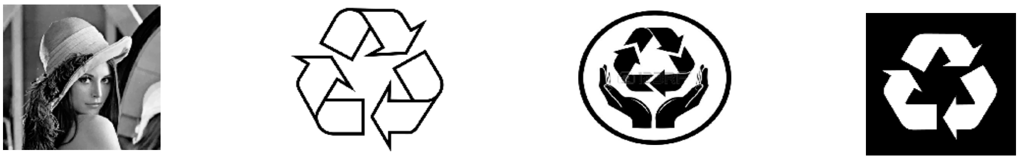
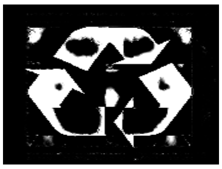
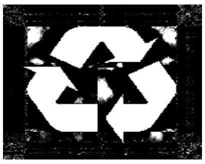
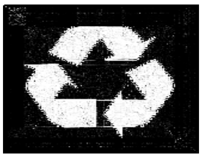
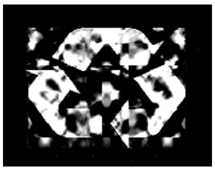
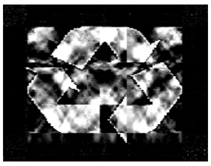
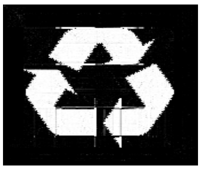
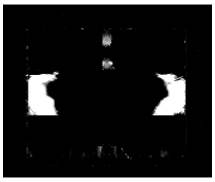
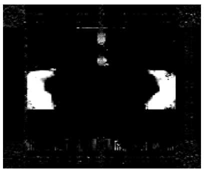
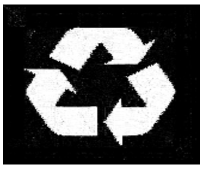
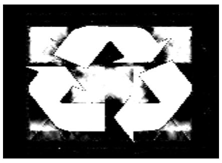
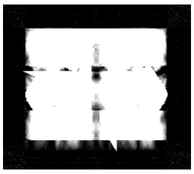
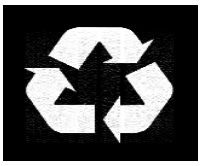
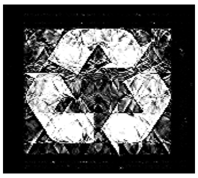
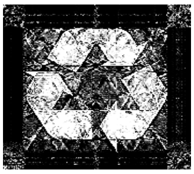
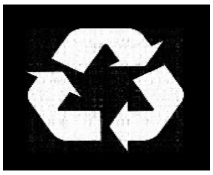


Figure 2. a. Original Image b. More White Pixels c. Black and White Pixels d. More Black Pixels

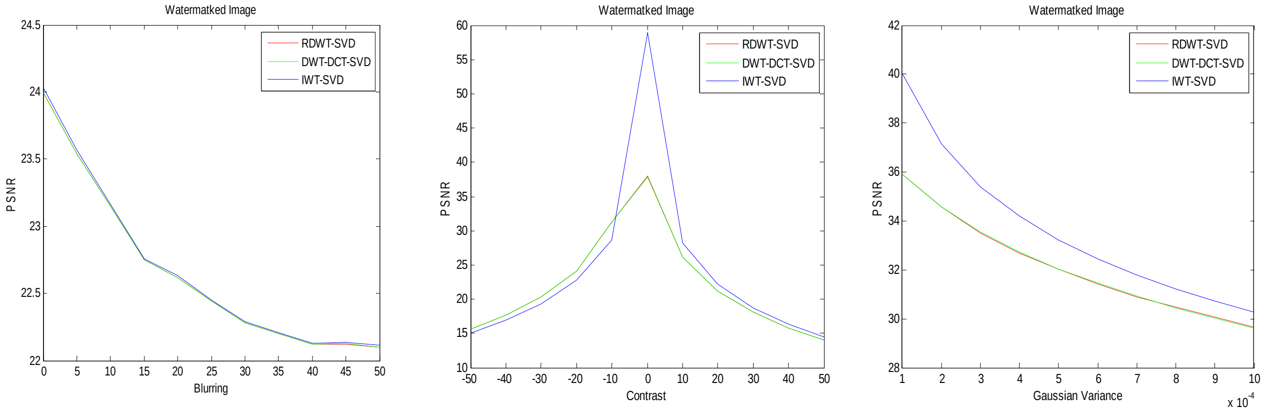
TABLE I. WATERMARKED IMAGE AND EXTRACTED WATERMARKS

	RDWT-SVD	**DWT-DCT-SVD**	**IWT-SVD**
Watermarked Image	 PSNR= 37.9272, CC= 0.99993	 PSNR= 38.0275, CC= 0.99891	 PSNR= 58.9116, CC= 0.99999
Extracted Watermark	 PSNR= 40.3897, CC= 0.99983	 PSNR= 40.8017, CC= 0.99985	 PSNR= 45.2956, CC= 0.99993
Attacks			
Brightness	Brightness PSNR= 14.4261, CC= 0.96121	Brightness PSNR= 15.4997, CC= 0.94374	Brightness PSNR= 15.747, CC= 0.94389
	Brightness  PSNR= 9.6866, CC= 0.70152	Brightness  PSNR= 14.3231, CC= 0.9123	Brightness  PSNR= 16.0236, CC= 0.93247
Cropping	Cropping PSNR= 10.0067, CC= 0.36454	Cropping PSNR= 10.0057, CC= 0.36449	Cropping PSNR= 10.118, CC= 0.36267
	Cropping  PSNR= 10.9566, CC= 0.77166	Cropping  PSNR= 10.155, CC= 0.71218	Cropping  PSNR= 17.4576, CC= 0.95208
Affine	Shear Attack PSNR= 8.0986, CC= 0.16149	Shear Attack PSNR= 8.0984, CC= 0.1615	Shear Attack PSNR= 8.1576, CC= 0.1614

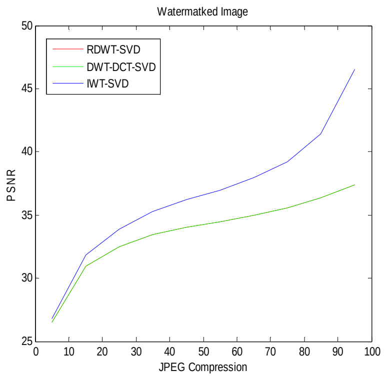
Transformation	Shear Attack  PSNR= 6.5803, CC= 0.31686	Shear Attack  PSNR= 6.5568, CC= 0.30176	Shear Attack  PSNR= 20.6521, CC= 0.97721
Histogram equalization	Histogram Equalization PSNR= 20.9969, CC= 0.99283	Histogram Equalization PSNR= 20.9966, CC= 0.99283	Histogram Equalization PSNR= 21.042, CC= 0.99294
	Histogram Equalization  PSNR= 8.518, CC= 0.7261	Histogram Equalization  PSNR= 6.6236, CC= 0.62124	Histogram Equalization  PSNR= 26.8658, CC= 0.99514
Sharpening	Sharpening PSNR= 24.2685, CC= 0.97975	Sharpening PSNR= 24.1478, CC= 0.97913	Sharpening PSNR= 24.5386, CC= 0.9781
	Sharpening  PSNR= 11.7223, CC= 0.82124	Sharpening  PSNR= 10.2193, CC= 0.74928	Sharpening  PSNR= 29.6838, CC= 0.9975

Graphical representation for Watermarked image perceptuality measured in PSNR and Extracted Watermark's robustness measured in NCC against attack's strength value.

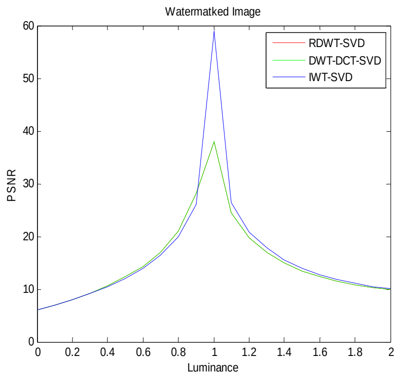
Watermarked Image (PSNR)



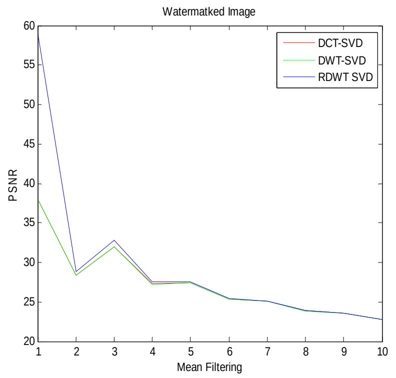
Blurring **Contrast** **Gaussian Variance**



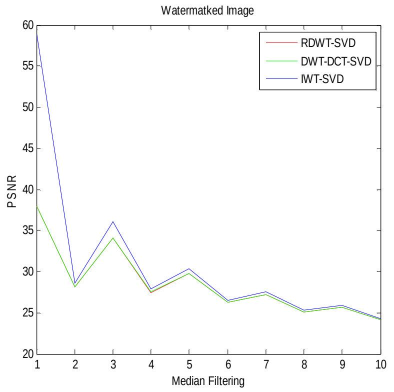
JPEG Compression



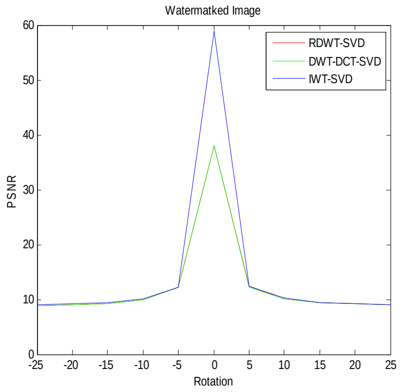
Luminance



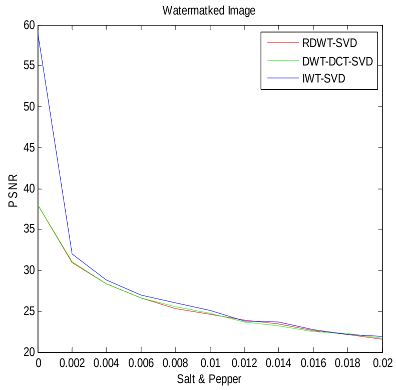
Mean Filtering



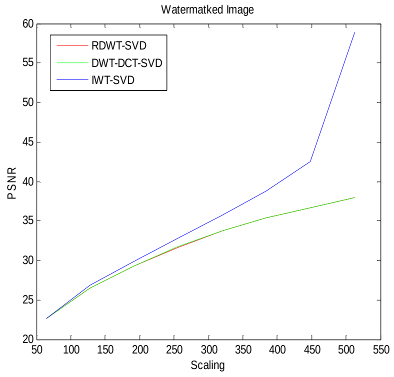
Median Filtering



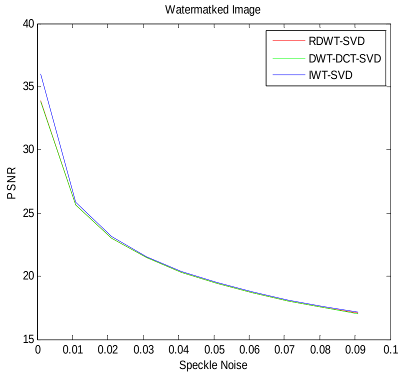
Rotation



Salt and Pepper

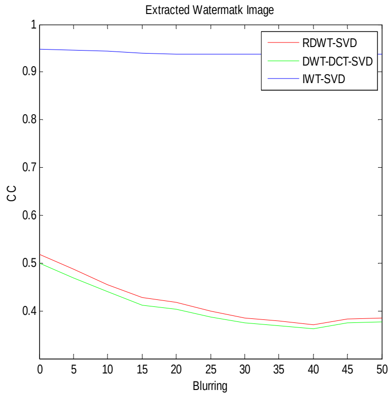


Scaling

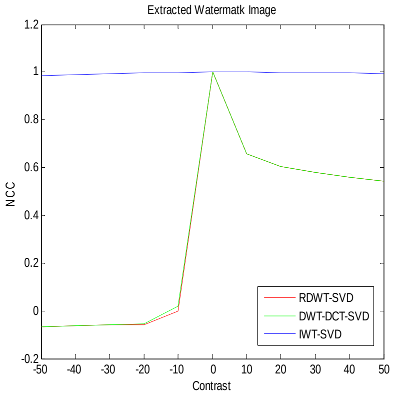


Speckle Noise

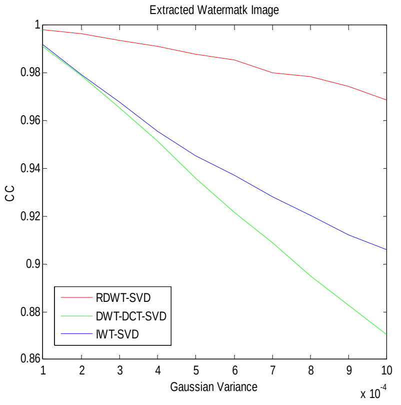
Extracted Watermark (NCC)



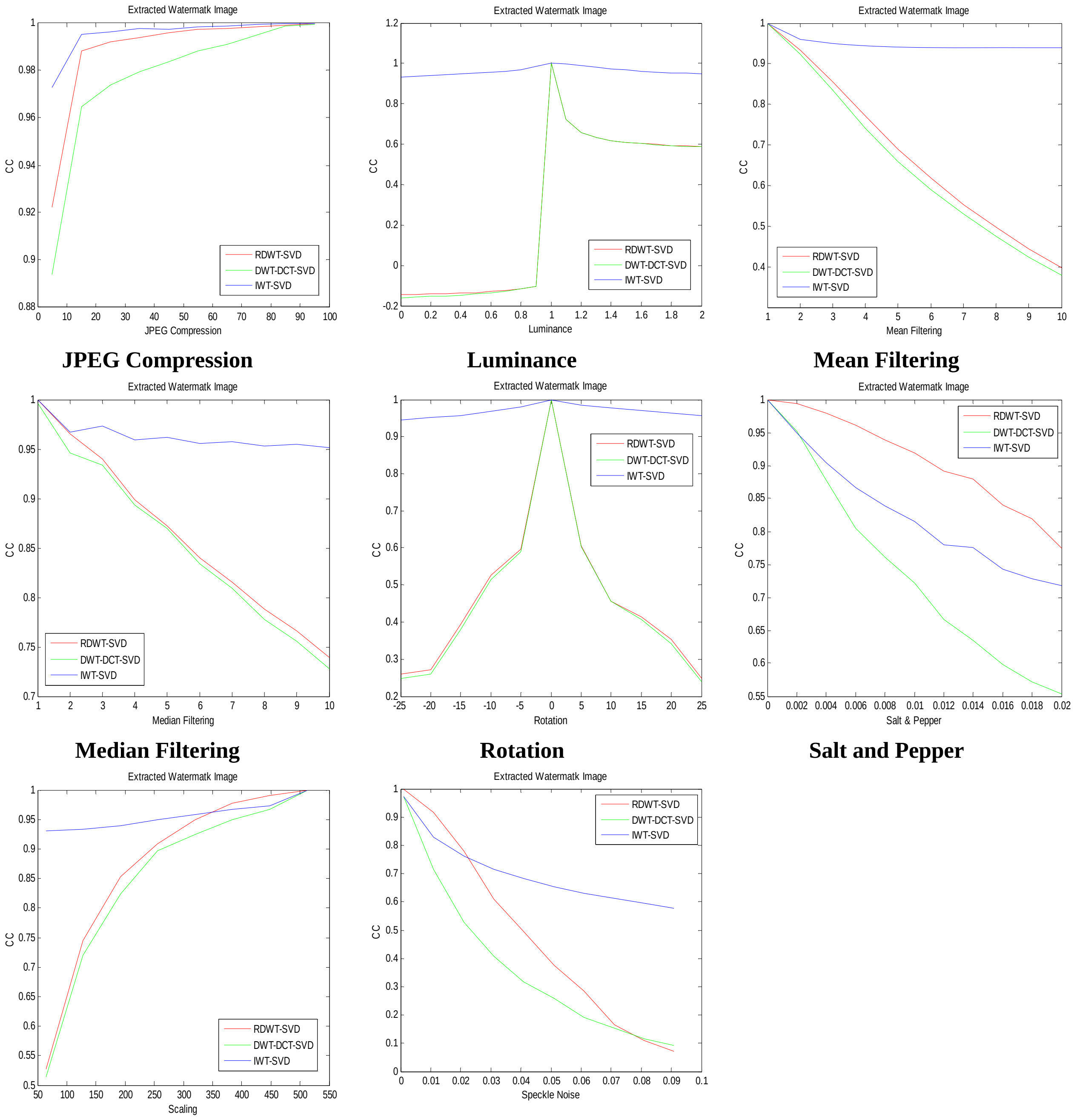
Blurring



Contrast



Gaussian Variance



JPEG Compression **Luminance** **Mean Filtering**

Median Filtering **Rotation** **Salt and Pepper**

Scaling **Speckle Noise**

Figure 3. Graphical representation for Watermarked image perceptuality and Extracted Watermark's robustness against attack's strength value.

VII. OBSERVATIONS

A. *Different Format Host Image*

Firstly, we observed the effect of different format original image on each watermarking algorithms. In RDWT-SVD watermarking the watermarked image has good PSNR in PNG format and extracted watermark has good NCC in BMP format for almost attacks for example, Gaussian noise, Rotation, median filtering, salt and pepper, affine transformation etc. DWT-DCT-SVD watermarking has no specific criteria as it shows variation for different attacks. The proposed watermarking technique IWT-SVD gave comparable results for all the formats in case of PSNR of watermarked image but for extracted watermark the PNG format gives good NCC against various attacks.

B. *Different Intensity Watermarks*

Second, we have seen the effect of intensity variation of watermarks on the watermarking techniques. RDWT-SVD technique gave good PSNR and NCC for more black pixel watermark. The rest two techniques gave comparable results for all types of watermark that is, they did not get much affected by the intensity of watermark.

C. Imperceptibility of Watermarked Image

Third, we talk about the perceptibility of the watermarked image. The proposed technique has higher value of PSNR than the other two which gave comparable values. Even after applying attacks on the watermarked image the quality does not degrade enough.

D. Computation Time

Of these algorithms, IWT-SVD approach wins the race; it takes time of 0.8 seconds in round figures both for embedding and extraction. Rest algorithms take more than 1 second to watermark. DWT-DCT-SVD is the first runner up in extracting but second in embedding and vice versa is the case for RDWT-SVD approach.

E. Robustness of Watermarks

And the last but most important observation is about the robustness of the watermark against attacks. Here we have applied 16 attacks to check this property for in depth analysis. The proposed technique is better than other two in almost all of the attacks except two. RDWT-SVD ranks first in Gaussian variance and salt & pepper attack. It works better than the DWT-DCT-SVD watermarking. The point to be noted here is that these techniques gave comparable results for many attacks, e.g. contrast, mean filtering, rotation, etc. A robustness comparison table on the basis of tolerance level, τ is shown below:

TABLE II. OBSERVATION TABLE

Attacks/Algorithms	**RDWT-SVD**	**DWT-DCT-SVD**	**IWT-SVD**
Blurring	Very low (0.68<τ)	Very low (0.5<<τ)	High (0.92>τ)
Contrast	Variable but Low (<0.76<τ)	Variable but Low (<0.76<τ)	High (0.95>τ)
Gaussian Variance	High (0.99>τ)	Very Low (0.8>τ)	Low (0.8>τ)
JPEG Compression	High (0.86>τ)	High (0.8>τ)	High (0.93>τ)
Luminance	Low (<<<τ)	Very Low (<<<τ)	High (0.85>τ)
Mean Filtering	Low (<<τ)	Low (<<τ)	High (0.85>τ)
Median Filtering	Low (<τ)	Low (<τ)	High (0.8>τ)
Rotation	Very Low (0.65<τ)	Very Low (<<<τ)	High (0.88>τ)
Salt & Pepper	Very High (0.8>τ)	High (0.82>τ)	Variable (<τ>)
Scaling	Low (0.8>τ)	Low (0.76<τ)	High (0.85>τ)
Speckle Noise	Low (<τ)	Very Low (0.65<τ)	High (0.78≤τ)
Brightness	Low (0.7<τ)	Very Low (0.67<τ)	High (0.9>τ)
Cropping	Low (0.72<τ)	Low (0.71<τ)	High (0.9>τ)
Affine Transformation	Very Low (0.40<<τ)	Very Low (0.39<<τ)	High (0.9>τ)
Histogram equalization	Low (0.72<τ)	Low (0.62<τ)	High (0.9>τ)
Sharpening	Low (0.82>τ)	Very Low (0.69<τ)	Low (0.8>τ)

VIII. CONCLUSION

We have studied three hybrid watermarking techniques on the basis of their perceptuality and robustness against attacks. These techniques can be used for copyright protection, authentication applications etc. Here the basic approach we have used is the SVD due to its inherent advantages. Different Wavelet Transform based watermarking algorithms i.e. DWT, RDWT, and IWT are then compared. It is observed that IWT-SVD based watermarking is a robust technique than the rest two, due to its lossless property. RDWT-SVD based technique is more robust against noise attacks. But still they are not secure; so in the next paper we will add some security mechanisms to make the algorithm more secure, reliable and efficient source for embedding information.

ACKNOWLEDGMENT

First of all I would like to thank almighty GOD for giving me strength to complete this work. Second, I would like to thank my family for supporting me and encouraging me to do work day and night, and is paramount in accomplishing the paper. Last but not the least, I would be thankful to all those who helped me directly or indirectly.

References

[1] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, Digital watermarking, vol. 53. Springer, 2002.

[2] K. A. Navas, M. C. Ajay, M. Lekshmi, T. S. Archana, and M. Sasikumar, “DWT-DCT-SVD based watermarking,” in Communication Systems Software and Middleware and Workshops. COMSWARE 2008. 3rd International Conference on, 2008, pp. 271–274.

[3] S. Lagzian, M. Soryani, and M. Fathy, “A new robust watermarking scheme based on RDWT-SVD,” International Journal of Intelligent Information Processing, vol. 2, no. 1, 2011.

[4] J. Panda, J. Bisht, R. Kapoor, and A. Bhattacharyya, “Digital image watermarking in integer wavelet domain using hybrid technique,” in Advances in Computer Engineering (ACE), 2010 International Conference on, 2010, pp. 163–167.

[5] S. Lingamgunta, V. K. Vakulabaranam, and S. Thotakura, “Reversible watermarking for image authentication using IWT.,” International Journal of Signal Processing, Image Processing & Pattern Recognition, vol. 6, no. 1, 2013, pp. 145-156.

[6] I. J. Cox, J. J. Kilian, and T. G. Shamoon, Secure spread spectrum watermarking for multimedia data. Google Patents, 1999.

[7] I. J. Cox, M. L. Miller, and J. A. Bloom, “Watermarking applications and their properties.,” in itcc, 2000, pp. 6–10.