International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

PERFORMANCE ANALYSIS OF DIFFERENT ATTACKS ON WATER MARKING

ADITI GIRDHAR[1], Dr. GURPREET SINGH[2]
[1,2]Yamuna Institute of Engineering & Technology, Yamunanagar

Article Received:08/06/2015 | Article Revised on:19/06/2015 | Article Accepted on:24/06/2015

ABSTRACT
Digital watermarking is distinguished according to media type (image, audio, video etc), visibility (visible and invisible), robustness level (fragile, semi-fragile androbust) and the need for original data (blind, semi-blind and non-blind). The system consists of watermark embedding, attacks and watermark extraction. Experimental results of the proposed methods' performance were analyzed using Peak Signal to Noise Ratio (PSNR) calculations for watermark imperceptibility .

Index Terms— Watermarking; Attack; DWT; CWT ;SVD; PSNR

INTRODUCTION

Watermarking

Digital watermarking is the process of embedding a low energy signal into another signal. The low energy signal is known as WATERMARK. Cover Signal is the one which embeds the watermark and the private key which is used to embed and detect the watermark signal is known as the Watermark Key. Digital Watermarking is used for various applications such as ownership of copyright, tracking of source, authentication, broadcast monitoring.

A. Types of digital watermarking

Visible and Invisible Watermarking-

Visible watermarking as the name suggests is that in which contents are visible and visible information can be put by anyone in the digital signal. Example:- on the right top of the television screen, logo of the broadcaster such as star plus, colors etc. are visible to everyone. Invisible watermarking is the way of just looking not viewing. Watermarking is done in such a way that it is not visible to the user. It provides image authentication and security to the information.

Robust and Fragile Watermarking

In robust watermarking the watermarked signal is capable enough to handle the attacks. In fragile watermarking the content of the signal gets affected through attacks.

Steganographic and Non-steganographic

The presence of watermark is not known to the user in steganography watermarking. Example: Finger printing applications.

In non-steganography watermarking user is aware of the watermarking. Example: used to detect piracy.

Public and Private Watermarking

In public watermarking users are authorized to detect watermark. In private watermarking users are not authorized.

Symmetric and Asymmetric

In symmetric watermarking same keys are used to embed and detect watermarks.

In asymmetric watermarking different keys are used to embed and detect watermarks.

Attacks

An attack is an activity performed to destroy the embedded watermark or to detect the original watermark and replace or modify with another watermark. To achieve robustness against attack is one of the major characteristics of watermarking. We found that the watermark embedded by using DDWT method showed strong robustness against many image attacks, including cropping, rotation, sharp, transform and histogram equalization.

A. **Histogram Attack**

To reduce the piracy and duplicity of the digital multimedia files, digital watermarking technique is dominating over the other available techniques. There are certain methods or attacks which are used to damage the watermark. One of the major attacks is histogram equalization and reducing the number of histogram equalized levels. Firstly, DWT is applied on the original image and then DCT on the 4×4 blocks to target the particular frequencies of the image for embedding the watermark which does not have more effect after histogram equalization.

B. Resize Attack

In the case of resize attacks, we are basically changing the size of the original image. That means either increasing or decreasing the total number of pixels in the image, and then trying to recover the hidden information from the resized image.

C. Rotation Attack

Rotation attack is one of the most common geometrical attacks on digital multimedia images. First the original watermarked image is rotated by various degrees in the clock- wise direction. Then the recovered information from the attacked watermarked image performance is analyzed.

D. Sharp Attack

In order to test the performance, the watermarked image suffers some different signal attacks, which includes filer, sharp enhancing. It is a non-trivial process that involves a trade-off between efficiency, smoothness and sharpness.

E. Transform Attack

Any geometric attacks are reversed by constructing a triangle from the middle peak and it's two closest peaks on X and Y. An affine transformation is found that converts the modified triangle into it's original shape.

RESULTS

256x256

Fig.1 Original Image 1

64x64

Fig.2 Original Image 2

Histogram Attack :

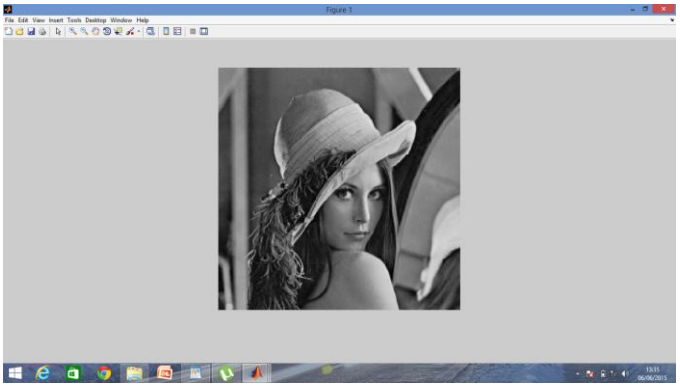

Fig. 3

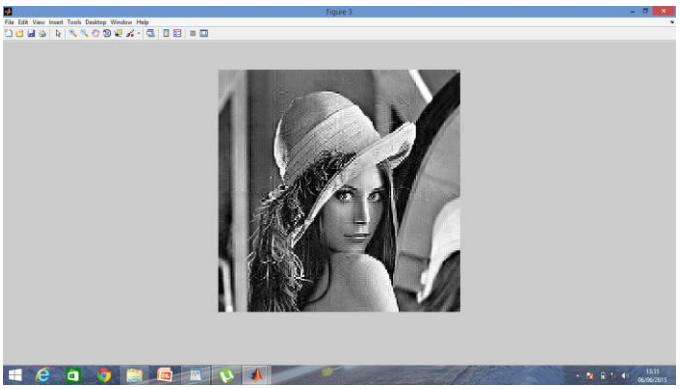

Fig.4

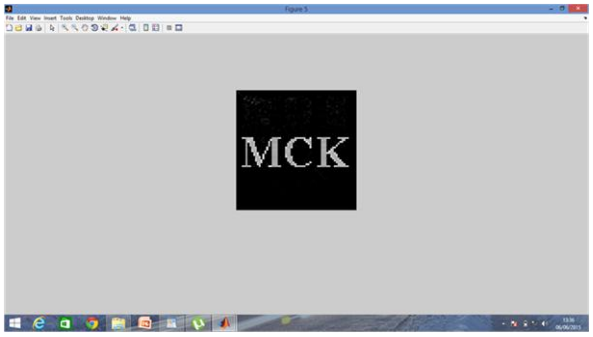

Fig. 5

Fig. 3, Fig.4, Fig.5, showing the images after Histogram attack.

Resize Attack :

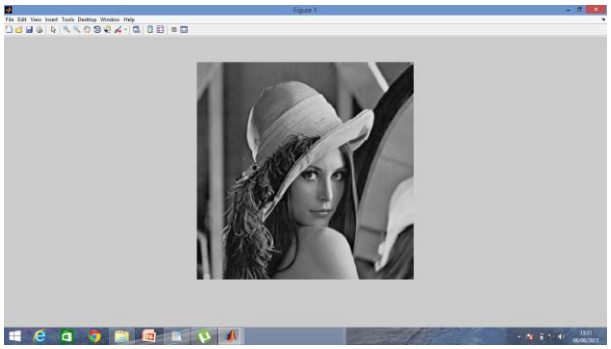

Fig.6

Fig. 7

Fig.6, Fig.7 showing the images after Resize attack.

Rotation Attack :

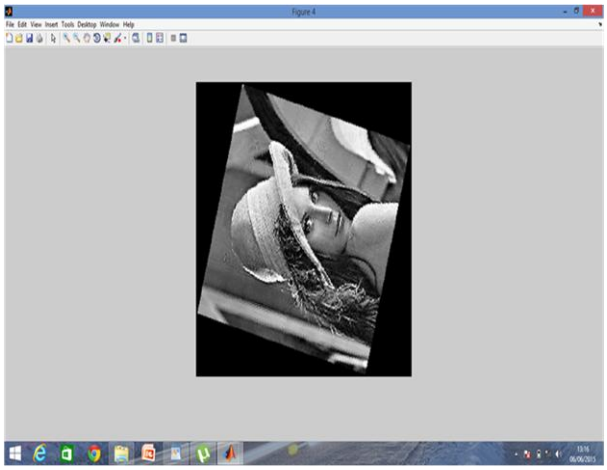

Fig. 8

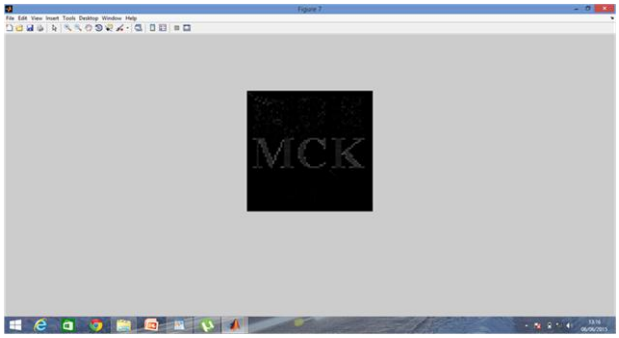

Fig.9

Fig.8,Fig.9 showing the images after Rotation attack.

Sharp Attack:-

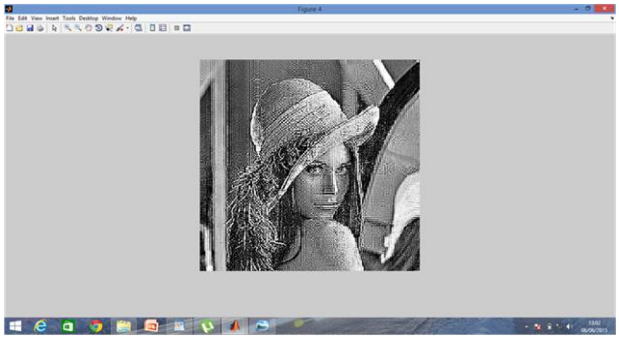

Fig.10

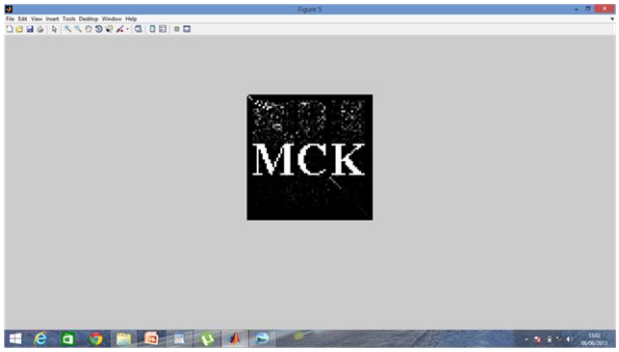

Fig. 11

Fig.10, Fig11 showing the images after Sharp attack.

Transform Attack :

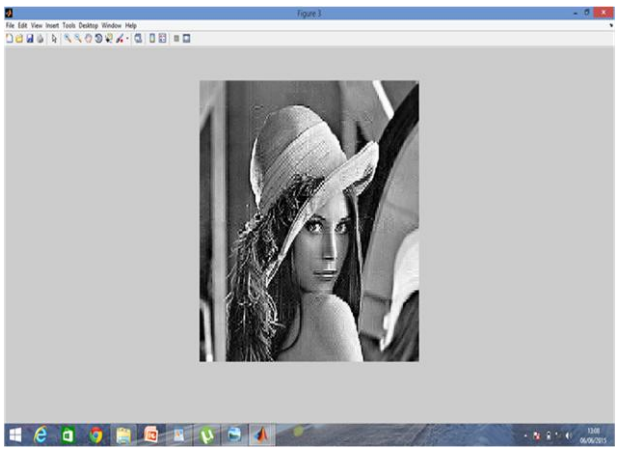

Fig. 12

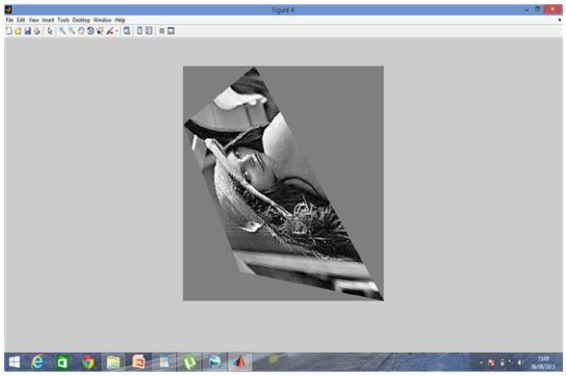

Fig. 13

Fig. 12, Fig.13, Fig.14, showing the images after transform attack.

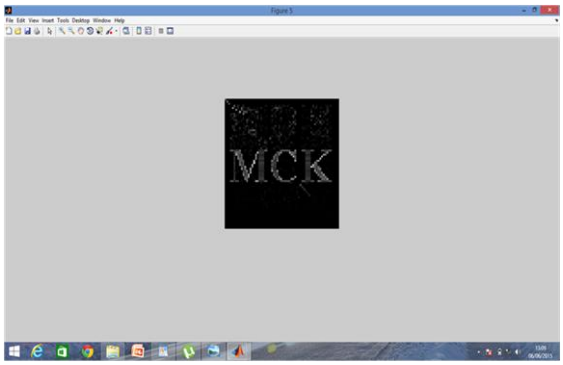

Fig. 14

PSNR Calculation

Higher values of PSNR mean that the stego-image is more similar to that of the original image. We used Peak Signal to Noise Ratios (PSNR) values to determine image quality. P**eak signal-to-noise ratio (PSNR)** is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.

$$PSNR = 10\log_{10}\frac{255^2}{MSE}$$

Where MSE represents the mean square error and is given by

$$MSE = \left(\frac{1}{mx,v}\right)\sum_{i=1}^{m}\sum_{j=1}^{N}(a_{ij}-b_{ij})^2$$

The *Mean Square Error (MSE)* and the *Peak Signal to Noise Ratio (PSNR)* are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

Image Size	Name	Image	PSNR Value
256*256	**Leena**		***18.857196***

256*256	**Barbara**		**18.002904**
256*256	**Peppers**		**18.267464**

CONCLUSION

To improve the requirements of security of watermarks, we successfully take advantage of the merits of DWT and SVD watermarking techniques. The robustness of our watermark scheme has been experimentally verified that it can resist both geometry and non geometry attacks such as cropping, rotation, sharp, waveform, histogram equalization and rescale. Experimental results show that our scheme is robust and that it can offer copyright protection for legal owners. The watermark is inserted in few of selected blocks of original image, so that perceptual quality of the watermarked image is good. Watermark is inserted into the blocks number of times so retrieval of watermark is good. PSNR value is calculated over three images Leena, Barbara, Peppers.

REFERENCES

[1]. Dinesh Kumar, Vijay Kumar, "CONTOURLET TRANSFORM BASED WATERMARKING FOR COLOUR IMAGES", The International journal of Multimedia & Its Applications (IJMA) Vol.3, No.1, February 2011.

[2]. Yusnita Yusof and Othman O. Khalifa, *Member, IEEE*, "Digital Watermarking For Digital Images Using Wavelet Transform", Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia.

[3]. Navnidhi Chaturvedi1, Dr.S.J.Basha, "Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR", International Journal of Innovative Research in Science, Engineering and Technology Vol. 1, Issue 2, December 2012

[4]. Dr. H. B. Kekre1, Dr.Tanuja Sarode2, Shachi Natu.**,"** Performance Evaluation of Watermarking Technique using Full, Column and Row DCT Wavelet Transform**"** International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 3, Issue 1, January 2014

[5]. Vijay Kumar and Dinesh Kumar ,“ Digital Image Steganography Based on Combination of DCT and DWT”

[6]. Barun Pandhwal, D.S. Chaudhari, “An Overview of Digital Watermarking Techniques”, International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-1, March 2013

[7]. Pooja Dabas, Kavita Khanna ,“ Efficient Performance of Transform Domain Digital Image Watermarking Technique over Spatial Domain”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013.

[8]. Jay Prakash Pandey, Gajendra Singh, “Digital Color Image Watermarking using DWT-SVD Techniques in YUV and RGB Color Spaces”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 1, January 2015 .

[9]. Prof. N. R. Bamane, Dr. Mrs. S. B. Patil,“ Comparison & Performance Analysis ofdifferent Digital Video Watermarking Techniques”, International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013.

[10]. Farooq Husain, Ekram Khan, Omar Farooq, “Digital Image Watermarking using Combined DWT and DFRFT”, International Journal of Computer Applications (0975 – 8887) Volume 60– No.11, December 2012 .

[11]. DINESH KUMAR, VIJAY KUMAR, “Digital Image Watermarking: A Review of SVD, DCT and DWT Based Approaches

[12]. Radhika v. Totla, K.S.Bapat,“ Comparative Analysis of Watermarking in Digital Images Using DCT& DWT ”, International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013

[13]. Qingtang Su,Yugang Niu, Xianxi Liu,TaoYao “A novel blind digital watermarking Algorithm for embedding color image into color image IEEE.

[14]. Meerwald, P. Digital image watermarking in the wavelet transform domain. Master’s thesis, University of Salzburg, 2001.

[15]. Fangjun Huang, Zhi-Hong Guan: A hybrid SVD DCT watermarking method based on LPSNR. Pattern Recognition Letters (2004)

[16]. Ramandeep Kaur1 and Harpal Singh2 “Image Watermarking In DCT, DWT and Their Hybridization Using SVD: A Survey” International Journal of Innovations in Engineering and Technology (IJIET).

[17]. Baisa L. Gunjal and Suresh N. Mali “Comparative Performance Analysis of DWT-SVD Based Color Image Watermarking Technique in YUV, RGB and YIQ Color Spaces” *International* Journal of Computer Theory and Engineering, Vol. 3, No. 6, December 2011.

[18]. Sangeeta Madhesiya, Shakil Ahmed “Advanced Technique of Digital Watermarking based on SVD-DWT-DCT and Arnold Transform” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, No 5, May 2013.

[19]. Md. Maklachur Rahman “A DWT, DCT AND SVD BASED WATERMARKING TECHNIQUE TO PROTECT THE IMAGE PIRACY” International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT) Vol. 4, No. 2, June 2013

[20]. Namita Chandrakar, Jaspal Bagga “Performance Analysis of DWT Based Digital Image Watermarking Using RGB Color Space” International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 1, January 2015

[21]. Hongxia Wang, Ke Ding, Changxing Liao (2008),“Chaotic Watermarking Scheme for Authentication of JPEG Images”, International Symposium on Biometrics and Security Technologies

[22]. Chen Li, Cheng Yang, Wei Li, “Wavelet Bases and Decomposition Series in the Digital Image Watermarking”. Advances in Intelligent and Soft Computing, Advances in Multimedia, Software Engineering and Computing Vol.2 , s.l. :Springer, 2012.