International Journal of Engineering & Technology, 7 (2) (2018) 1-5

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Effect of different attacks on image watermarking using dual tree complex wavelet transform (DTCWT) and principle component analysis (PCA)

M S Sudha [1] *, T C Thanuja [2]

[1] *Research scholar, Department of Electronics and Communication Engineering, Jain University Bengaluru*
[2] *Department of Very Large scale Integration and Embedded System, Centre for Post graduation Studies. Vesvaraya Technological University, Belgaum-590018, India*
**Corresponding author E-mail: sudhams@sapthagiri.edu.in*

Abstract

Perceptibility and robustness are two incongruous requirements demanded by digital image watermarking for digital right management and other applications. A realistic way to concurrently satisfy the two contradictory requirements is to use robust watermark algorithm. The developed algorithm uses DTCWT and PCA techniques to embed watermark signal in host signal. To prove the algorithm robustness without much affecting perceptibility several attacks like noises, cropping, blurring, rotation are applied and tested by varying attack parameters. Parameters like Peak signal noise ratio and Correlation Coefficient are calculated for each attack. Attack percentage is varied and performance parameters are calculated to prove the robustness of the developed algorithm.

Keywords: *Attack; DTCWT; Perceptibility; Robustness; PCA; Cropping.*

1. Introduction

Robustness is a measure of immunity of watermark, against attempts to image modification and manipulation. Imperceptibility is the most significant requirement in watermarking system, and it refers to the perceptual similarity between the original image before watermarking process and the watermarked image. The challenge is that imperceptibility could be achieved, but the robustness and the embedding capacity will be reduced, and vice versa, imperceptibility may be sacrificed by increasing the robustness and the embedding capacity.

Attacks are the intentional distortion introduced at transmission in order to check the robustness. These attacks types can be divided into three main categories [1].

Unauthorized removal, unauthorized embedding, and unauthorized detection. According to the specific usage of watermarking, the specific feature should be available in the watermark to resist the attacks [2]. Therefore, for unauthorized removal, the watermark should be robust and not to be removed, and for unauthorized embedding (also known as forgery), the watermark should be fragile or semi fragile to detect any modification.

In this paper, section 1 describes watermark embedding and extraction algorithm, section 2 describes embedding and extraction algorithm. Section 3 describes the application of different attacks like Gaussian Noise, Salt and Pepper Noise, Speckle noise, Poisson noise, rotation attack, compression attack, resizing and blurring, contrast attack on developed watermarking algorithm.Section 4 describes conclusion.

2. Embedding and extraction of watermarking

Image watermarking is a growing technology to protect the copy right for the digital images [3]. The Fig. 1 shows the block diagram to embed the data called watermark data or image. This embedded information [9] is insensible to human visual system. This embedded image is transmitted through the channel and reaches the receiver. During the journey the image may be corrupted by many attacks i.e. different noises, compression cropping, rotation, contrast etc.

The extraction process will extract watermark, it is expected to be similar to the original watermark image. Figure.2 shows extraction process.

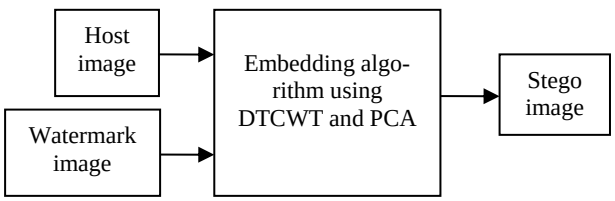

Fig. 1: Process of Embedding.

Embedding algorithm is developed in dual tree complex wavelet transform domain which is an advanced version of DWT. principle component analysis and Least Significant Bits (LSB) technique are used in the embedding process to generate the watermarked or stego image. Inverse dual tree complex wavelet transform domain is used and LSB algorithm. The extracted watermark image may not be same as original watermark and quality of host image may also be degraded. To study the robustness of the algo-

rithm intentionally some attacks are introduced before extraction example different noises like Gaussian, Poisson, speckle , compression attack, cropping, rotation, contrast etc are applied in different proportion and resisting capacity of the algorithm is checked.

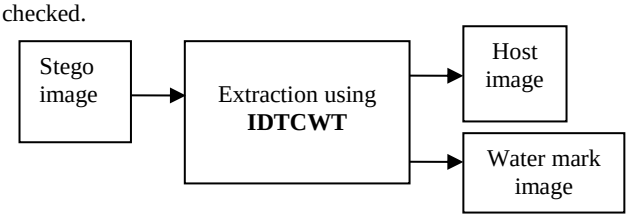

Fig. 2: Process of Extraction.

After the extraction, correlation coefficient between original watermark and extracted watermark is calculated. PSNR (in db) between host image and embedded image calculated using equation (1).

$$PSNR = 10\log_{10}(\frac{\max^2}{MSE}) \quad (1)$$

Mean square error is given by equation (2)

$$MSE = (\frac{1}{mn})\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)] \quad (2)$$

Correlation coefficient is calculated between original watermark image and extracted watermark image given by equation (3).

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\left(\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_m (B_{mn} - \bar{B})^2\right)\right)^{1/2}} \quad (3)$$

A is original watermark image and B is extracted watermark image. A_{mn} =original watermark image. Image $\bar{A}$ = mean of (A) and B_{mn} =Extracted watermark. $\bar{B}$ = Mean of (B).

3. Effect of different attacks on the watermarking

In image processing, the image is corrupted by different types of noises. Noises are of two type additive and multiplicative noise. Speckle noise [4] is multiplicative noise, so it's difficult to remove the multiplicative noise as compared to additive noise like white Gaussian noise. Filters are used to de-noise. Median filter is the best known order statistics filter in image processing. The median filter at is used at extraction to remove Gaussian, Speckle, Pepper, Poisson noise.

3.1. Effect of gaussian noise

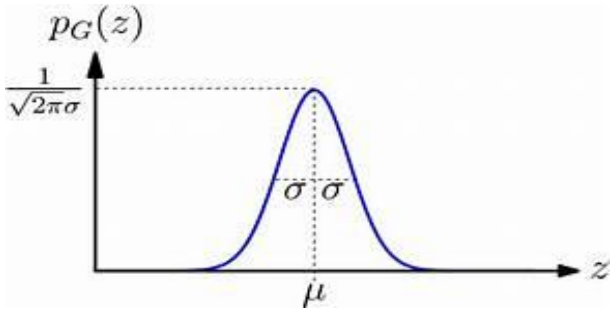

Fig. 3: PDF of Gaussian Noise.

Additive Gaussian noising is a process that adds a noise signal to an image in order to deliberately corrupt the image, hence reducing its visual quality.

Table 1: Gaussian Noise Effect

Host image Armin.jpg	Watermark image Barbara.jpg		
Mean=0 variance	PSNR	MSE	CC
0.001	52.4179531 50.2169339	0.38	0.9950
0.01	PSNR: 50.2169339 dB EC_bpp =	0.62	0.9950
0.1	51.1980888	0.50	0.9948
0.2	51.1910328	0.50	0.9948
0.3	51.3723518	0.48	0.9947
0.4	51.0203055	0.52	0.9945
0.5	52.2378784	0.39	0.9943
0.8	51.9649506	0.42	0.9944
1	48.3802590	0.95	0.9957

The statistical property of this noise follows a Gaussian Probability Density Function (PDF) as shown in Fig. 3. A Gaussian PDF, often called normal PDF, is the most commonly used probability [5] distribution function to generate random numbers since it is believed to model closely many real life randomly occurring events. In addition, the central limit theorem states that the distribution of the sample means of a sufficiently large number of samples will always approximate to the Gaussian distribution. The Gaussian PDF f(x) is of a random variable x is defined as:

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \quad (4)$$

To illustrate the effect of adding Gaussian noise to the watermarked image, different values of σ 2 (variance) are taken and the corresponding CC and PSNR are calculated. Correlation coefficient is almost constant and nearly one. PSNR varies from 52.41 to 48.38 shown in Table 1.

Fig.4: Guassian Attack.

Fig. 5: Median Filter.

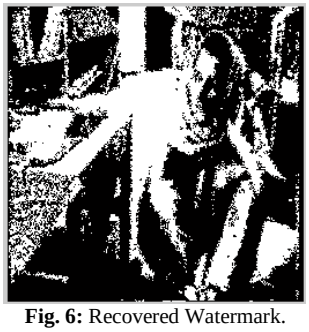

Fig. 6: Recovered Watermark.

Fig. 7: Host After Extraction.

3.2. Salt and pepper noise

Salt-and-pepper noise is also known as impulse noise. This noise can be caused by sharp and sudden disturbances in the image signal. It presents itself as sparsely occurring white and black pixels. An effective noise reduction method for this type of noise is a median filter. Probability distribution function of pepper and salt takes the form of two impulse functions at two discrete locations at location a and b as shown in Fig. 8. The Salt and Pepper PDF p(z) can be calculated using the two impulse functions .Salt and Pepper noise represents itself as randomly occurring white and black pixels if b >> a, intensity b will appear as a white pixel in the image. Conversely, intensity a will appear as a black pixel. If either P_a or P_b is non-zero and especially if they are approximately equal, impulse noise values will resemble salt-and-pepper granules randomly distributed over the image.

Table 2: Effect of Pepper Noise

Host image Armin.jpg	Watermark image Barbara.jpg		
Mean=0 variance	PSNR in db	MSE	NCC
0.01	53.5762547	0.29	0.9962
0.05	53.1642341	0.32	0.9960
0.1	52.8964976	0.34	0.9956
0.2	51.4527013	0.47	0.9943
0.3	49.8004663	0.69	0.9896
0.4	48.0017003	1.04	0.9820
0.5	44.5839130	2.28	0.9642
0.8	37.4733407	11.73	0.8734

The variance is varied from 0.01 to 0.8 and the mean is kept zero, the corresponding CC and PSNR are calculated. Algorithm is resistant to 0.8 variance of pepper noise.

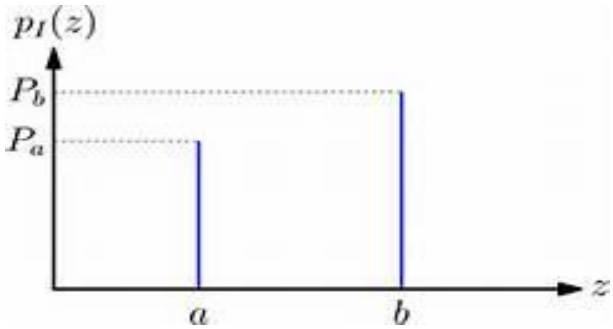

Fig. 8: PDF of Pepper and Salt.

3.3. Speckle noise

Speckle noise in these images affects edges [2] and fine details which limit the contrast resolution. Speckle noise is multiplicative noise and it is difficult to remove .Median filter, Lee filter, wavelet filter etc are used to remove it. Median filter is used in this case. Table 4 shows effect of speckle noise on PSNR and CC.

Table 3: Speckle Noise Effect

Host image Armin.jpg	Watermark image Barbara.jpg		
Mean=0 variance	PSNR in db	MSE	NCC
0.01	50.69	0.29	0.9957
0.02	53.1642341	0.32	0.9947
0.03	52.8964976	0.34	0.9937
0.04	51.4527013	0.47	0.9926
0.05	49.8004663	0.69	0.9919
0.06	48.0017003	1.04	0.9900

3.4. Poisson noise

Poisson noise is one type of multiplicative noise. This type of noise occurs in almost all coherent imaging system [5] such as laser, acoustics and SAR (Synthetic Aperture Radar). Poisson distribution has the property that its variance is equal to its expectation, and that its standard deviation grows with the square root of the signal. In practice, Poisson noise is often modelled using a Gaussian distribution whose variance depends on the expected Poisson count. For small Poisson counts, Poisson noise is generally dominated by other signal-independent sources of noise, and for larger counts, the central limit theorem ensures that the Poisson distribution approaches a Gaussian. Poisson noise is generated from the data instead of adding artificial noise to the data. Fig. 9 shows Poisson attack on stego image. Fig. 10 shows extracted host after Poisson attack and Fig. 11 shows recovered watermark. It is found that PSNR is found to be 51.9427 dB, MSE is 0.42 and correlation coefficient is 0.9966.

Fig. 9: Poisson Attack.

Fig. 10: Extracted Host.

Fig. 11: Recovered Watermark.

3.5. Rotation attack

Rotation attack is among the most popular kinds of geometrical attack on digital multimedia images. Different levels of rotations have been implemented. Stego image is rotated by 1º, 15º, till 120º. If stego image is rotated clockwise, [6] the same level of rotation in anticlockwise direction is implemented [8] at extraction. PSNR, MSE and CC are calculated for each rotation.

Table 4: Effect of Rotating the Image

Host image Armin.jpg	Watermark image Barbara.jpg		
Rotation in degree	PSNR in dB	MSE	CC
1 MSE: 3.25 PSNR: 43.0393948	43.039	3.25	0.5560
15	41.1558184		0.2114
100	41.0393332	5.16	0.2387
120	41.1620971	5.01	0.1641

3.6. Compression attack

Compression attack is generally an unintentional attack occurs in almost all multimedia application [7]. Practically all images currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark embedding in the same domain where the compression takes place. For instance, the Discrete Cosine Transform (DCT) domain image watermarking is more robust to Joint Photograph Expert Group (JPEG) compression than the spatial-domain watermarking. Similarly Discrete Wavelet Domain (DWT) domain watermarking is robust to JPEG 2000 compression [8]. The enhanced DWT is DTCWT which is much more efficient in image compression. It saves more space compared to DWT. This is shown in Table 5.

Table 5: Compression effect

Host image	Q factor	PSNR	CR in bits	CR in BPP	Space saved
Armin MSE: 3.25 PSNR: 43.0393948	40 80	53.0919228 53.3791	3.5556	0.444	71.89
desert	40 80	59.6829439 59.3366426	4	0.5	75
lenna	40 80	31.1713974 31.1901356	4	0.5	75
book	40	31.2710893	3.5556	0.444	71.89

3.7. Cropping and intensity transformation

Cropping is removing the parts of an image to improve framing, accentuate subject matter or change aspect ratio. Depending on the application, this may be performed on a physical photograph, artwork or film footage, or achieved digitally using image [9] editing software. This can also be used as an intentional attack to manipulate. The Matlab Image cropping tool is used to crop the image. One can position interactively using the mouse. Image intensity values are adjusted at watermark extractor to map the[10] values in intensity image to new values in the output image such that 1% of data is saturated at low and high intensities of the image.

This increases the contrast of the output image. An image of 512x512 is taken rectangle cropping is carried out for 5% to 50%. Watermark extraction is possible till 50%. Table4 shows PSNR and CC for the [11] corresponding cropping.

Table 6: Cropping Effect

Host image Armin.jpg	Watermark image Barbara.jpg		
% of crop	PSNR in dB	MSE	NCC
5 MSE: 3.25 PSNR: 43.0393948	49.46	0.74	0.9978
15	49.5	0.746	0.9978
30	49.56	0.748	0.9978
50	49.66	0.7499	0.9978

3.8. Resizing and blurring attack

Resizing is performed before blur operations .The output image is scale times the size of input image [11]. The input image can be a grayscale, RGB, or binary image. If scale is between 0 and 1.0, output image is smaller than input image. If scale is greater than 1.0, output image is larger than input image. Blurring is performed with help of filter. In Matlab tool the filter command is h= fspecial ('disk', radius) returns a circular averaging filter (pillbox) within the square matrix of size 2*radius+1.

Blurred = imfilter (I, H,'replicate'); imfilter is N-dimensional filtering of array I multidimension filter (H). Replicate key word replicates boundaries of the blurred image. Image radius is increased to vary blurring in the image, the corresponding PSNR, CC is calculated. The result a show PSNR varies from 49 to 53db.CC is below 0.1, this proves recovered watermark is not same as original watermark. This scheme is not very much resistant to blur attack.

Fig. 12: Stego Image.

Fig. 13: Blurred Stego.

Fig. 14: Recovered Image.

3.9. Contrast attack

Histogram equalization is performed to enhance the contrast of the stego image by transforming the values in an intensity image [12], or the values in the colormap of an indexed image, so that the histogram of the output image approximately matches a specified histogram.

Fig. 15: Stego Image.

Fig. 16: Contrast Image.

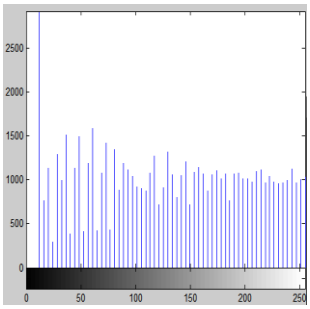

Fig. 17: Histogram of the Image.

Fig. 18: Extracted Host.

4. Conclusion

The developed algorithm based on DTCWT and PCA, whose robustness is checked by introducing distortion or attacks on it. A robust watermarking algorithm technique is one which is resistant to any kind of attack .This paper covers noise attacks, Rotation attack, Compression attack, Cropping attack, Contrast attack on the watermarking algorithm. The algorithm prove to be robust against all attacks except rotation attack, a further extension of the work is required to prove robustness against rotation attack.

Acknowledgement

I would like to thank Sapthagiri College of engineering for their kind support throughout the research work and also thanks to my family, friends and colleagues, for their continuous motivation and support.

References

[1] Mitesh Patel, Swati, Alpesh"The study of various attacks on Digital watermarking technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 5, May 2014.

[2] Prabhishek Singh, Aayush Agarwal, Jyoti Gupta Singh "Image Watermark Attacks: classification and Implementation" International Journal Electronics and communication Technology. Vol.4 Issue 2 April2013 ISSN: 2230-7109.

[3] M.S. Sudha, T.C. Thanuja "A Robust Image Watermarking Technique using DTCWT and PCA" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8252-8256 © Research India Publications.

[4] Amandeep Kaur, Karamjeet Singh "speckle noise reduction by using wavelets" NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.

[5] Ayushi Jaiswal, J.P. Upadhyay, Ravi Mohan S., P. Bohre "A Novel Approach for Reduction of Poisson Noise in Digital Images". Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.1275-1279.

[6] Ruanaidh J. J. K. O., Pun T., (1998), "Rotation, scale and translation invariant spread spectrum digital image watermarking," Signal Process, Vol. 66, No. 3, pp. 303-317. https://doi.org/10.1016/S0165-1684(98)00012-7.

[7] Ahmed Hassan Hadi " Robust Image Watermarking Against Different Attacks: Noising, (Jpeg) Compression, And Filtering"Journal of Babylon University/Pure and Applied Sciences/ No.(6)/ Vol.(21): 2013

[8] Sanyam Agarwal, Priyanka, Usha Pal "Different types of Attack in Image Watermarking including 2D,3D Images" International Journal of science and engineering research, Volume 6, Issue 1,January -2015.

[9] Tefas A., Nikolaidis N, and Pitas I., (2009), "Chapter 22 – Image Watermarking Techniques and Applications," in The Essential Guide to Image Processing (Second Edition), B. Al, Ed., ed Boston: Academic Press, pp. 597-648.

[10] Md. Asikuzzaman, Md.Jahangir Alam,Mark pickering "A Blind and robust video watermarking Scheme in the DTCWT and SVD Domain" IEEE International Conference on Digital lmage Computing: Techniques and Applications Pages1-6 2014/11/25.

[11] Baisa L Gunjal , Dr. Suresh N Mali "Handling Various Attacks in Image Watermarking" CSI communications, 2013 - csi-india.org

[12] Deepak Aggarwal, .Sandeep Kaur, Anantdeep "An Efficient Watermarking Algorithm to Improve Payload and Robustness without Affecting Image Perceptual Quality" Journal of computing, volume 2, Issue 4, April 2010, ISSN 2151-9617.