ISSN (Online): 2230-7893
www.IJCEM.org

A Novel Approach for Watermarking using Dual Watermarking Technique in Noisy Regions

Rakhee Lakhera[1], Alka Gulati[2], Shital Gupta[3]

[1] Research Scholar, LNCT Bhopal, India.
rakhee.lakhera@gmail.com

[2] Associate Prof. of CSE, LNCT Bhopal, India.
gulati.alka@gmail.com

[3] Assist. Prof. of CSE, LNCT, Bhopal, (M.P.) India
shitalbehare@yahoo.co.in

Abstract

Digital Watermarking is one of the most prominent technique used for protection of ownership rights of digital media which is text, audio, video or image. For providing more security to the information and to enhance the hiding capacity of an image and avoid abrupt changes in image edge areas, as well as to achieve better quality of the stego-image, a novel image data hiding technique by Wavelet Watermarking and frequency domain is proposed in this paper. The paper focuses on Image Adaptive watermarking methods in the Discrete Wavelet Transform Domain and frequency domain since they yield better results regarding robustness and transparency than other watermarking schemes. In this paper the technique is proposed to hide text data into noisy region of a digital image. The Discrete Wavelet Transform Domain and frequency domain dual adaptive watermarking algorithm which will be used for the novel application for watermarking. It helps, for providing more security to the information and result show our algorithm is best for data hiding in image.

Keywords- Wavelet Watermarking, frequency domain, PSNR, Image steganography, Image encrypton.

- INTRODUCTION

Popularity of the Internet and the rapid growth of multimedia technology, users have more and more chances to use multimedia data. Consequently, the protection of the intellectual property rights of digital media has become an urgent issue. Digital watermarking has attracted considerable attention and has numerous applications, including copyright protection, authentication, secret communication, and measurement.

There are several techniques for embedding a watermark into a digital image. In general, watermarking techniques for images are classified into two main categories namely the spatial domain approach and the frequency domain approach [3].

The spatial domain approach entails spatial watermarks which are created in the image spatial domain and are embedded directly into an image's pixel data. Frequency domain or spread spectrum techniques involve spectral or transform based watermarks which are embedded into an image's transform coefficients using the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) and the Fast Fourier Transform (FFT). These methods work by using the transforms to analyse the data and thus manipulate the coefficients produced by the transforms in order to embed the information into an image [7]. Other transform domain techniques include the Mellin-Fourier transform, Fractal Transform, etc

Blind watermarking methods perform verification of the watermark without the use of the original image. Most other techniques need the original image in order to detect the watermark and are usually more robust. Image-adaptive watermarking techniques are usually transform-based and are very robust. Image adaptive techniques were mainly developed for image compression. Steganographic and non-steganographic watermarking techniques where steganographic watermarking techniques ensures that the users are unaware that a watermark is present and in non-steganographic watermarking.

This becomes particularly important as the technological disparity between individuals and organizations grows. Governments and businesses typically have access to more powerful systems and better encryption algorithms then individuals. Hence, the chance of individual's messages being broken increases which each passing year. Reducing the number of messages intercepted by the organizations as suspect will certainly help to improve privacy.

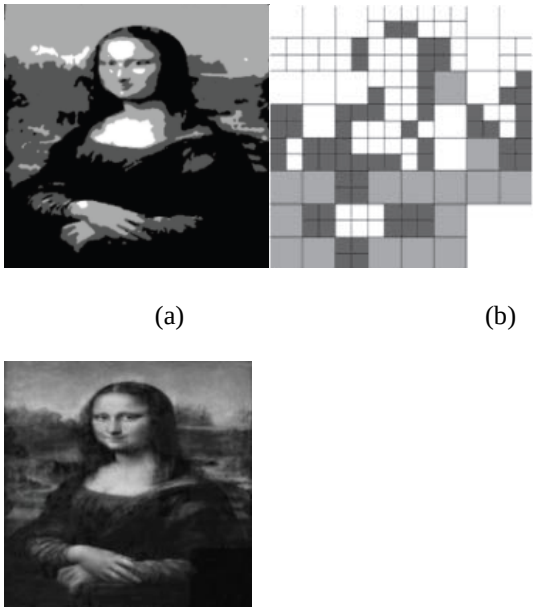
Watermarking technology has received enormous level of attention of researchers and practitioners alike.

Unfortunately, due to the same reason, watermarking technology has also attracted the attentions of hackers and criminals alike who are interested in breaking the watermarks in order to crack the copyright protection system. As a result, there is a constant challenge on the researchers to keep improving the robustness of the watermarking technique while at the same time maintaining its transparency as to not intruding any legitimate use of the media. Progress in this area has been steady as can be seen from a healthy number of publications in the field and the sheer number of institutes around the world that deal with the issue [1]. In the more specific field of digital image watermarking, one of the most notable techniques is region-based image watermarking [2]. The paper described a method for embedding and detecting chaotic watermarks in large images. An adaptive clustering technique is employed in order to derive a robust region representation of the original image. The robust regions are approximated by ellipsoids, whose bounding rectangles are chosen as the embedding area for the watermark. The drawback of this technique is due to limited number of suitable regions for storing the watermark the watermark storing capacity can be low.

In this paper, we present a novel watermarking technique which works by adaptively embedding the watermark data into different region of the host image. The rationale of our approach is based on the research finding we came into in our previous study [3][4]. This finding will be described in detailed in this paper for convenience. Most first generation digital watermarking algorithm embedded the watermarking into the time domain samples or transform domain to transform coefficients, but this leads to a poor robustness of time domain algorithms to the signal processing like compression, noise and filtering, transform domain watermarking uses the idea of audio masking effect and spreads spectrum technology to improve the robustness, simultaneous reduces the performance of anti-synchronization attack. The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) [8].

- RELATED WORK

In this Research paper [5] here they advancement of digital image watermarking technology have reviewed an analysis of on a number of attack types on image watermarking. The analysis was carried out using two image analysis tools namely Image Histogram and Fourier Spectrum for frequency domain analysis. Using the results of the experiments, they argue that existing techniques have different sensitivity and robustness levels to different attacks. The results also uncover a number of common similarities between different types of watermark attack.



(a) (b)

(c)

Figure 1. (a) MRF segment tied host image, (b) watermark insertion region and (c) watermarked image

They have presented a novel digital image watermarking technique that takes into account the results of previous analysis and testing of the hypothesis. There technique utilizes a number of technologies namely dual watermarking, image segmentation and partitioning, and DWT-SVD to fulfill the design criteria set to prove the hypothesis. The experiment results show that the technique is more robust to attacks than the original DWT-SVD technique. In addition to the improving the robustness of the watermark to attacks, they can also show a novel use the region-adaptive watermarking technique as a means to detect if certain type of attacks have occurred. This is a unique feature of watermarking algorithm which separates it from other state-of-the-art watermarking techniques. The watermark detection process uses coefficients derived from the Region-Adaptive Watermarking algorithm in a linear classifier. The experiment conducted to validate this feature shows that in average 94.5% of all watermark attacks can be correctly detected and identified.

ISSN (Online): 2230-7893
www.IJCEM.org

- PROPOSED TECHNIQUE

- *Frequency Domain*

In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain. Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather than in smoother regions. The benefit is two-fold; Degradation in smoother regions of an image is more noticeable to the HVS, and becomes a prime target for lossy compression schemes.
Taking these aspects into consideration, working in a frequency domain of some sort becomes very attractive. The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) [8].

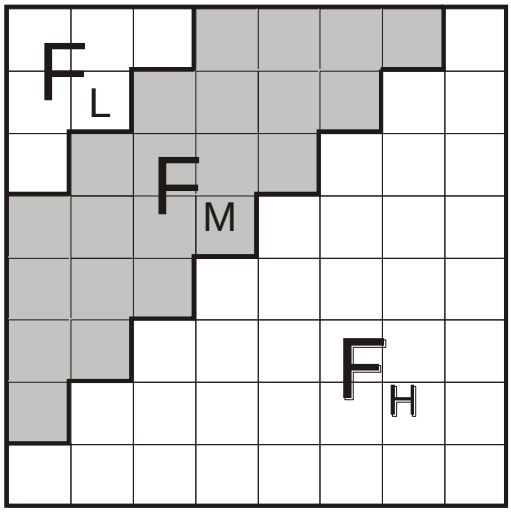


Figure 2 - Definition of DCT Regions
One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (FM) of an 8x8 DCT block as shown below in figure 2. FL is used to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [7].

The swapping of such coefficients should not alter the watermarked image significantly, as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermark can be improved by introducing a watermark "strength" constant k, such that Bi(u1,v1) - Bi(u2,v2) > k. Coefficients that do not meet this criteria are modified though the use of random noise as to then satisfy the relation. Increasing k thus reduces the chance of detection errors at the expense of additional image degradation [6].

Another possible technique is to embed a PSN sequence W into the middle frequencies of the DCT block. We can modulate a given DCT block x,y using the equation shown below in figure 7.

$$I_{W\,x,y}(u,v) = \begin{cases} I_{x,y}(u,v) + k * W_{x,y}(u,v), & u,v \in F_M \\ Ix,y(u,v), & u,v \notin F_M \end{cases}$$

Equ 1 - Embedding of image watermark into DCT middle frequencies [8]

For each 8x8 block x,y of the image, the DCT for the block is first calculated. In that block, the middle frequency components FM are added to the pn sequence W, multiplied by a gain factor k. Coefficients in the low and middle frequencies are copied over to the transformed image unaffected. Each block is then inverse-transformed to give us our final watermarked image IW [8].

The watermarking procedure can be made somewhat more adaptive by slightly altering the embedding process to the method shown below in figure 8.

$$I_{W\,x,y}(u,v) = \begin{cases} I_{x,y}(u,v) * (1 + k * W_{x,y}(u,v)), & u,v \in F_M \\ Ix,y(u,v), & u,v \notin F_M \end{cases}$$

Equ 2 - Image dependant DCT image watermark [8]

This slight modification scales the strength of the watermarking based on the size of the particular coefficients being used. Larger k's can thus be used for coefficients of higher magnitude…in effect strengthening the watermark in regions that can afford it; weakening it in those that cannot [8].

For detection, the image is broken up into those same 8x8 blocks, and a DCT performed. The same PSN sequence is then compared to the middle frequency values of the transformed block. If the correlation between the

sequences exceeds some threshold T, a "1" is detected for that block; otherwise a "0" is detected. Again k denotes the strength of the watermarking, where increasing k increases the robustness of the watermark at the expense of quality [8].

- *Wavelet Watermarking*

The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below in figure 3.

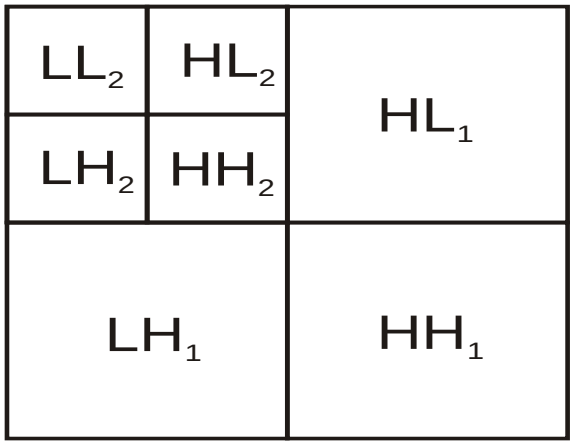


Figure 3 - 2 Scale 2-Dimensional Discrete Wavelet Transform

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [8].

One of the most straightforward techniques is to use a similar embedding technique to that used in the DCT, the embedding of a data in the detail bands according to the equation shown below in Equ 3.

$$I_{W\,u,v} = \begin{cases} W_i + \alpha |W_i| x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases}$$

Equ 3 - Embedding of a image Watermark In the Wavelet Domain

Where, Wi denotes the coefficient of the transformed image, xi the bit of the watermark to be embedded, and a scaling factor. To detect the watermark we generate the same pseudo-random sequence used in data generation and determine its correlation with the two transformed detail bands. If the correlation exceeds some threshold T, the watermark is detected.

This can be easily extended to multiple bit messages by embedding multiple watermarks into the image. As in the spatial version, a separate seed is used for each PN sequence, which is then added to the detail coefficients as per Equ 3. During detection, if the correlation exceeds T for a particular sequence a "1" is recovered; otherwise a zero. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered.

Furthermore, as the embedding uses the values of the transformed value in embedded, the embedding process should be rather adaptive; storing the majority of the watermark in the larger coefficients.

PSNR

In order to better compare this new technique with the existing algorithm based on 8 bits binary information, the hiding capacity of an image along with the PSNR value (Peak Signal to Noise Ratio). The PSNR value gives the measurement of the distortion of carrier image after hiding information. The signal in this case is the original data, and the noise is the error introduced by compression.

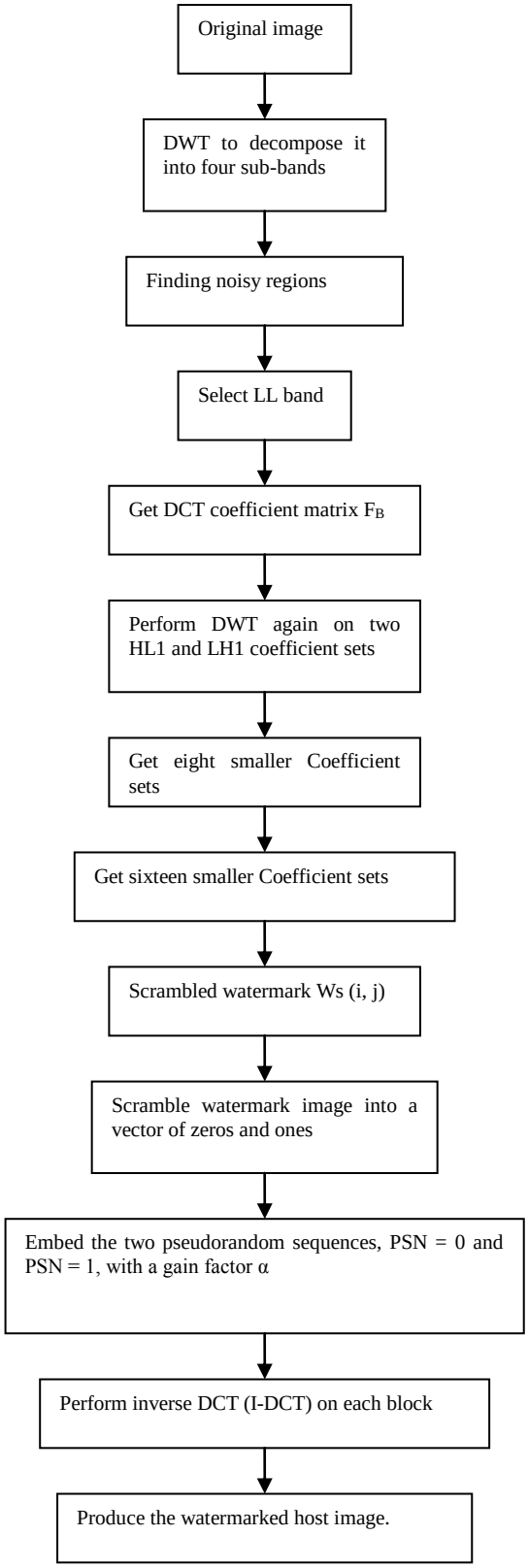
The PSNR is defined as:

$$PSNR = 10\log_{10}\frac{(MAX^2 I)}{(MSE)}$$

Here, MAXI is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using B bits per sample, MAXI is $2B-1$.And MSE stands for Mean Square Error. For two m×n monochrome images I and K where one of the images is considered a noisy approximation of the other.

The higher the PSNR, the better the quality of the compressed or reconstructed image. When the two images are identical, the MSE will be zero. For this value the PSNR is undefined i.e. ∞.

Flowchart for Embedding Algorithm:



Extracting Algorithm:

Step 1: Take Watermarked host image.
Step 2: Perform inverse DCT (I-DCT) on each Block.
Step 3: Embed the two pseudorandom sequences,
PSN = 0 and PSN = 1, with a gain factor α.
Step 4: Gain the Scrambled Watermark Ws (i, j).
Step 5: Extraction of data from watermarked Image.
Step 6: Get Watermarked Data in text file.
Step 7: Get Original image.

- PROPOSED ALGORITHM

In Figure 4 shows the proposed watermark technique. The embedding process of the proposed technique will be illustrated by the block diagram shown in Figure 4.

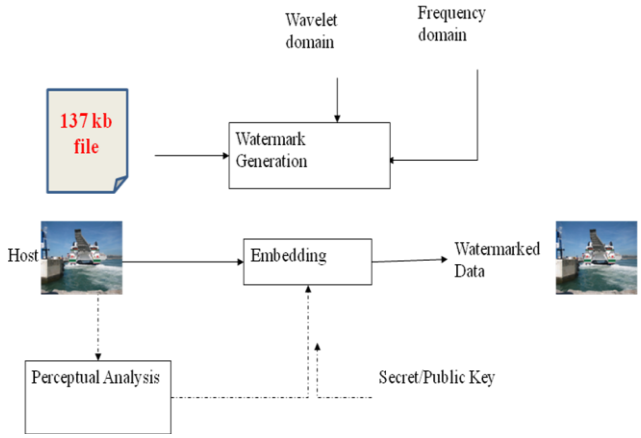
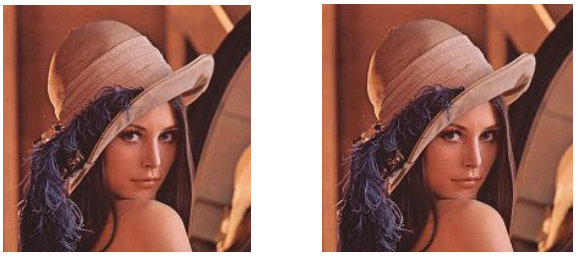


Fig 4 Block diagram of propose Algorithm

- TEST RESULTS AND ANALYSIS

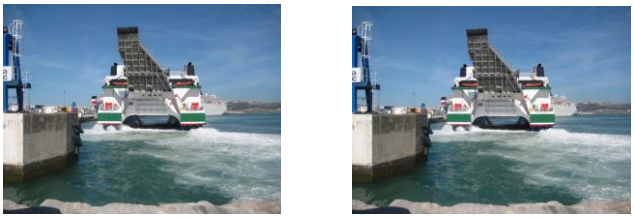
First, robustness evaluations were limited to testing against JPEG compression and the addition of random noise. Evaluating algorithms against all attacks across a full range of gain values is well beyond the scope of this paper. The other robustness metrics described in table 1 will only be touched on briefly, should the algorithm prove exceptionally resistant or exceptionally vulnerable to the attack.



a b

Fig 5 (a) Lena as an original Image, (b) Lena after watermarked image.

ISSN (Online): 2230-7893
www.IJCEM.org



a b

Fig 6 (a) Boat as an original Image, (b) Boat after watermarked image.

a b

Fig 7 (a) flower as an original Image, (b) Flower after watermarked image

Figure 5,6,7.(a) is an original watermark which used in original image and Figure 5,6,7.(b) is a extracted watermark which is extracted from the watermarking image at the receiving side.

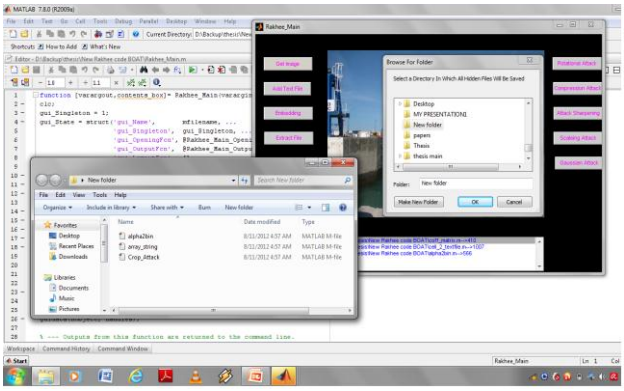


Fig 8 Screen snapshot

We have tried to test this reversible data hiding algorithm based on DWT hiding in noisy area and the result shows that it can hide more data than the existing data hiding algorithm. And finally compare this result with the different images. Experimental results show the hiding capacity depends on the original image and has little relation to data message file. Fig 8. Shows an original image (24 bit bmp file), into which, 3 data files are going to be hidden. These files are extracted and saved into a specified folder.

The PSNR of each watermarked image will be given of each picture however these pictures are only to be taken lightly. PSNR does not take aspects of the HVS into effect so images with higher PSNR's may not necessarily look better than those with a low PSNR. This will prove particularly true in the case of the DCT and DWT domain techniques.

S. No	Image Type	PSNR Value	NC Value
1	Flower	59.71	1
2	Boat	56.64	1
3	Lena	56.14	1

Table 1 Show Different PSNR and NC Value for all three Images after embedding before attack

Here above in table 1 show different PSNR and NC values of all the three images, in which flower image has the best Results.

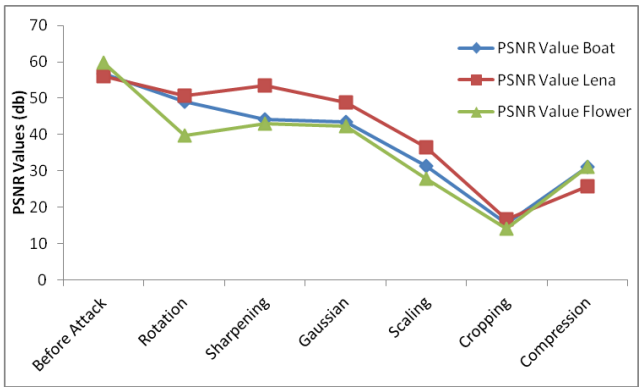


Fig. 9 Comparing PSNR values of three images before and after attack

Fig. 9 shows different values of PSNR for all three images that we have gained before attack and after applying different attacks on all the three images.

Performance requirements are similarly only to be used as a rough guideline. In general, algorithms were implemented in the most straightforward way, not the most computationally optimal. Furthermore, MATLAB may handle certain programming constructs differently from other languages, thus the best performing algorithm may vary for each language and implementation.

To detect the watermarked attacked we test the robustness of the proposed watermarking scheme, seven watermark removal attacks are applied to the watermarked image. They are Gaussian noise, salt and pepper noise, sharpen, smoothing, median filter, histogram equalization and JPEG compression attack. The severity of these attacks can be adjusted by modifying their corresponding parameter

values. Definitions of these parameters can be found is given in [9].

Attack	PSNR Value			NC Value		
	Boat	Lena	Flower	Boat	Lena	Flower
Before Attack	56.64	56.14	59.71	1	1	1
Rotation	49.14	50.69	39.72	0.99	0.54	0.7
Sharpening	44.2	53.55	43.05	0.95	0.6	0.83
Gaussian	43.44	48.74	42.38	0.87	0.38	0.77
Scaling	31.3	36.4	27.95	0.21	0.09	0.14
Cropping	15.46	16.7	14.18	0.13	0.15	0.11
Compression	31.17	25.78	31.13	0.51	0.41	0.51

Table 2 Show comparing Results of PSNR and NC Value for all three images after Attack

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.

Image sharpening can be achieved in the frequency domain by using a high pass filter, which attenuates the low-frequency components without disturbing high-frequency information in the Fourier transform. A high pass filter $H(\omega)$ is obtained from its low pass filter $L(\omega)$ counterpart using $H(\omega) = 1 - L(\omega)$ in the frequency domain

In rotational attack we tilde the image in 180 degree and PSNR value obtained not good and also NC value are not good which indicate this attack is not supportable.

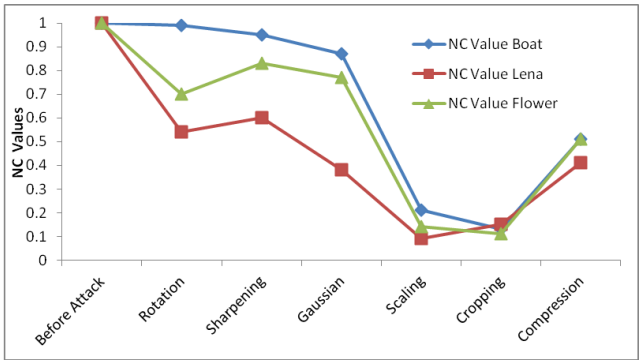


Fig. 10 Comparing NC values of three images before and after attack

The graph above shows the simulation result of different attacks on watermarked image. Here values of PSNR have been calculated for all the 3 images. After having a look on this table 2 and we can understand that the quality of all 3 images has less effected by Sharpenning, guassian, and scaling. And more degraded after the compression and cropping attack. Here rotation angle is $180^{0,}$ sharpening measure is 50%, scaling measure 50%.

Different watermark attacks have different coefficient to detect. Fig. 10 above shows NC values before attack and Further change in these values after applying different attacks on all the three images. Some of the attacks only require one coefficient which include Gaussian noise and salt and pepper noise, moreover, the rest of them need 2 factors.

S. No	Attacks
1	Sharpening
2	Gaussian
3	Scaling
4	Rotation
5	Cropping
6	Compression

Table 3 Show Different Attacks

CONCLUSION

The wavelet domain and frequency domain both will be proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation. Here we have taken 3 different images of different-2 sizes and watermark embedding is applied to all these images. Embedded file size is same for all three images so that we can compare different results between all these three images. We have tried to test this data hiding algorithm based on DWT hiding in noisy area and the result shows that it can hide more data and the quality of watermark image under attack in the proposed algorithm is better. The experimental results shows that Flower the biggest image among all three images that we have taken has the best result in comparison of other two image because PSNR and NC value of image is depend in size and qualities of image and also this image provides more noisy space for data to be hidden.

The experimental results will performed and analyze of different images file is implemented in matlab tool. Blind steganalyzers generally extract some exquisite features to measure the embedding noise. However, our algorithm modifies the pixels in noisy regions and leaves the pixels in smooth regions unchanged. It is obvious that the subtle noise brought by our algorithm could be well concealed by the noisy environment. Extensive experimental results

verified that it is more secure to embed secret message in noisy regions than in smooth regions of image. The counters proposed to these attacks typically rely on discovering the exact rotation, or shifting used in the attack, and then transforming the image back into its pre-attack state. Typically these techniques are computationally pricey, and unpredictable. This remains one of the major problems in the development of robust digital watermarking for digital images.

REFERENCE

[1] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., Information Hiding—A survey, Proceeding of the IEEE, Special Issue on Protection of Multimedia Content, 1062-1078, July 1999.

[2] A. Nikolaidis and I. Pitas, "Region-based image watermarking," Image Processing, IEEE Transactions on, vol. 10, no. 11, pp. 1726-1740, 2001.

[3] Cl.Song, S.Sudirman and M.Merabti, ―A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks‖, Proc 11th of PostGraduate Network Symposium, 119-124, June, 2010.

[4] C.Song, S. Sudirman, M.Merabti and D.L.Jones, ―Analysis of Digital Image Watermark Attacks‖, 6th IEEE International Workshop on Digital Rights Management, 2010.

[5] S. Sudirman, M. Merabti, D. Aljumeily, "Region-Adaptive Watermarking System and Its Application", Developments in E-systems Engineering, PP-215-220, IEEE 2011

[6] N.F. Johnson, S.C. Katezenbeisser, "A Survey of Steganographic Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75

[7] J.R. Hernandez, M.Amado, and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure", in IEEE Trans. Image Processing, vol. 9, pp 55-68, Jan. 2000

[8] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol 17, pp 20-43, September 2000

[9] Cl.Song, S.Sudirman and M.Merabti, ―A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks‖, Proc 11th of PostGraduate Network Symposium, 119-124, June, 2010.

[10] Rakhee Lakhera, Shital Behare, Alka Gulati, - A Novel Approach for Watermarking using Dual Watermarking Technique‖, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.