International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Optimizing the Effect of Cropping and Rotation Attacks on Watermarked Images using Back Propagation Neural Network in DWT Domain

Dr. N. Ramamurthy, Dr. K. C. T. Swamy, Gude Ramarao, H. Shravan Kumar

Abstract; Hiding an image in another image is the technique used for copy write protection. In this proposed work, the watermark is inserted into blue plane of the cover image, In this watermark extraction and embedding process, the back propagation neural network in conjunction with biorthogonal wavelets is utilized to improve the efficiency. The performance is tested by normalized correlation coefficient. The imperceptibility of the watermark is tested by cropping and rotation attacks effectively.

Keywords; Watermark, Wavelets, neural network, rotation, compression.

I. INTRODUCTION

Due to the quick and large development of transmission and additionally the widespread use of information superhighway, there is a want for economical, powerful and effective techniques to protect data [1]. Completely different watermarking techniques are developed in special and remodel domain strategies, however, in recent years; the watermarking techniques supported remodel domain ar developed to produce higher lustiness and physical property.

Digital Image watermarking techniques classified as private, semi private and public watermarking techniques. In private watermarking technique the knowledge of cover image and secret key required to recover the watermark from the cover image [2]. In semi-private or semi blind watermarking technique each the secrete key and also the watermark needed to extract the inserted watermark. In blind or public watermarking technique solely the secrete key's enough to extract the watermark [3]. Private watermarking techniques have high robustness than the other two techniques. But the drawback of private watermarking techniques is that they require original information to extract the watermark.

The main necessities of any watermarking technique embody hardiness, visibility, and capability. hardiness is that the strength of the watermark in order that it will stand up to totally different image process attacks like cropping, rotation and compression, etc[4]. Visibility of the watermark related to imperceptibility so that the appearance of the watermarked image may not be degraded by the presence of the watermark. The capacity of the watermark defined as the amount of data carried by it.

The technique of digital image watermarking is used to embed copyright information into multimedia content. Generation of watermark, watermark insertion, detection of watermark and attacks on watermarked image are the different steps in digital image watermarking. There are four essential factors which include robustness; imperceptibility, capacity, and blindness used to determine the quality of the watermarked image[5]..If the presence of the watermark is not destroying the imperceptibility of the cover image, then the technique is said to be more imperceptible. The blind watermarking technique cannot require the cover image to detect the watermark. The non-blind watermarking technique needs the cover image to detect the watermark. If the secret key and watermark bit sequence are required to detect the presence of the watermark, then the technique is referred to as semi-blind watermarking [6].

The watermarking techniques classified as spatial domain and transform domain techniques based on the domain of watermark insertion. In these techniques the location and luminance of the image pixels are processed directly and the drawback of this method is that the lossy compression can easily destroy these bits .In transform domain methods, special transformations are used to process the coefficients infrequency domain to hide the watermark [7]. In transform domain methods the watermark is inserted in to frequency coefficients of the host image. Low frequency coefficients are not selected to embed watermark, because they suppressed by filtering as noise.The transform domain method provides much better robustness against compression, filtering, rotation, cropping and noise attack compared to spatial domain technique[8].

Wavelets also process an image from low to the high resolution sequentially so that the missing data can be detected at another level [9]. The watermark must be embedded in high frequency coefficients for better imperceptibility, while low frequency coefficients must be selected for high robustness. Hence the watermark coefficients must be embedded in middle frequency coefficients to achieve the balance between robustness and imperceptibility [10]. .

Revised Manuscript Received on December 30, 2019.

* Correspondence Author

Dr. N. Ramamurthy, Professor, Department of Electronics and Communication Engineering, G. Pullaiah College of Engineering and Technology, Kurnool (A.P) India. E-mail: eceramamurthy@gpcet.ac.in

Dr. K. C. T. Swamy, Associate Professor, Department of Electronics and Communication Engineering, GPCET, Kurnool, (A.P) India.
E-mail: ecekctswamy@gpcet.ac.in

Gude Ramarao, Associate Professor, Department of Electronics and Communication Engineering, GPCET, Kurnool, (A.P) India.
E-mail: eceramarao@gpcet.ac.in

H. Shravan Kumar, Associate Professor, Department of Electronics and Communication Engineering, GPCET, Kurnool, (A.P) India.
E-mail: shravanece@gpcet.ac.in

In blind or public watermarking technique solely the secrete key's enough to extract the watermark . Private watermarking techniques have high robustness than the other two techniques. But the drawback of private watermarking techniques is that they require original information to extract the watermark.

II. WATERMARK EMBEDDING USING BACK PROPAGATION NEURAL NETWORK

A digital image is decomposed into low and high frequency subbands using first level decomposition. The low frequency subband is further decomposed, since the energy of the image is diffused further and the watermarks can be inserted with more intensity. In this work, the fourth level decomposition is implemented on cover image to increase the signal to noise ratio.

The watermark is embedded into low frequency components will decline the visual quality of the watermarked image. However, if the watermark is embedded into high frequency components, the robustness of the watermarked image will be affected and the watermark can be easily destroyed with normal image processing operations. In this work, the watermark is embedded into high and middle frequency coefficients using back propagation neural network to provide better robustness and imperceptibility. The training process of the back propagation neural network will be completed before watermarking and weights are adjusted using error signals which are back propagated to hidden and input layers.

Algorithm to embed watermark using BPNN:

Step 1: Read and acquire the color image of size NxN.

Step 2: Resize the selected color image of size NxN into 512x512 pixels and use it as cover image.

Step 3: Compute Red, Green and Blue planes of the cover image and select Blue plane to embed the watermark.

Step 4: Read the bitmap of size 64x64 Barbara as the watermark.

Step 5: Compute fourth level DWT on the Blue plane of the cover image to get the frequency subband coefficients {HH$_1$,

Step 6: Select the high and middle frequency coefficients to embed the watermark, and use the key to select the beginning position of the watermark.

Step 7: Apply the DWT coefficients to BPNN to perform quantization and then get the output $BPNN(round\left(\frac{T_{(g+key)}}{Q}\right))$; where $T_{(g+key)}$ is the selected cover image coefficient to embed the watermark, and Q is quantization value.

Step 8: Embed the watermark using

$$T'_{(g+key)} = BPNN(round\left(\frac{T_{(g+key)}}{Q}\right)) + X_g$$

Where$\mathrm{T}'_{(\mathrm{g+key})}$ is the watermarked image coefficient and X_g is the random watermark sequence.

Step 9: Apply IDWT on each coefficient to get the watermarked image.

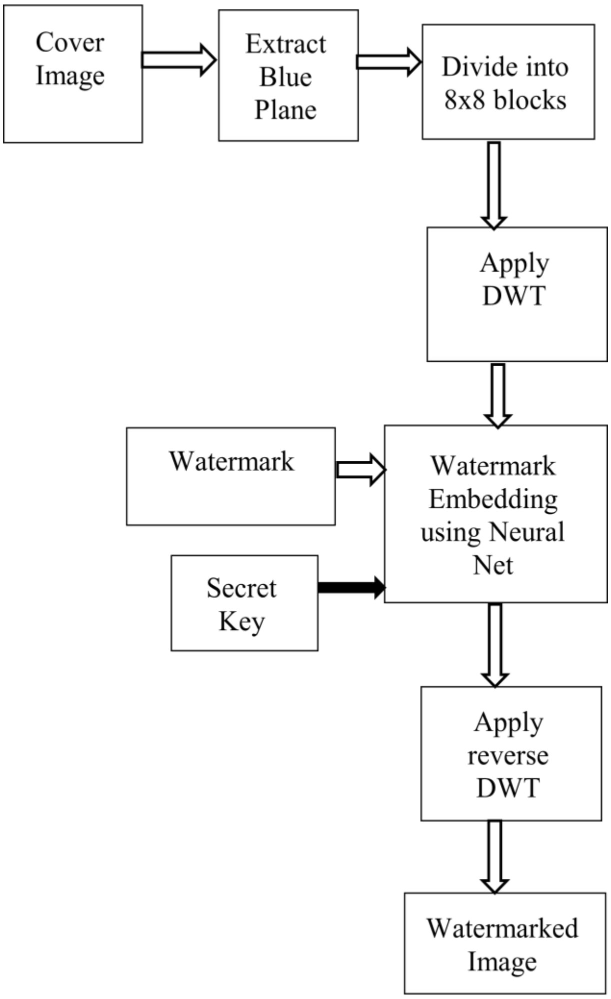

Fig.2.1: Watermark Embedding using BPNN

III. EXTRACTION OF WATERMARK USING NEURAL NETWORK

The watermark extraction method is kind of opposite to the method of watermark embedding. The detection of the watermark is obtained by the trained neural network. The parametric statistic is employed to sight the similarity between the initial watermark and extracted watermark. The block diagram representation of extraction process of watermark is shown in figure (3.1).

Watermark Extraction Algorithm using BPNN:

Step 1: Select the Blue plane of the watermarked image and apply DWT.

Step 2: Quantize the DWT coefficient $T''(g)$ by Q using BPNN to get $BPNN\ (round\ (T''(g)/Q)$.

Step 3: Extract the watermark X'_g using the equation

$$X'_g = T''(g) - BPNN(round\left(\frac{T''(g)}{Q}\right))$$

Step 4: Measure the similarity between the original watermark X_g and the extracted watermarkX'_g.

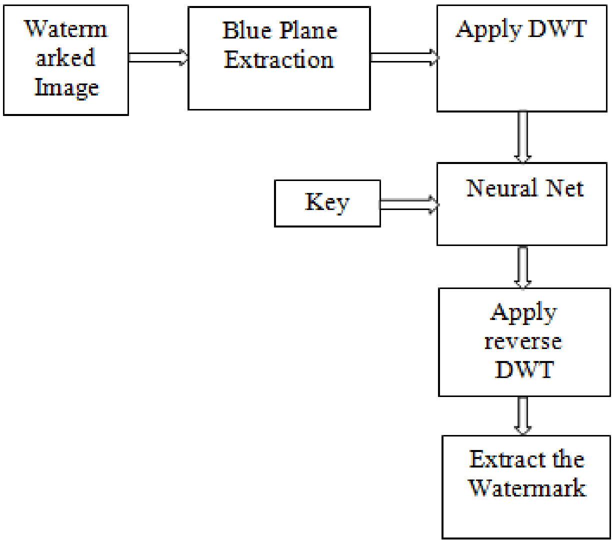

Fig.3.1: Watermark Extraction using BPNN

IV. EXPERIMENTAL RESULTS

Pears and peppers color images of 512x512 size are used as the cover images and grey scale bitmap of size 32x32 the watermark. The Peak Signal to Noise Ratio of the watermarked image is

$$PSNR = 10\log_{10}\left(\frac{R*R}{MSE}\right) \quad \dots\dots\dots\dots \quad (4.1)$$

‘ R’ represents fluctuation at max in cover image=511;

MSE is Mean Square Error, given by

$$MSE = \sum_{p=1}^{r}\sum_{q=1}^{c}\frac{[F(p,q) - F'(p,q)]^2}{rc} \quad \dots\dots\dots \quad (4.2)$$

‘r’ represents rows in the digital image

c = number of columns in the digital image

$F\ (p,q)$and $F\,'(p,q)$ represent blue plane of cover image and watermarked image.

The similarity between the original watermark$W\ (x,y)$ and the extracted watermark $W\,'(x,y)$is calculated using the formula

$$NCC = \frac{\sum_x\sum_y W(x,y)*W'(x,y)}{\sum_x\sum_y W(x,y)*W(x,y)} \dots\dots\dots \quad (4.3)$$

The robustness of the watermarked image is tested by attacks such as Cropping, and Rotation attacks.

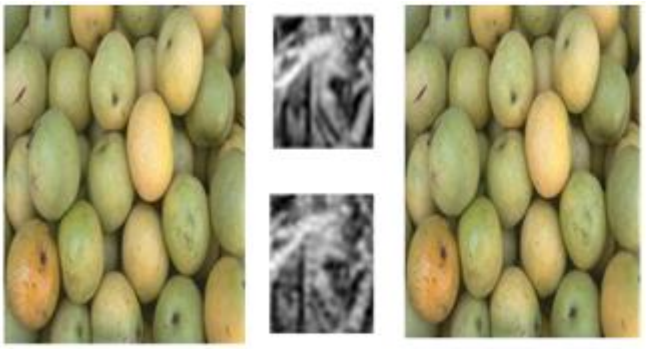

Fig. 4.1 Cover image, Watermark image, Extracted watermark and Watermarked image

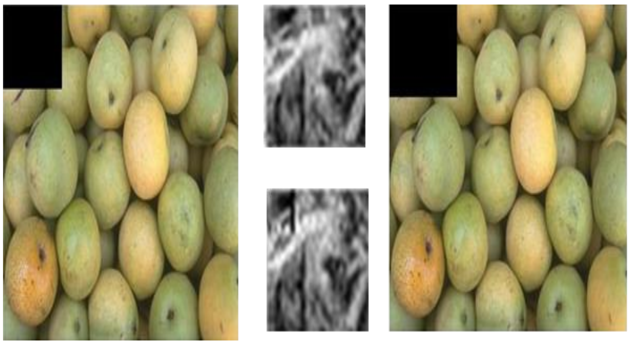

Fig4.2: 5 % cropping attack, Extracted watermark for 5% cropping attack, Extracted watermark for 10% cropping attack, 10% cropping attack

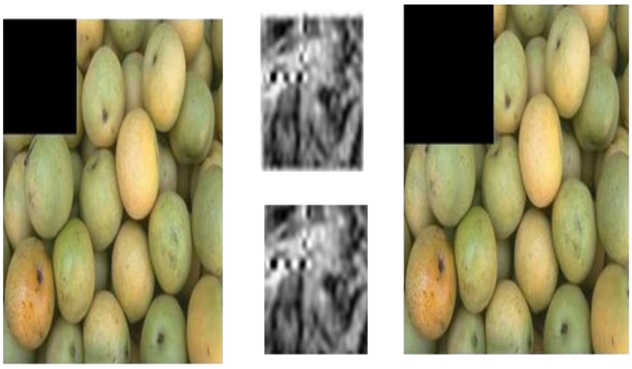

Fig.4.3: 15 % cropping attack, Extracted watermark for 15% cropping attack, Extracted watermark for 20% cropping attack, 20% cropping attack

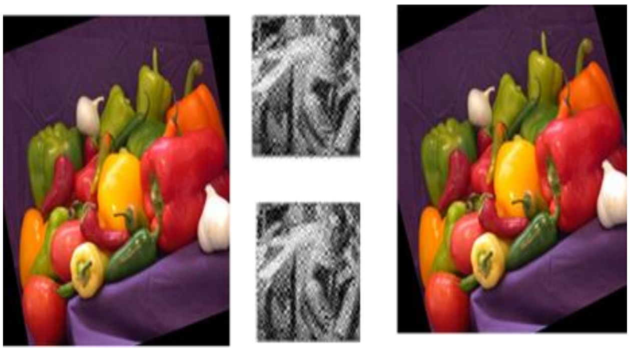

Fig4.4:15 degrees rotation attack, Extracted watermark for 15 degrees rotation attack, Extracted watermark for 20 degrees rotation attack, 20 degrees rotation attack.

Table 4.1: PSNR for cropping and rotation attacks

Type of attack	Intensity			
	5%	10%	15%	20%
PSNR for cropping	29.6547	28.6244	27.5744	26.1349
PSNR for rotation	23.5404	21.1039	19.9095	19.3169

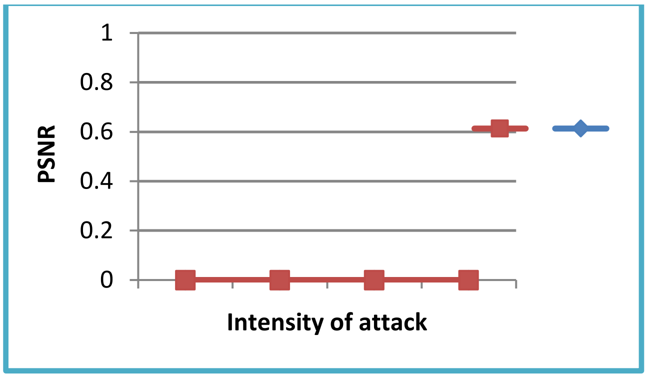

Chart 4.1: Variation of PSNR for cropping and Rotation

V. CONCLUSIONS & FUTURE SCOPE

In this paper, the imperceptibility measured by finding peak signal to noise ratio. The robustness tested by measuring the normalized correlation coefficient against cropping and rotation attacks. The proposed algorithms can be extended for multiple watermark insertion and for video images can be developed. The proposed algorithms are designed to embed a single watermark and hence the algorithms can be developed to embed multiple watermarks.

REFERENCES

1. Amarjot Kaur & Jagdeep Singh “Digital Image Watermarking Techniques: A Review”, IARCS, Volume 8, No. 8, September-October 2017.
2. Nallagarla Ramamurthy et al, “Detection of Glaucoma using Adaptive Neuro Fuzzy in DWT Domain”, International Journal of Recent Technology and Engineering (IJRTE),ISSN: 2277-3878, Volume-7, Issue-6S, March 2019,pp 314-317
3. Nallagarla Ramamurthy et al, “Interpolation of the Histogramed MR Brain Images for Resolution Enhancement”, International Journal of Innovative Technology and Exploring Engineering (IJITEE),ISSN: 2278-3075, Volume-8 Issue-11, pp 1253-1256,September 2019
4. Wang Chunpeng, Wang Xingyuan, Zhang Chuan, Xia Zhiqiu “Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution” Signal Processing, 11 December 2016.
5. X.Y. Wang, Y.N. Liu, S. Li, H.Y. Yang, P.P. Niu, Robust image watermarking approach using polar harmonic transforms based geometric correction. Neurocomputing 174 627-642. doi: 10.1016/j.neucom.2015.09.082
6. Yue Li ,Dong Liu ; Houqiang Li ; Li Li ; Zhu Li ; Feng Wu “Learning a Convolutional Neural Network for Image Compact-Resolution" IEEE Transactions on Image Processing ,Volume: 28 , Issue: 3 , March 2019
7. Annegreet Van Opbroek et al “Transfer Learning for Image Segmentation by Combining Image Weighting and Kernel Learning” IEEE Xplore,2019.
8. Atoany Fierro-Radilla et al,“A Robust Image Zero-watermarking using Convolutional Neural Networks” 2019 7th International Workshop on Biometrics and Forensics, IEEE Xplore,2019.
9. Mahmood Al-khassaweneh “Robust and Invisible Watermarking Technique Based on Frei-Chen Bases” IEEE International Conference on Electro Information Technology, IEEE Xplore,2019.
10. “Robust Image Zero-watermarking using Convolutional Neural Networks” 7th International Workshop on Biometrics and Forensics, IEEE Xplore,2019.

AUTHORS PROFILE

Dr. N. Ramamurthy, did his B.Tech and from S. V. University. He received his Ph.D. from JNTUA, Ananthapuramu. Currently, he is working as professor & Dean IQAC at G.Pullaiah college of Engineering and Technology, Kurnool.

Dr. K. C. T. Swamy, received his M.Tech and Ph.D. from Osmania University. He is the Principle Investigator for SERB project of worth 40 lakhs at G.Pullaiah College of Engineering and Technology, where he is currently working as Associate Dean of R&D, Kurnool. A.P, India.

Gude Ramarao, did his B.Tech at V. R. Siddhartha Engineeing college, Vijayawada and M.Tech at JNTUA, Ananthapuramu. At present, he is working as associate professor & Placement coordinator in G.Pullaiah College of Engineering and Technology, Kurnool, A.P, India.

H. Shravan Kumar, did his B.Tech and M.Tech at JNTUH, Hyderabad. Currently, he is working as Associate Professor of ECE in G.Pullaiah College of Engineering and Technology, Kurnool, A.P India.