

A Novel Robust Crypto-Watermarking Scheme Based on Hybrid Transformers

A.M. El-Assy, M.A. Mohamed, M.E.A. Abou-El-Seoud, H.E.S. Mostafa

Abstract— The rapid growth of digital computer technology has recently led to the widespread use of digital media from digital documents, video and digital images due to the ease and speed of transfer, distribution and copying over computer networks. However, this technology lacks the protection of its digital products from illegal use and imitation. The protection of intellectual property rights for digital media has therefore become a major concern. For this reason, this paper attempts to provide an easy; fast way; imperceptible and robust solution to achieve this goal by using watermark technology in static grey scale images. this paper present a proposed technique depends on integration of encryption with discrete wavelet transform; discrete cosine transform, singular value decomposition, and principal component analysis (PCA). this method provides High resiliency and the good visual quality of the watermark images extracted from the several distorted watermarked images Where NC value reached almost 1 when applying most types of attacks Especially when images are cropped and compressed, which these are one of the worst types of attacks that destroy intellectual property. The resulting PSNR achieved up to 93.23613 dB. In addition, the results of proposed algorithms have been compared with many new related algorithms, published in trusted journals to prove that proposed technique is the best.

Index Terms— Digital watermarking, discrete wavelet transform (DWT); discrete cosine transform (DCT), singular value decomposition (SVD), principal component analysis (PCA), copyright protection.

1 INTRODUCTION

In recent years the usage of internet has increased tremendously, the growth of the technology has simplified sharing of the digital images, videos or any other legal document. So, illegal reproduction of data has also emerged with this extraordinary revolution and is raising questions and concerns about ownership rights. The problem of unauthorized access can be solved by adding digital watermarking to the image. Watermarking (data hiding) [1], [2] is the process of embedding data into a multimedia element such as image, audio or video. Watermarking may be visible or invisible, blind or non-blind, fragile, robust or semi-fragile etc. The watermark may be any text, image or logo of the distributor which acts as the ownership information of the valid or authorized distributor in order to guarantee the ownership and the integrity. The basic requirements for a secure watermarking scheme are imperceptibility, robustness, capacity and security.

Digital image watermarking is mainly grouped into two classes: transform domains [3], [4], [7], [8], and spatial domains [1], [5], [6]. The most commonly used transforms are: the discrete Fourier transform (DFT) [9], discrete cosine transforms (DCT) [10], [11], [7], discrete wavelets transform (DWT) [12], [13], [14], and singular value decomposition (SVD) [15], [16]. Mohananthini, et al [17] presented an optimization of different watermarking plot with genetic algorithms. The inserting and extricating handle employments the combination of discrete wavelet transform(DWT) and singular value deterioration (SVD). However, this algorithm adds the watermark

information to the singular values of the diagonal matrix, Nevertheless, the watermark is embedded in SVD domain, which causes large information transmission because of the left/right orthogonal matrices. Xiaoyi, et al [18] present a hybrid digital watermarking scheme based on DCT, the implanting concentrated of the watermark was decided agreeing to the texture sorts gotten by SVM, and the position of the watermark was embedded on the premise of the optimized GA. To upgrade the robustness of watermarked image while considering the trade-off between transparency and robustness, but unfortunately there are some disadvantages like adaptive genetic not ensure the convergence of the genetic algorithm and algorithm less adaptive because the classification using SVM inaccurate classification. Boris Escalante-Ramírez, et al [19] present watermarking scheme based on a perceptive model that takes advantage of the masking characteristics of the HVS, hence permitting the era of a watermark that cannot be recognized by a human eyewitness. this watermark resisted most of geometric attacks, the worst case being image under a scaling attack.

To advance progress watermark robustness and imperceptibility, Ansari et al. [20] presented an improved robust watermarking algorithm based on the combination between SVD and the integer wavelet transform (IWT) Compared with the previous method, this strategy accomplishes promising execution. Singh, D.; et al. [21] proposed a blind and robust technique in the DWT, SVD, and DCT domains, DCT applied on the matrices generated from the most significant bit-planes and the least significant bit-planes of the watermark and imbedded into the singu-

lar values of the carrier image using a DWT-SVD-based method. To enhance the watermark imperceptibility, Xiao Zhou et al [22] present hybrid watermarking method based on The discrete wavelet transform (DWT), all phase discrete cosine biorthogonal transform (APDCBT) and singular value decomposition (SVD), The watermark signal has modified DC coefficients of each sub-block in HL and LH sub-bands to take advantage of low frequency aggregation property of APDCBT. Sanjana Sinha et al [23] present a new technique based on Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA), This method has benefited from the advantages of PCA whereas reduces correlation among the wavelet coefficients. To increase the security level of the watermarking algorithm, Basant Kumar et al [24] combine between spread-spectrum watermarking algorithm and discrete wavelet transform (DWT). Low uncorrelated code has been generated from the watermark signal and embedded in to DWT coefficients.

To overcome the impediments of the current watermarking schemes and upgrade the security of digital multimedia information this paper has been presented the proposed techniques in transformed domain. the watermarking algorithm based on combining two techniques: spread spectrum technique and transform techniques. the combining of two techniques improved the performance of the watermarking algorithms that are based solely on one techniques. The proposed algorithm works by applying biorthogonal wavelet transform (BWT), discrete cosine Transform (DCT), Principal Component Analysis (PCA), and Singular Value Decomposition (SVD).

This paper is organized as follows: Section 2 describes the Transforms used for Watermarking. Section 3 explains the steps for the proposed algorithm. Section 4 discusses the results which are compared with similar previous algorithms and Section 5 concludes the research work.

2. TRANSFORMED DOMAIN TECHNIQUES

2.1 DISCRETE WAVELET TRANSFORM

Wavelet transform disintegrates an image into a set of four sub band which can be reassembled to reconstruct the original image without error. Dwt apply 2-D filters in each dimension. The input image has been divided by this filters into four non-overlapping multi-resolution sub bands, a diagonal HH1, horizontal HL1, vertical LH1 detail components and lower resolution approximation image LL1. Most signal information of original image is in the low frequency district. While the upright detail, the level detail and the diagonal detail of the original image is in LH, HL and HH frequency district respectively [25], [26].

2.1.1 BIORTHOGONAL WAVELET TRANSFORM

Biorthogonal wavelet bases have been used to gain greater flexibility in the construction of wavelet bases. Within the biorthogonal case, instead of having one scaling and wavelet function, there are two scaling functions that will create diverse multiresolution investigation, and appropriately two distinctive wavelet functions. The double scaling and wavelet functions have the taking the following properties: They are zero exterior of a segment, the calculation calculations are maintained, and in this way exceptionally simple, the related channels are symmetrical, the functions used within the calculations are less demanding to construct numerically than those utilized within the Daubechies wavelets [27].

2.2 DISCRETE COSINE TRANSFORM

The DCT have been used to convert a signal into elementary frequency components. this transform DCT is a way to separate the spectral regions of the image according to their energy. DCT-based watermarking is based on two facts. The first fact is the most important visual parts of the image lie into low-frequencies Sub-band which has much of the signal energy, the second fact is that the image components of high frequency are usually removed through compression and noise attacks [28, 29, 30].

2.3 SINGULAR VALUE DECOMPOSITION

SVD is a practical numerical method used to decompose the matrix into three matrices that are of the same size as the original matrix (31). Then SVD of original matrix A is defined as

$$AA = USV^T \quad (1)$$

Where U and V are orthogonal matrices; S is Diagonal elements which called singular values

2.4 PRINCIPAL COMPONENT ANALYSIS

It could be a dimension-reduction tool that can be utilized to diminish an expansive set of factors to a little set that still contains most of the data within the huge set. (PCA) could be a scientific strategy that changes a number of (conceivably) related factors into a (littler) number of uncorrelated factors called principal components. The first principal component accounts for as much of the inconstancy within the information as conceivable, and each succeeding component accounts [32].

2.4.1 PCA ALGORITHM:

This algorithm used to calculate the principal components of second quadrant

Step 1: the second quadrant is converted into a row vector D with N^2 elements

Step 2: the mean μ and standard deviation σ of the elements of vector D have been Computed.

Step 3: according to the following equation Z have been computed

$$Z = \frac{(D - \mu)}{\sigma} \quad (2)$$

Step 4: Carry out principal component analysis on Z (size $1 \times N^2$) to obtain the principal component coefficient matrix coefficient (size $N^2 \times N^2$).

Step 5: Calculate vector pcax.

$$pcax = Z * coeff \quad (3)$$

Where pcax represents the principal component of second quadrant.

2. PROPOSED ALGORITHM

The proposed watermarking scheme is combined BWT, DCT, SVD, PCA, and pn-code techniques to develop a new hybrid non-blind image watermarking scheme that is imperceptible to a variety of attacks. The proposed technique is given by the following algorithm

3.1 EMBEDDING PROCESS

Step 1: DWT is applied to host image of size 512×512 to decompose it into four non overlapping sub-bands LL, HL, LH and HH each of size 264×264 using biorthogonal mother function.

Step 2: Convert the $n \times n$ binary watermark logo into a vector '0's and '1's.

Step 3: Generate pseudorandom sequence

Step 4: Encrypt watermark using XOR between watermark and pn-code.

Step 5: Apply DCT to HL band and get DCT coefficient matrix h.

Step 6: Map DCT coefficient matrix h into four quadrants q1, q2, q3 and q4 by using zigzag scanning.

Step 7: apply PCA on second quadrant using PCA algorithm.

Step 8: Apply SVD on the PCA components of the quadrant.

$$[u, s, v] = SVD(pcax) \quad (4)$$

Where pcax represents the principal component of second quadrant

Step 9: modified singular values by adding values of the Encrypted watermark with strength α

$$temp = s + \alpha * EW \quad (5)$$

Where Temp represents modified singular values of the PCA components of the second quadrant

Step 10: Apply SVD to modified singular values of the PCA components

$$[u1, s1, v1] = SVD(temp) \quad (6)$$

Step 11: apply inverse SVD to obtained the modified PCA components

Step 12: apply inverse PCA to obtained modified second quadrant

Step 13: Mapping coefficients from zigzag scanning to original position matrix H*.

Step 14: Apply inverse DCT to H* to produce HL*.

Step 15: Apply inverse DWT to LL, LH, HL*.and HH to get watermarked image

3.2 EXTRACTION PROCESS

Step 1: DWT is applied to watermarked image of size 512×512 to decompose it into four non overlapping sub-bands LL, HL, LH and HH each of size 264×264 using biorthogonal mother function.

Step 2: Generate pseudorandom sequence)

Step 3: Apply DCT to HL band and get DCT coefficient matrix h.

Step 4: Map DCT coefficient matrix h into four quadrants q1, q2, q3 and q4 by using zigzag scanning.

Step 5: apply PCA on second quadrant using PCA algorithm.

Step 6: Apply SVD on the PCA components of the quadrant of watermarked image.

$$[ru, rs, rv] = SVD(rpcax) \quad (7)$$

Step 7: apply invers SVD as in equation

$$SN = u1 * rs * v1^t \quad (8)$$

Step 8: the encrypted watermark bits are extracted from the singular value of the principal component of second quadrant as in equation

$$REW = (SN - S) / \alpha \quad (9)$$

Where REW represents the encrypted watermark bits are extracted from the singular value of the principal component of second quadrant.

Step 9: decrypt watermark using XOR between encrypted watermark and pn-code to get the recovered watermark.

4. DIGITAL IMAGES DATASET

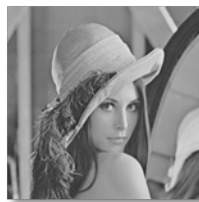
The proposed techniques tested on three standard still images of size 512×512 ; (i) (Lena.bmp), (ii) (boat.tiff), and (iii) (Barbara.png) as a host image; and used a small black and white image of size 32×32 as a watermark image as shown in figure 1.

5. PERFORMANCE EVALUATION METRICS:

Watermarking techniques are usually assessed as for three metrics: imperceptibility, capacity, and robustness against various type of attacks.

5.1 IMPERCEPTIBILITY

Imperceptibility depends on human visual system, it is mean that the watermark should not be noticeable to the viewer and when embed the watermark into a host image there is no distortion introduced to the digital watermarked image. In this paper mean square error, peak signal to noise ratio, and correlation coefficients, used to measure the imperceptibility.



Lena.bmp



boat.tiff



Barbara.png



HF image

Fig. 1. host and watermark images

5.1.1 MEAN SQUARE ERROR (MSE)

$$MSE = \frac{1}{M \cdot N} \sum_{i=1}^M \sum_{j=1}^N (I(i, j) - IW(i, j))^2 \quad (10)$$

Where I: represents the cover image, I_w : represents the watermarked version of the cover image, M: represents rows, N: represents columns, and F: represents the image frames.

5.1.2 PEAK SIGNAL TO NOISE RATIO (PSNR)

$$PSNR = 20 \log \frac{2^n - 1}{\sqrt{MSE}} \quad (11)$$

5.1.3 NORMALIZED CORRECTION (NC)

$$R = \frac{1}{N} \left[\frac{\sum_{i=1}^N (X_i - \bar{X}) \sum_{i=1}^N (Y_i - \bar{Y})}{\sum_{i=1}^N (X_i - \bar{X})^2 \sum_{i=1}^N (Y_i - \bar{Y})^2} \right] \quad (12)$$

Where X represent the watermark image, and Y represent the recovered watermark image

5.2 CAPACITY

The effective watermarking ought to be able to carry more data but ought to not degrade the image. to measure the capacity we used water document ratio.

5.2.1 WATERMARK-TO-DOCUMENT RATIO (WDR)

$$WDR = 10 \times \log \frac{\sum_{i=1}^M \sum_{j=1}^N (I(i, j) - I_w(i, j))^2}{\sum_{i=1}^M \sum_{j=1}^N I^2(i, j)} \quad (13)$$

5.3 ROBUSTNESS

Watermark robustness can be checked by applying various types of attacks such as Gaussian blur, Gaussian noise, median filter, JPEG compression, sharpening, rotation, cropping, contrast adjustment, and histogram equalization and tested the ability of watermarking to resist this attack.

5.3.1 THE BIT CORRECT RATIO (BCR)

$$BCR = \frac{100}{l} \sum_{n=0}^{l-1} \begin{cases} 1 & W'_n = W_n \\ 0 & W'_n \neq W_n \end{cases} \quad (14)$$

6. EXPERIMENTS AND RESULTS

The proposed watermarking technique and other techniques which have been explained in [23], [24], [17] were tested without and with attacks like: Gaussian blur, Gaussian noise, median filter, JPEG compression, sharpening, rotation, cropping, contrast adjustment, and histogram equalization.

In figure 2 and figure 3 the human eyes will see the effect of noises on watermarked images and the best extracted watermark image after applying the attacks on watermarked image like: Gaussian blur with (5*5) box filter, Gaussian noise with (variance .3), median filter with (5*5) box filter, JPEG compression, sharpening, rotation by an angle of 10 degrees, cropping by 40%, contrast adjustment using .8 gamma factor, and histogram equalization.

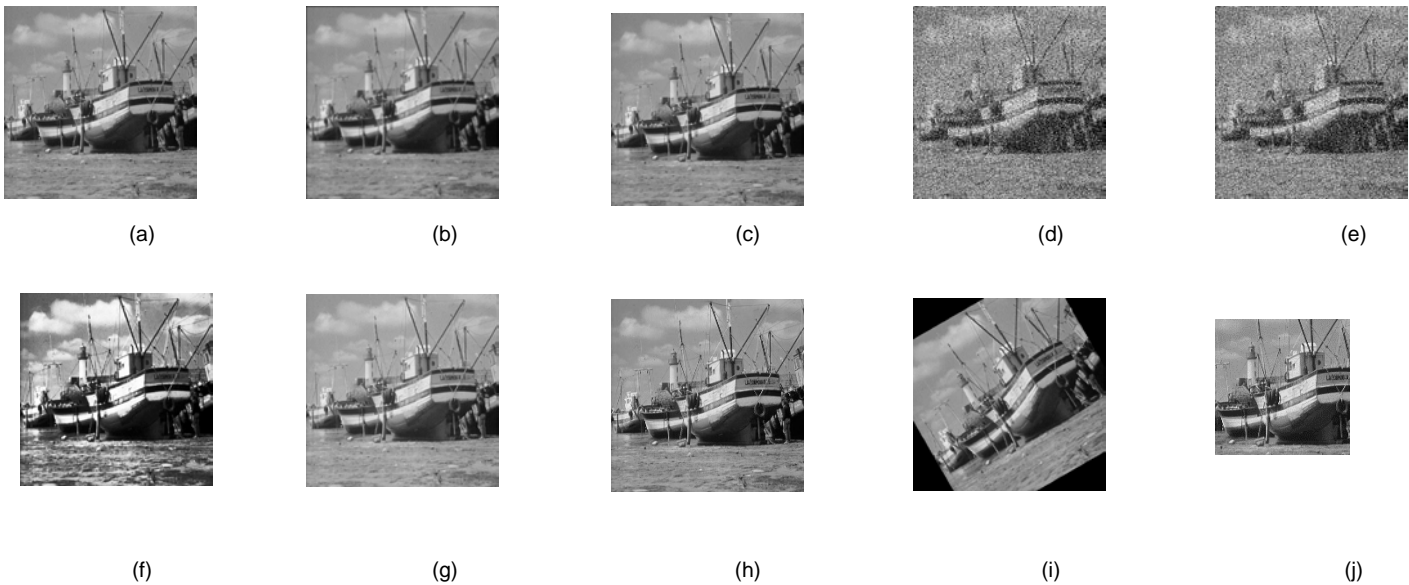


Fig.2. shows different types of noisy attacked image, (a) Watermarked image without attack; (b) Watermarked image with Gaussian blur (5x5); (c) Watermarked image with median filter(5x5); (d) Watermarked image with salt and paper noise(.01); (e) Watermarked image with Gaussian noise(.3); (f) Watermarked image with histogram equalization; (g) Watermarked image with Gamma correction 0.8; (h) Watermarked image with JPEG compression (70%); (i) Watermarked image with rotation 10°; (j) Watermarked image with cropping by 40%

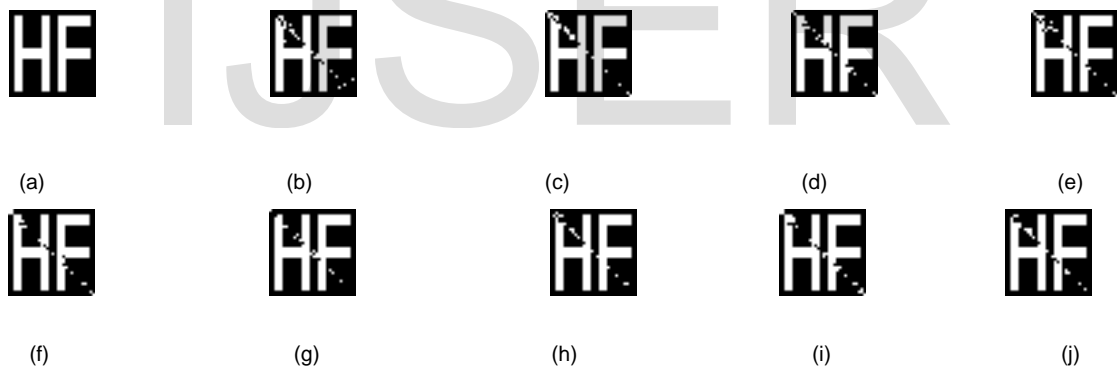


Fig. 3. shows the extracted watermark image from corresponding noisy attacked image When Applied second Proposed Technique , (a) Extracted image without attack; (b) Extracted image with Gaussian blur (5x5); (c) Extracted image with median filter(5x5); (d) Extracted image with salt and paper noise(.01); (e) Extracted image with Gaussian noise(.3); (f) Extracted image with histogram equalization; (g) Extracted image with Gamma correction 0.8; (h) Extracted image with JPEG compression (70%); (i) Extracted image with rotation 10°; (j) Extracted image with cropping by 40%; (k) Extracted image with cropping by 50%

The following tables show the value of the data collected from the watermarked image after performing the various attacks as shown previously

TABLE 1.
PERFORMANCE RESULTS IN TERMS OF AVRAGE PSNR

| Attacks | S. Sinha et al[23] | B. Kumar et al [24] | N. Mohananthini et al [17] | Proposed |
|--------------------|--------------------|---------------------|----------------------------|-------------|
| no attack | 8.06E+01 | 60.29460236 | 31.66284264 | 93.23613181 |
| Gaussian noise(.3) | 8.404450607 | 8.414343849 | 8.419548257 | 8.414619954 |

| | | | | |
|------------------------------------|-------------|-------------|-------------|-------------|
| Gaussian blur(5×5) | 28.61257692 | 28.6123788 | 28.57925568 | 29.21244714 |
| Median(5×5) | 36.25322081 | 36.24295809 | 35.65861894 | 36.25356815 |
| Salt and pepper noise (.01) | 10.47008411 | 10.46494769 | 10.41543798 | 10.46774589 |
| Histogram Equalization | 17.12029362 | 18.12920192 | 17.82800993 | 18.12029362 |
| Gamma correction 0.8 | 22.81118802 | 22.80431191 | 22.36062054 | 23.81118802 |
| Jpg compression (70%) | 37.87021515 | 37.84598094 | 30.19293466 | 41.87021515 |
| Jpg compression (50%) | 32.326 | 31.29669494 | 30.77988457 | 33.49533618 |
| Jpg compression (30%) | 29.36 | 30.68857594 | 29.7242648 | 31.83125847 |
| Cropping by 50% | 9.023645 | 9.045705646 | 9.032790555 | 9.077481673 |
| Cropping by 40% | 7.807063544 | 7.807 | 7.798926412 | 8.807063537 |
| Rotation 10° | 9.962593079 | 10.6221 | 10.59493032 | 12.62249726 |

TABLE 2.

PERFORMANCE RESULTS IN TERMS OF MAXIMUM MSE

| Attacks | S. Sinha et al[23] | B. Kumar et al [24] | N. Mohananthini et al [17] | Proposed |
|-----------------------------|--------------------|---------------------|----------------------------|-------------|
| no attack | 5.34E-07 | 0.05700772 | 41.6015625 | 2.90E-05 |
| Gaussian noise(.3) | 8.81E+03 | 8.79E+03 | 8.78E+03 | 8.79E+03 |
| Gaussian blur (5×5) | 83.97233213 | 83.97616289 | 84.61908773 | 83.97484142 |
| Median(5×5) | 14.45678844 | 14.49099137 | 16.5779953 | 14.41563227 |
| Salt and pepper noise (.01) | 5.48E+03 | 5.48E+03 | 5.54E+03 | 5.48E+03 |
| Histogram Equalization | 9.41E+02 | 9.39E+02 | 1.01E+03 | 9.41E+02 |
| Gamma correction 0.8 | 3.19E+02 | 3.20E+02 | 3.54E+02 | 3.19E+02 |
| Jpg compression (70%) | 9.962593 | 10.01834 | 48.35801 | 9.962593 |
| Jpg compression (50%) | 29.06988 | 44.31279 | 50.98066 | 29.07681 |
| Jpg compression (30%) | 45.3965 | 5.07E+01 | 55.88019 | 42.65348 |
| Cropping by 50% | 6600.171 | 7.60E+03 | 7.62E+03 | 9.72E-01 |
| Cropping by 40% | 1.01E+04 | 1.01E+04 | 1.01E+04 | 1.01E+04 |
| Rotation 10° | 5.29E+03 | 5.29E+03 | 5.32E+03 | 5.29E+03 |

TABLE 3.
PERFORMANCE RESULTS IN TERMS OF AVRAGE ABSOLUTE WDR

| Attacks | S. Sinha et al[23] | B. Kumar et al [24] | N. Mohananthini et al [17] | Proposed |
|-----------------------------|--------------------|---------------------|----------------------------|-------------|
| no attack | 8.03E+01 | 54.92252548 | 26.29076576 | 87.86405493 |
| Gaussian noise(.3) | 3.032373726 | 3.042266968 | 3.047471376 | 3.042543072 |
| Gaussian blur (5×5) | 23.24050004 | 23.24030192 | 23.20717879 | 24.24037026 |
| Median(5×5) | 30.88114393 | 30.8708812 | 30.28654206 | 31.88149126 |
| Salt and pepper noise (.01) | 5.098007226 | 5.092870804 | 5.0433611 | 5.095669005 |
| Histogram Equalization | 12.74821674 | 12.75712504 | 12.45593305 | 13.94821674 |
| Gamma correction 0.8 | 17.43911114 | 17.43223503 | 16.98854366 | 18.23911114 |
| Jpg compression (70%) | 32.49814 | 32.4739 | 24.82086 | 32.49814 |
| Jpg compression (50%) | 26.36 | 27.92462 | 25.40781 | 28.15273 |
| Jpg compression (30%) | 25.36 | 24.3165 | 22.35219 | 27.48866 |
| Cropping by 50% | 3.659 | 3.673629 | 3.660714 | 3.73488 |
| Cropping by 40% | 2.434987 | 2.435 | 2.42685 | 2.434987 |
| Rotation 10° | 5.250412877 | 5.25 | 5.222853439 | 6.25042038 |

TABLE 4.
PERFORMANCE RESULTS IN TERMS OF AVRAGE NC

| Attacks | S. Sinha et al[23] | B. Kumar et al [24] | N. Mohananthini et al [17] | Proposed |
|-----------------------------|--------------------|---------------------|----------------------------|----------|
| no attack | 1 | 1 | 1 | 1 |
| Gaussian noise(.3) | 0.65775 | 0.399403 | 0.522319 | 0.964289 |
| Gaussian blur (5×5) | 0.977687 | 0.493255 | 0.544607 | 0.953205 |
| Median(5×5) | 0.976047 | 0.690093 | 0.316552 | 0.958235 |
| Salt and pepper noise (.01) | 0.753022 | 0.430582 | 0.581631 | 0.95857 |
| Histogram Equalization | 0.970624 | 0.574191 | 0.998583 | 0.975116 |
| Gamma correction 0.8 | 0.97895 | 0.908276 | 1 | 0.981763 |
| Jpg compression (70%) | 0.971971 | 0.745468 | 1 | 0.967698 |

| | | | | |
|-----------------------|----------|----------|----------|----------|
| Jpg compression (50%) | 0.9658 | 0.649028 | 0.997171 | 0.971767 |
| Jpg compression (30%) | 0.9566 | 0.590357 | 0.702621 | 0.955276 |
| Cropping by 50% | 0.236 | 0 | 0.854943 | 0.959554 |
| Cropping by 40% | 0.900694 | 0.8745 | 0.613651 | 0.961349 |
| Rotation 10° | 0.953205 | 0.56981 | 0.439424 | 0.941819 |

TABLE 5.

PERFORMANCE RESULTS IN TERMS OF AVRAGE ABSOLUTE BCR

| Attacks | S. Sinha et al[23] | B. Kumar et al [24] | N. Mohananthini et al [17] | Proposed |
|-----------------------------|--------------------|---------------------|----------------------------|----------|
| no attack | 100 | 100 | 65.625 | 100 |
| Gaussian noise(.3) | 74.12109 | 47.36328 | 37.59766 | 97.46094 |
| Gaussian blur (5×5) | 98.4375 | 60.35156 | 19.43359 | 97.67969 |
| Median(5×5) | 98.33984 | 80.07813 | 44.14063 | 97.07031 |
| Salt and pepper noise (.01) | 80.66406 | 48.33984 | 65.52734 | 97.07031 |
| Histogram Equalization | 97.94922 | 69.53125 | 65.52734 | 98.24219 |
| Gamma correction 0.8 | 98.53516 | 93.94531 | 65.625 | 98.73047 |
| Jpg compression (70%) | 98.04688 | 81.73828 | 65.625 | 97.75391 |
| Jpg compression (50%) | 96.364 | 75.48828 | 65.42969 | 98.04688 |
| Jpg compression (30%) | 94.365 | 69.43359 | 40.625 | 96.875 |
| Cropping by 50% | 80.368 | 22.3659 | 58.00781 | 97.16797 |
| Cropping by 40% | 92.67578 | 66.235 | 37.89063 | 97.26563 |
| Rotation 10° | 96.67969 | 70.259 | 44.53125 | 95.80078 |

- 1 The Proposed technique has a good performance on imperceptibility and robustness as compared to previous technique.
- 2 The strength of this method lies in the integration of several different methods, as a result of this we got a high NC, PSNR, WDR, BCR when applying various attacks such as JPEG compression, Gaussian Noise, Gaussian Blur, Salt & Pepper Noise and Rotation with cropping.
- 3 In JPEG compression, although the compression ratio has been increased, the value of NC, PSNR, WDR have good value unlike other techniques.

- 4 This technique provides a good solution for cropping attack, where it is shown through the process of comparison that it maintains good results no matter what the cut part of the image

7. CONCLUSIONS

The proposed digital watermarking algorithm combined five techniques based on BWT-DCT-PCA- SVD- spread-spectrum. The proposed scheme has shown both the significant improvement in perceptibility and the robustness under various types of image processing attacks. The proposed algorithm can effectively resist certain attacks such as JPEG compression, and rotation. the strength of this

method lies in that it can balance most attacks and give high value to PSNR, WDR, NC, and BCR. Finally, the proposed scheme has been able to meet three important properties: security, imperceptibility and robustness, and makes a trade-off among them. Therefore, the proposed method is a useful tool for ownership identification and copyright protection.

6. REFERENCE

- [1] C. I. Podilchuk and E. J. Delp, "Digital Watermarking: Algorithms and Applications," IEEE Signal Processing Magazine Journal, vol. 18, no. 4, pp. 33-46, July 2001.
- [2] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2002.
- [3] W.-C. Hu, W.-H. Chen, and C.-Y. Yang, "Robust image watermarking based on discrete wavelet transform, discrete cosine transform and singular value decomposition," Journal of Electronic Imaging, vol. 21, no. 3, p. 033005, July 2012
- [4] P. Taoaand and A. M. Eskicioglu, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain", Internet Multimedia Management Systems Proceedings of the SPIE, vol. 5601, pp. 133-144, 2004.
- [5] C. Das, S. Panigrahi, V. K. Sharma, and K. K. Mahapatra, "A novel blind robust image watermarking in DCTdomain using inter-block coefficient correlation", International Journal of Electronics and Communications, vol. 3, no. 2, pp. 244-253, March 2014
- [6] R. Z. Liu, and T. N. Tan, "An SVD-based watermarking scheme for protecting rightful ownership", IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121-128, 2002.
- [7] M. Mondal and D. Barik, "Spatial Domain Robust Watermarking Scheme for Color Image," International Journal of Advanced Computer Science, vol. 2, no. 1, pp. 24-27, January 2012.
- [8] C. Qin, P. Ji, W. J. Wang, and C. C. Chang "Fragile image watermarking scheme based on VQ index sharing and self-embedding", Multimedia Tools and Applications, vol. 76, no. 2, pp 2267-2287, January 2016
- [9] Y. P. Hu, Z. J. Wang, H. Liu, and G. J. Guo, "A geometric distortion resilient image watermark algorithm based on DWT-DFT", journal of software, vol. 6, pp. 1805-1812, 2011.
- [10] J. C. Patra, J. E. Phua, C. Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression," Digital Signal Processing, vol. 20, no. 6, pp. 1597-1611, 2010.
- [11] S. D. Lin, S. C. Shie, J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," Computer Standards & Interfaces, vol. 32, no. 1-2, pp. 54-60, 2010.
- [12] D. Kundur, D. Hatzinakos, "Toward robust logo watermarking using multi-resolution image fusion," IEEE Transactions on Multimedia, vol. 6, no.1, pp. 185-197, 2004.
- [13] H. M. Al-Otum, N. A. Samara, "A robust blind color image watermarking based on wavelet-tree bit host difference selection," Signal Processing, vol. 90, no. 8, pp. 2498-2512, 2010.
- [14] Z. F. He, and Y. H. Zhang, "Fusion on the wavelet coefficients scale-related for double encryption holographic halftone watermark hidden technology," IEICE Transaction on Information and system, vol. E98-D, pp. 1391-1395, 2015.
- [15] A. A. Mohammad, A. Alhaj, S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership," Signal Processing vol. 88, no. 9, pp. 2158-2180, 2008.
- [16] C. C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," Optics Communications, vol. 284, no. 4, pp. 938-944, 2011.
- [17] N. Mohananthini and G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms," Journal of Electrical Systems and Information Technology, vol. 3, no. 1, pp. 68-80, 2016.
- [18] X. Zhou, C. Cao, J. Ma, and L. Wang, "Adaptive Digital Watermarking Scheme Based on Support Vector Machines and Optimized Genetic Algorithm," Hindawi Mathematical Problems in Engineering, Volume 2018, Article ID 2685739, 9 pages.
- [19] B. Ramirez, and S. L. Gomez-Coronel "A Perceptive Approach to Digital Image Watermarking Using a Brightness Model and the Hermite Transform," Hindawi Mathematical Problems in Engineering, Volume 2018, Article ID 5463632, 19 pages.
- [20] I. A. Ansari, M. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," Engineering Applications of Artificial Intelligence, vol. 49, pp. 114-125, March 2016.
- [21] D. Singh, and S. K. Singh, " DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection," Multimedia Tools and Applications, vol. 76, pp. 13001-13024, 2017.
- [22] X. Zhou, H. Zhang, and C. Wang, "A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD," Symmetry, vol. 10, pp. 77, March 2018
- [23] S. Sinha, P. Bardhan, S. Pramanick, A. Jagatramka, D. K. Kole, and A. Chakraborty, "Digital Video Watermarking using Discrete Wavelet

- [24] Transform and Principal Component Analysis," International Journal of Wisdom Based Computing, Vol. 1, no. 2, pp. 7-12, August 2011.
- [25] B. Kumar, H. V. Singh, S. P. Singh, A. Mohan, "Secure Spread-Spectrum Watermarking for Telemedicine Applications," Journal of Information Security, vol. 2, pp. 91-98, 2011.
- [26] H. Olkkonen, "Discrete wavelet transforms algorithms and applications," InTech, August 2011.
- [27] V. S. Jabade, and S. R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques," International Journal of Computer Applications, Vol. 31, no. 1, October 2011.
- [28] A. Z. Averbuch, and V. A. Zheludev, "Construction of Biorthogonal Discrete Wavelet Transforms Using Interpolatory Splines," Applied and Computational Harmonic Analysis, vol. 12, pp. 25-56, 2002.
- [29] Z. Yujin, "Image Processing and Analysis," Tsinghua University Press, Beijing, 1998.
- [30] G. Strang, "The Discrete Cosine Transform" SIAM Review, Vol. 41, no. 1, pp.135-147, 1999.
- [31] K. R. Roa and P. Yip, "Discrete Cosine Transform: Algorithms, Advantages, Applications ," Academic Press, Boston, 1990.
- [32] K. Baker, "Singular Value Decomposition Tutorial," March 29, 2005.
- [33] I. T. Jolliffe, and J. Cadima, "Principal component analysis: a review and recent developments," Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, vol. 374, 2016.