2018 International Conference on Communication, Information & Computing Technology (ICCICT), Feb. 2-3, Mumbai, India

Comparison of Key Transform Domain Watermarking Methods Based on Performance Measures

Swapnil D. Daphal*, Prashant K. Aher*, Shailesh B. Galande† and Sonal K. Jagtap‡
*Department of E&TC Engineering
MIT Academy of Engineering, Alandi, Pune
Email:sddaphal@entc.mitaoe.ac.in, pkaher@entc.mitaoe.ac.in
†Department of Computer Engineering,
PGM College of Engineering, Wagholi, Pune
Email:sgalande11@gmail.com
‡Department of E&TC Engineering
Smt. Kashibai Navale College of Engineering, Vadgaon Bk., Pune
Email:skjagtap.skncoe@sinhgad.edu.in

***Abstract*—Robust digital image watermarking (DIW) scheme is need of the prevailing digital technology. In this paper, the implementation details and methodologies of major transform domain algorithms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) are compared based on peak signal to noise ratio (PSNR) and normalized correlation(NC). The impact of different attacks on these methods is evaluated. Experimental results shows that DWT is more resilient to all attacks in terms of NC values. However, the SVD shows superiority in terms of PSNR in all adverse condition except the geometrical attacks. DCT gives high quality watermarked image with geometrical attacks but with poor quality of extracted watermark. Efficacy of the DIW system can be improved by taking different combination of these algorithms and their variants.**

Keywords-Digital image watermarking; Peak signal to noise ratio; Normalized Correlation;

I. Introduction

A. Digital Image Watermarking

With advent in technology, digital media is becoming the key component of security. Authenticity is the key concern involved in the transport and navigation of data. Copyrighted digital media is the need of todays era. Digital image watermarking is strong solution to illegal distribution of the digital images. In this paper, in order to maintain the ownership of digital images different approaches of the digital image watermarking has been compared. However, watermark can be ruptured and digital signature can be totally destroyed by incorporating noise. Also in this paper, the focus has been given to illustrate the compatibility of the algorithm to withstand various common noises. Any robust watermarking scheme involves mainly three components,

1) Cover Signal
2) The watermark signal
3) Robust Watermark embedding algorithm

Robustness of the watermarking scheme is solely dependent on the algorithm used for the embedding.The method by which the secret data or information is kept into various multimedia data is referred as digital image watermarking. The digital signature included in the data is sometimes visible and invisible in certain instances. In DIW, watermark image is kept in the cover image in such a way that the no any attack could degrade the signature image kept in the procedure. The block schematic for the digital image watermarking is given in the figure 1.

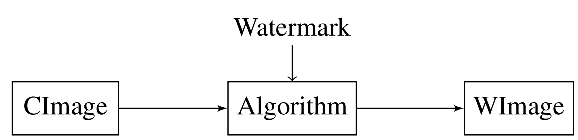

Fig. 1. Watermark embedding

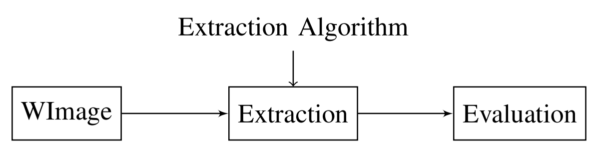

Fig. 2. Watermark extraction

- **Embed the watermark**
Cover Image of suitable dimension is selected irrespective of the statistical consideration. The watermark image is selected as the digital signature for the process. Using suitable embedding algorithm the watermark image is embedded into the cover image. Watermark may be visible or invisible depending upon the selection of algorithm. Watermarked image is transmitted over the network.

- **Attack the Watermarked Image**
  In order to destroy the authenticity of the watermark image the noise is added intentionally by the unwanted user. This may involve overloading the image with various types of attacks like Gaussian noise, rotation, scaling etc.
- **Extraction**
  The digital signature included in the first stage is extracted in this stage. The extracted watermark is compared with original image to check the efficiency of the algorithm. Figure 2 shows the extraction of the watermark.

B. Related Work

Since origin, this field has immensely seen different algorithms and methods. These methods have been are strongly criticized by different researcher and improvements were given on regular intervals. In [1] the research conducted on image forensics was put before the world, the issues and the solutions were given to improve the scenario in watermarking aspect.It triggered the need to look to upon the major digital watermarking method.Image independent digital watermarking method in frequency domain was proposed in [2] [3]. The feasibility of the method was validated through objective analysis. Similarly, attempts were made to overcome the shortcomings of the existing methods and blind watermarking algorithm in color space was given in [4]. Robustness of the algorithm was validated by using different noisy conditions and attacks. The watermark capacity was tested for video by applying blind watermarking algorithm on MPEG-2 in [5] [6]. This algorithm was mainly based on DCT and it was found that the with respect to previous methods it has shown the improved performance. Apart from this watermarking scheme for multiple cover images and multiple owners was proposed and it was validated that method is more robust, perfect imperceptibility and satisfies the blindness and security properties. The suitability of the DWT algorithm was given in [7] but no comments were made on the robustness of the system to extract the watermark. DWT-SVD combined watermarking method was discussed in [8]. Multi resolution capability of the wavelet with singular value decomposition was explored to make the system robust [9]. Innovative techniques to make use of properties of DWT in the watermarking was proposed in [10] [11] [12].The trend came to suggest the algorithms which can produce the adaptive watermarks and results shown that these algorithms are more robust and can be easily employed by changing the statistical parameters of the images [13] [14] [15]. In [16] Fan transform as a new scrambling method was suggested for color images. Again in [17] robustness of the DWT method was explored by testing the images against different attacks specially compression. Application specific strategies were made to address the exact issues related to the performance in [18]. Improvement in the performance were noted by using special technique like particle swam optimization in [19]. Recently,combination of fractal encoding method and DCT for double security and encryption was suggested in [20]. It was evident that if properly tuned, the use of new techniques and methods can give superior performance than classical methods.

Digital Image Watermarking is the method by which the authorized user includes signature by various means. Recent studies have given ample insight into the field of watermarking. Amid all the state of the art techniques, spatial domain t and transform domain are two major section under which all the algorithms are kept. Spatial domain techniques allow direct interaction with pixel values and are easy to access. However, watermark embedded in this manner is easy to destroy. Transform domain techniques are said to be more secure and less prone to the attacks. There are certain variants of the transform domain techniques like singular value decomposition which is more suitable for the clean environment.

C. Spatial Domain

This section gives the overview of spatial domain techniques. The feature associated with it are as follows:

1) Direct interaction with pixel
2) Original signal stays in the same domain during the processing
3) The watermark signal is statistically independent of the cover signal
4) Algorithms are strictly restricted to the pixel processing

Less complexity and simplicity in implementation are the advantages which are counted for pixel domain operation. In the applications which demand less delay and good response spatial domain algorithm are always preferred over the other domain algorithm. However, there are some demerits while using the spatial domain methods. It needs absolute spatial synchronization which may lead to high susceptibility to the attacks caused by the absence of synchronization; Neglecting the time domain behavior may image processing and optimization of the watermark more susceptible to the various performance degrading issues.

D. Transform Domain

Since 1998, the advancement in the area of digital image watermarking has given origin to the different advanced algorithms. In transform domain, the watermark is embedded evenly in overall range of the carrier signal unlike the spatial domain approach. It makes impossible to destroy the identity of the watermark from the carrier image once it is embedded. In this approach, depending on the kernels transforms are classified mainly as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). In DCT, watermarking is achieved in hierarchical levels. Transform domain techniques makes use of property of alternate domains to overcome spatial domain limitations. In DFT, the watermark information is mainly carried in phase of carrier signal. Singular value decomposition gives the best low rank representation guaranteeing that the most of the details are preserved and neglecting extra values which are least important. In this paper, comparative statement regarding performances and implementation of these different transform has given, to assist the beginners in this field.

978-1-5386-2051-9/18/$31.00 ©2018 IEEE

E. Performance Affecting Factors

Watermarking algorithms perform well in ideal conditions. The ability of any algorithm to reproduce the watermark should be as high as possible. To secure high reliability of watermark detection the process must be invariant to the alterations imposed from both intentional and unintentional distortions. These distortions, are the staple reason for the degradation of performance of system. Following are major contributors to the distortions involved in the process.

1) Noise added during the process: Any random signal with given statistical distribution is inserted into the watermarked image, aiming to destroy the watermark identity. In some cases, noise gets introduced during the natural phenomenon of transmission, conversion etc. Attacker may worsen the performance of the system by varying the statistical parameter of the process.

2) Filtering methods: Filtering does not imply to the degradation of the watermarked image, but affect the performance of the system significantly. In order to design a system which is resilient to filtering attack, the trade off must be maintained while selecting the watermark and the filtering operation.

3) Compression: This is generally a unintentional attack introduced while distributing the images over the Internet or over the transmission medium. The significant amount of compression may mislead to the detection of the watermark in the image.

4) Geometrical Attacks: Geometrical attacks do not eliminate the watermark by itself, but to distort it through spatial modifications of the water- marked image. With such attacks, watermarking extraction algorithm loses the synchronization with embedded data. These attacks are further classified into attacks associated with affine transformations and relevant projective transformation. These attacks are mainly are rotation, scaling, change of aspect ratio, translation and shearing.

5) Cropping: This is a general attack since in many cases the intruder is interested in a tiny portion of the watermarked object, such as parts of a certain picture or frames of video sequence. With this in mind, in order to survive, the watermark needs to be spread over the overall length of the image or video portion where this attack takes place.

F. Performance Measures

1) Peak Signal to Noise Ratio: PSNR gives the information regarding quality of the watermarked image. It is evaluated between the original image and watermarked image. Higher the PSNR value higher is the quality of the watermarked image.

$$\text{PSNR} = -10\,\log_{10}\frac{\text{MSE}}{N^2} \tag{1}$$

2) Signal to Noise Ratio: Signal-to-noise ratio estimates the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise. While SNR is commonly quoted for electrical signals, it can be applied to any form of signal.

$$\text{SNR} = \frac{\sum_{x=1}^{P}\sum_{y=1}^{Q}[\,\hat{g}(x,y)\,]^2}{\sum_{x=1}^{P}\sum_{y=1}^{Q}[\,\hat{g}(x,y)-g(x,y)\,]^2} \tag{2}$$

3) Normalized Correlation: This is the parameter to identify the robustness of the watermarking algorithm.

$$\text{NC} = \frac{1}{N_w}\sum_{j=0}^{N_w-1} w(j)\,w'(j) \tag{3}$$

Here, N_w is the size of the watermark in terms of pixel length. $w(j)$ and $w'(j)$ are the jth watermark bit in the original watermark and the extracted watermark, respectively.

This paper is organized as follows. Section II gives overview the transform domain methods. Experimental results and discussions are given in Section III. The conclusion is stated in section IV.

II. Methodology

Different algorithms are suggested for watermarking in transform domain. In this section major member from the transform domain are discussed with their implementation in brief.

A. Discrete Cosine Transform

Let P be a original gray level image of size $M \times N$. $P4$ will be acting as a carrier image.

$$P = \{\ p(m,n),\ 0 \le m < M,\ 0 \le n < N\ \} \tag{4}$$

where $p(m,n)\ \epsilon\ \{0,1,2,...,(2^L-1)\}$ is the intensity of pixel $p(m,n)$ and L is the number of bits used in each pixel. Before applying the DCT, carrier image is divided into (8×8) blocks. The image P is segmented into $\left(\frac{M}{8}\times\frac{N}{8}\right)$ blocks.

$$P_b = \left\{P_b(k,l),\ 0 \le k < \frac{M}{8},\ 0 \le l < \frac{N}{8}\right\} \tag{5}$$

where the original image block is expressed as,

$$P_b(k,l) = \left\{P_b(k\times8+m, l\times8+n),\ 0\le k<\tfrac{M}{8},\ 0\le l<\tfrac{N}{8}\right\} \tag{6}$$

$$P_b(k,l) = \left\{p(k\times8+m, l\times8+n),\ 0\le m<8, 0\le n<8\right\} \tag{7}$$

High compression ratio, high computational complexity and low error rate are the characteristics of the DCT.

$$(\mathbf{P}_b)_{u,v} = \frac{C(u)}{\sqrt{\frac{N}{2}}}\frac{C(v)}{\sqrt{\frac{N}{2}}}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(\mathbf{p}_b)_{i,j} \cos\frac{(2i+1)u\pi}{2N}\cos\frac{(2j+1)v\pi}{2N} \tag{8}$$

where,

$$C(u) = \begin{cases}\frac{1}{\sqrt{2}}, & \text{for u=0}\\ 1, & \text{otherwise}\end{cases}$$

The coefficients are mostly zero after applying the DCT. Generally lower frequency and higher frequency comes with high and lower values in the image, respectively. It is preferable to embed watermark into image parts with middle and lower frequency.

B. Discrete Wavelet Transform

Discrete wavelet transform is a transform with multi resolution analysis feature. In terms of numerical and functional analysis DWT is wavelet transform where wavelets are sampled at the intervals set by some predefined rules. The temporal resolution is key parameter which makes DWT more superior to Fourier Transform. It combines both frequency and position details of the signal. Segregation of signal depending upon the frequency details is the key theme behind the DWT. Each stage of wavelet decomposition has four subimages with equal size. Here, LL_x stands for the approximation subimage, and LH_x, HL_x and HH_x refers to the horizontal, vertical and diagonal direction high frequency details of subimages, respectively. Here, $x = 1, 2, 3, ...(x \epsilon N)$, is the level of the wavelet decomposition, is illustrated in figure 3.

Higher frequency subimages are more susceptible to attacks

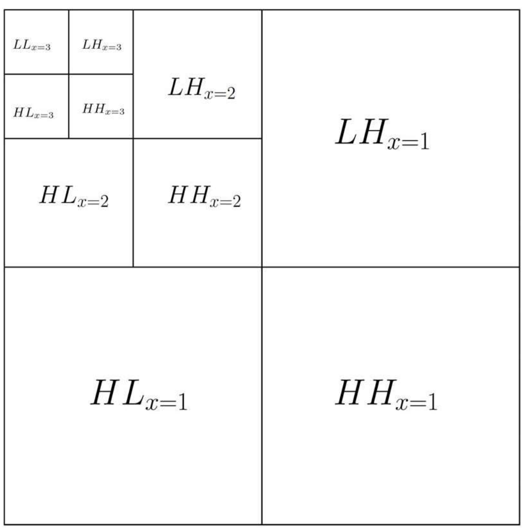

Fig. 3. DWT Decomposition

and contents are more prone to vary with respect to response of various data transmission schemes, hence information hidden these region may get lost easily.

C. Singular Value Decomposition

Let a digital image A is considered as array of non negative scalars that may be considered as $M \times N$ matrix X given below,

$$X = \{x_{i,j}\}_{N \times N}$$

Any matrix M of size $N \times N$ can be represented by its singular value decomposition in the form as follows,

$$\begin{aligned} X &= U S V^T \\ &= [u_1, u_2, u_3, ..., u_N] \times S \times [v_1, v_2, v_3, ..., v_N]^T \end{aligned} \quad (9)$$

where,

$$S = \begin{pmatrix} \sigma_1 & & & \\ & \sigma_2 & & \\ & & ... & \\ & & & \sigma_2 \end{pmatrix}$$

U and V are $N \times N$ real unitary matrices with column vector u_i and v_i, respectively. S is the $N \times N$ diagonal matrix with σ_i (singular values) satisfying,

$$\sigma_1 \geq \sigma_2 \geq \sigma_3 \geq ...\sigma_r \geq \sigma_{r+1} \geq = ... = \sigma_N = 0 \quad (10)$$

The singular values comes with good stability. It ensures even small variations to the image will not significantly change the corresponding singular values. SVD can efficiently represent the statistical properties of the image. Brightness and geometry characteristics of the image are well represented by singular values and singular vectors of the SVD. An image may have small singular values with respect to the first singular values. While reconstructing the image of these small values are being ignored that does not affect the quality of the image to the larger extent.

Fig. 4. Cover image: Pepper

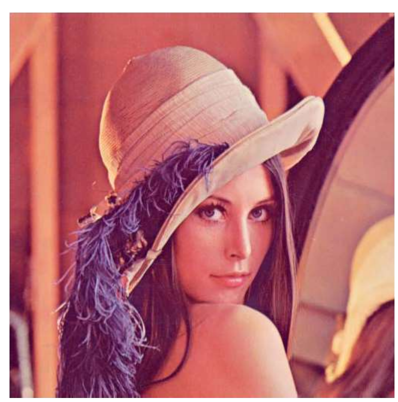

Fig. 5. Cover image: Lena

III. Results and Discussions

During the experimentation, different standard images like Pepper, Lena and Baboon are taken which has different

TABLE I
PERFORMANCE EVALUATION: WITH PEPPER AS A COVER IMAGE

Sr. No	Attacks	DCT		DWT		SVD	
		PSNR	NC	PSNR	NC	PSNR	NC
1	No Noise	40.4361	**1**	38.4806	**1**	**52.3218**	0.9797
2	Gaussian Noise ($\sigma_v = 0.01$)	19.1659	0.8413	20.1035	**0.9944**	**20.1482**	0.0502
3	Gaussian Noise ($\sigma_v = 2$)	5.5204	0.3916	6.4864	**0.9125**	**6.5136**	-0.0803
4	Salt and Pepper	21.1722	0.9051	22.2055	**0.9966**	**22.2288**	0.0697
5	Rotation (30)	6.5933	0.2588	**6.7451**	**0.9998**	6.5593	0.1722

TABLE II
PERFORMANCE EVALUATION: WITH LENA AS A COVER IMAGE

Sr. No	Attacks	DCT		DWT		SVD	
		PSNR	NC	PSNR	NC	PSNR	NC
1	No Noise	41.0595	**1**	41.211	**1**	**52.6447**	0.9745
2	Gaussian Noise ($\sigma_v = 0.01$)	19.6872	0.8594	20.0209	**0.9941**	**20.0375**	0.0583
3	Gaussian Noise ($\sigma_v = 2$)	6.2415	0.4079	6.5698	**0.9133**	**6.5917**	-0.0592
4	Salt and Pepper	22.0153	0.9214	22.4700	**0.9968**	**22.604**	0.0894
5	Rotation (30)	**7.6070**	0.2509	7.3193	**0.9998**	7.2859	0.2067

intensity distribution(Image size, 512×512, 8 bit, color). Coin image(Image size, 300×246 (Later resized suitably), 8 bit, gray scale) is taken as watermark image and selected for the embedding purpose.

Embedding is done with different algorithms mainly DCT, DWT and SVD. The watermarked image is passed through extraction phase wherein the watermark image is extracted from it. Extracted watermark is then compared with original watermark to evaluate the performance of different algorithm. The quality of the watermarked image is compared with original image using PSNR. Table I, table II, table III shows comparative analysis with cover image Pepper, Lena and Baboon for the discussed methods under different attacks, respectively.

Under clean environment the NC values of DCT and DWT are almost same while DWT is showing bit improvement in terms of PSNR. After juxtaposing these method against the SVD, it gives the highest PSNR with slight degradation in the NC. Under the influence of Gaussian noise with variable variance SVD shows the worst performance in terms of NC still keeping the highest PSNR. However, DWT shows the appropriate results even in noisy conditions. It is also worth to note that, there is slight variation in the performance measures with respect to the cover image selected for the watermarking purpose.

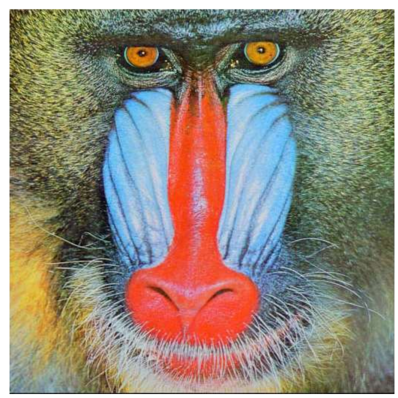

Fig. 6. Cover image: Baboon

Fig. 7. Watermark image: Coins

TABLE III
PERFORMANCE EVALUATION: WITH BABOON AS A COVER IMAGE

Sr. No	Attacks	DCT		DWT		SVD	
		PSNR	NC	PSNR	NC	PSNR	NC
1	No Noise	40.5484	0.9917	30.9415	**1**	**51.6179**	0.9790
2	Gaussian Noise ($\sigma_v = 0.01$)	19.1335	0.8021	19.7349	**0.9941**	**20.0050**	0.0623
3	Gaussian Noise ($\sigma_v = 2$)	5.7836	0.4379	6.6320	**0.9131**	**6.6932**	-0.0565
4	Salt and Pepper	21.5657	0.8747	21.9863	**0.9967**	**22.4948**	0.1009
5	Rotation (30)	**7.1386**	0.2285	6.9523	**0.9993**	6.5235	0.2230

IV. CONCLUSION

The paper presents the comparison of major transform domain watermarking methods like DCT, DWT and SVD in both clean and noisy environment. It has been found that for clean environment SVD shows the highest watermark quality with slight compromise in watermark restoration process. However, DCT and DWT give optimal results in terms of NC with slight degradation in the PSNR. Under the influence of geometrical attack the watermarked image quality is higher with DCT However NC value is found to be higher with DWT. In terms of watermark extraction DWT performs well in all conditions making it more robust against attacks. The nature of cover image also plays a partial role in assessing the performance of the method. In order to improve the performance of the watermarking method combination of any of these methods can preferred.

REFERENCES

[1] Z. Guojuan and L. Dianji, "An overview of digital watermarking in image forensics," in *International Joint Conference on Computational Sciences and Optimization*, 2011.

[2] Q. Wang and S. Sun, "DCT-based image independent digital watermarking," in *Proceedings of ICSP2000*. IEEE, 2000, pp. 942–945.

[3] M. Shen, W. Xu, S. Wang, and P. J. Beadle, "Application of independent component analysis to detection of digital image watermarking," in *Signal Processing, 2004. Proceedings. ICSP '04. 2004 7th International Conference on*, vol. 3, Aug 2004, pp. 2596–2599 vol.3.

[4] X. Bin, "A blind watermarking algorithm based on color space conversion in DCT domain." IEEE, 2011.

[5] L. Jianfeng, Y. Zhenhua, Y. Fan, and L. li, "A MPEG2 video watermarking algorithm based on DCT domain," in *Woekshop on Digital Media and Digital Content Management*. IEEE, 2011, pp. 194–197.

[6] W. Weina, "Digital audio blind watermarking algorithm based on audio characteristic and scrambling encryption," in *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, March 2017, pp. 1195–1199.

[7] R. Dubolia, R. Singh, S. singh, and R. Gupta, "Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based onPSNR," in *International Conference on Communication System and Network Technologies*. IEEE, 2011, pp. 593–596.

[8] K. Bhagyashri, "All frequency band DWT-SVD robust watermarking technique for color images in YUV color space." IEEE, 2011, pp. 295–299.

[9] S. B. Ftima, M. Talbi, and T. Ezzedine, "Lwt-svd secure image watermarking technique," in *2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)*, vol. 1, April 2017, pp. 510–517.

[10] M. Manoochechri, H. Pourghassem, and G. Shahgholian, "A novel synthetic image watermarking algorithm based on discrete wavelet transform and fourier mellin transform." IEEE, 2011, pp. 265–269.

[11] M. E. Hajji, H. Douzi, D. Mammass, and R. Harba, "A robust wavelet based watermarking algorithm using mixed scales." IEEE, 2010.

[12] S. S. Gonge, V. M. Thakare, A. A. Ghatol, and S. A. Ladhake, "Combined dwt image watermarking and aes technique for digital 2-d image," in *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Dec 2016, pp. 1–10.

[13] L. Chunhua and F. Li, "Adaptive image watermarking algorithm based on biorthogonal wavelet transform." IEEE, 2011.

[14] Y. Chang-hui, F. Wan-li, and Z. Hong, "The digital watermarking technology based on neural network." IEEE, 2011.

[15] H. Xu and C. Shujuan, "An adaptive image watermarking algorithm based on neural network," in *International Conference on Intelligent Computation Technology and Automation*. IEEE, 2011, pp. 408–411.

[16] W. Li and J. Fan, "Double scramb about color image based on Fan transform." IEEE, 2011, pp. 3931–3934.

[17] S. H. Seyedi, A. S, Hassan, and Ali, "A blind image adaptive data hiding method in wavelet domain with robustness against compression." IEEE, 2011, pp. 345–349.

[18] L. Zhai and Q. hu, "Researches on digital image watermarking algorithm in DWT domain with chaotic encryption." IEEE, 2011, pp. 3321–3324.

[19] Y.-R. Wang, W.-H. Lin, and L. Yang, "A blind PSO watermarking using wavelet trees quantization," in *International Conference on Machine Learning and Cybernetics*. Gulin: IEEE, July 2011, pp. 1612–1616.

[20] S. Liu, Z. Pan, and H. Song, "Digital image watermarking method based on DCT and fractal encoding," *IET Image Processing*, vol. 11, no. 10, pp. 815–821, 2017.