

A Robust Digital Image Watermarking Methodology using an Ensemble-Based Classifier for Mitigation of Geometrical Attacks

Rakesh Kumar Verma¹, Dr. Shiv Kumar², Dr. Varsha Namdeo³

¹Department of Computer Science & Engg, Sarvepalli Radhakrishnan University, Bhopal, India.

rakeshvermabplsrk@gmail.com

²Department of Computer Science & Engg, Sarvepalli Radhakrishnan University, Bhopal, India.

sivakum.slm09@gmail.com

³Department of Computer Science & Engg, Sarvepalli Radhakrishnan University, Bhopal, India.

varsha_namdeo@yahoo.com

Article Info

Page Number: 4480 – 4496

Publication Issue:

Vol 71 No. 4 (2022)

Abstract

Digital watermarking is an effective approach to the problem of copyright protection, thus maintaining the security of digital products on the network. Recently, several machine learning based digital watermarking algorithms have been proposed. The major factors of the watermark image are sustainability and imperceptibility against geometrical attacks. The digital content was deformed by the processing of geometrical attacks such as cropping, sharing, and translation. The process of authentication of digital content is compromised in terms of quality and security. This paper proposed a machine learning-based ensemble classifier for the optimization of embedding coefficient. The optimized embedding coefficient increases the strength of robustness factors. The process of optimization focuses on two elementary parameters: correlation coefficient and PSNR value. The minimum value of the correlation coefficient of pixel value increases the compactness of the watermark image and the source image. The primary phase of the optimization-based watermarking algorithm is feature extraction. This paper applies discrete wavelet transform methods for feature extraction. The discrete wavelet transform is a rich texture feature component of raw images. The lower content of noise is optimized by machine learning

Article History**Article Received:** 25 March 2022**Revised:** 30 April 2022**Accepted:** 15 June 2022**Publication:** 19 August 2022

algorithms. The proposed algorithm is simulated in MATLAB tools. For the validation of algorithms, we applied various standard watermarking images and estimated CC and PSNR. The experimental results outperform the existing methods of watermarking.

Keywords: - Watermarking, Robust, Ensemble Classifier, Optimization PSNR, Geometrical Attack.

Introduction

The rapid growth of information technology and easy accessibility needs the concept of data hiding and security. The security of multimedia data has various approach such as steganography, encryption and digital watermarking [1, 2, 3]. The contribution of digital watermarking is very high concerning other methods of digital data security and copyright protection [4]. The process of digital watermarking methods proceeds in two different ways, such as spatial domain and frequency-based methods of digital image watermarking [5, 6]. The spatial based watermarking methods operate the shifting of pixel to the left to right and vice-versa. The very famous algorithm of the spatial domain is LSB and RSB [7, 8]. The strength of these watermarking methods is weak and easily compromised with the geometrical attack. Despite the spatial image digital watermarking algorithm, the transform-based watermarking methods are very efficient and more secured [9, 10, 11]. The multiple derivatives of transform are applied for the processing of digital image watermarking. The major contribution of wavelet transforms, the wavelet transform has multiple variants that change the characteristics of digital image watermarking [12, 13, 14]: the concept of multi-layer decomposition of transform in the form of high frequency and low frequency [15]. The processing of low-frequency watermark embedding moves to the next level of security. The transform DWT and WPT have certain bottleneck issue, such as translation invariance is not supported by DWT [16]. It also faces a problem of the input image's dyadic size and many other issues such as impulsive noise. These limitations overcome with stationary wavelet transform (SWT)[17], also called redundant transform. The application of transform in digital image watermarking direct embedding process and feature-based watermarking. Recently various authors and research scholar reported the feature-based watermarking algorithm is efficient instead of the direct embedding of transform. The optimization of watermarking process enhances the security strength of watermarking process. For the process of optimization using ensemble-based classifier. The ensemble-based classifier optimizes the feature components of transform [12]. The process of

ensemble design based on decision tree and KNN. The decision tree classifier able to select feature of component for the processing of embedding of image. The ensemble classifier model $M=2$. The mode of ensemble or level of classifier derived the process of watermarking. The proposed algorithm increases the value of PSNR (Peak to signal ratio) and symmetry of watermark image. The proposed algorithm applied on different set of watermark image and verify the strength of watermarking algorithm. The strength of watermarking algorithm deformed the possibility of geometrical attacks. The various geometrical attack intercepts the watermark information and find the position of watermark [15]. The geometrical attack changes the location of coordinate system of watermark image and estimate the embedding position of watermark image. The rest of paper organized in section II. Describe the related work. In section III. Describe the process of proposed methodology. In section IV experimental result analysis and finally conclude in section V.

II. Related Work

In this [1] researchers discussed the Discrete Cosine Transform domain, an image watermarking approach is designed to give sufficient robustness towards common watermarking attacks. Then, using the Artificial Bee Colony algorithm, an instructional procedure is carried out by picking a group of photos wherein the watermarking is implemented and optimized. The ideal strength values, as well as the features are extracted that comprise the training images, are gathered as observation data. The optimal power flow fitness function is calculated at distinct characteristics of the embedding toughness to extract the features from an image. Eventually, through using optimum embedding parameters indicated by the K-Nearest Neighborhood regression technique, a fresh batch of photos is picked to be watermarked. In this [2] researchers discussed a virtual watermarking algorithm which is based on the DCT and fractal encoding. To enhance the classic DCT method, the presented method combines nonlinear encoding and DCT for double encryptions. As the first decryption, the image is encoded using fractal encoding, as well as the encrypted characteristics are then employed in the DCT technique as the subsequent encrypted communications. To begin, a personal image with personal scales is encoded using the cyclic embedding method. Digital watermarking is used to apply encoding settings. The researchers then add electronic copyrighting to the s their image in order to reversibly use DCT, allowing them to retrieve the personal image from of the carrier image using proprietary encoding scales. Furthermore, assaulting experiments on the carrier picture are carried out utilizing a variety of attacking strategies. In this [3] authors discussed about a new scan-chain oriented watermarking technology for hard IP core that can be

used as an independent copyright protection method During the process of scan chain ordering for test power optimization, the steganography bits constrain the cost of one connection style over the other for certain pairings of scan cells in the optimization process, which is entirely dependent on the output of the IP core underneath the chosen test vector for watermark verification. Because both connection options are present at the watermarked locations, the watermark is more concealed. Along with these scenarios, the test results show that comprehensive authentication may be achieved with low test power overhauled. In this [4] researchers discussed the topic of identifying attacks in a homogenous number of co system is described. The agents' sharing information is governed by network architecture, so each robot is managed to achieve both locally and globally goals. Each agent has its own local estimator and anomaly detector. Researchers discussed requirements on the integrity of the under-attack system in the case of a replay attack to a segment of the system, where the attack cannot be noticed by any of the agents. Following that, a detecting approach based on using a watermark information control strategy is given, wherein the watermarking signal is disseminated among the agents via the network. In this [5] researchers discussed the least significant bit (LSB) was employed to introduce a watermark again for input image by the investigators. Because only LSB-based approaches are insufficient in an attack-free context and lossy and lossless, they really aren't sufficient. To indicate the existence of confidential material and retrieve data from s their image, the scientists deployed a Synthetic Applications Neural Network (ANN). When a machine learning technique is learned, trained up, and applied to a few novel apps, it is intrinsically unstable. There'd be a unique identifier inside the usual solution because there are comparatively straightforward ways to alter the neural network architecture so that it achieves the very same function as before and with a different overall representation. In this [6] authors discussed the images are separated into 8 x 8-pixel non-overlapping chunks. For every image block, the variable pixel value was determined. The anchoring regions were chosen from image blocks with both the highest random value. As an outcome, discrete cosine transforms were used to transform it (DCT). The fingerprint bits were implanted using a set of anchoring rules with the various embedding intensities stated before. Before being inserted, the binary watermark was jumbled using an Arnold Transform for added protection. The test findings showed that the suggested system had a greater detection accuracy than the other current schemes. With a PSNR of 46 dB, the discussed scheme produced watermarked image quality. The suggested technique also resulted in a high level of watermark extraction resistance in the face of diverse attempts. In this [7] discussed the rapid advancement of memory technology and information interchange enc their ages

the advancement of information security technology. Tampering and data ownership concerns may emerge during the transfer of messages. One way for overcoming the difficulty is fragile watermarking, which takes use of sensitivity to tamper with the inserted watermark components. Once an image with a watermark has been edited by other users, it can be used to detect tampering and recover images. This report discusses the foundations and properties of a fragile watermarking algorithm attention to the significance of this fragile watermarking technique. The fundamental aspect of this research is that it summarizes existing mechanisms for selection, creation, watermark implantation, identification, and tamper sensing and step by step procedure. In this [8] Researchers present a unique blind picture watermarking methodology centered on a deep neural encoder-decoder network that can successfully learn attacking patterns. For more information, a discrete watermark image is concealed into selective wavelet blocks using the median of an ideal encoding strategy, in which the quality image deterioration is minimized over the Mean Square Error metric for a significant image imperceptibility improvement. The embedding maps of numerous attacks simulated as digital image modifications of the watermarked image are then exposed for building the deep learning-based watermark extraction model, which are defined as the wavelet coefficient quality exchanges. As an outcome, the trained model could exactly retrieve the embedded watermark buried in an assaulted image from its own embedded map. [9] The chaotic function of the mentioned mapping is demonstrated that use the bifurcation diagram, Linearization coefficient, cobwebs graph, and trajectories schematic. The recommended map can also be used as pseudo-random random generator based on the DIEHARD, ENT, and NIST test automation. The simulations show that now the described watermarking technique is resistant to a wide range of image processing techniques, including salt and pepper, cropping, low-pass filter, wiener filter, blurring, and so on. The simulation outcomes between the discussed watermarking scheme and several similar approaches reveal that the discussed methodology beats most comparable techniques in terms of performance, encryption techniques, and resilience. In this [10] researchers discussed a revolutionary forgery detection method is mainly based on the supervised learning technique The support vector neural network is used to enable classification algorithm, while the fruit fly optimization technique is used to enable optimization. The photos are first given into the decision surface, and then the Viola–Jones method is used to detect the face. The Gaussian filtering With F their and texturing operator is often used to extract features from the face identified images, and the characteristics are concatenated to present the input to the classifier. The classification then classifications the features using the fruit fly optimizer to indicate the occurrence of the

manipulation. In this [11] researchers discussed the Heart sound processing in the Wavelet Coherence (WTC) methodology was presented. The WTC compares the spatial frequency correlation between two waveforms. The ECG signal is characterized by parameters taken from the WTC function. The Dragonfly algorithm is used to determine these properties (FFA). The Levenberg Marquardt Neural Network (LM NN) classifier receives the optimized features from the FFA as input. The performance of the classifier is increased with the help of optimized smaller features, according to the research. The baseline of the ECG may fluctuate, but the QRS curves are normally normal. In this [12] authors explained how to automate brightness equalization, equalization, and sound quality compression in order to minimize inter-channel aural masking and increase overall mix quality. To evaluate inter-channel auditory masking, researchers updated and enhanced the MPEG psychoacoustic model's masking threshold technique. Finally, using a numerical optimization technique, the researchers developed an intelligent system for masking minimization. Researchers investigated if their based on an improved approach might be used to create an automatic mix with less aural masking and higher the perceived clarity. In this [13] discussed the S-DWF is a secure digital watermarking framework that uses a 'image dithering' type of decomposition followed by a key-based watermarking technique, according to the proposed research. With the addition of various noise levels, the proposed S-DWF was implemented in a numerical computing platform and performance assessed. The analysis found that, when compared to the current baseline, the described S-DWF achieves greater information security in terms of Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER). In this [14] authors discussed a two-level DWT followed by FWHT is used to deconstruct the red channel of the host image. The non-overlapping chunks of the FWHT parameters are then partitioned. Then, using Heisenberg decomposition, each selected block is quantized to include the watermark information in the upper Heisenberg matrix H 's first row, first column element. The maximum signal-to-noise ratio, normalized cross-correlation, and structural similarity index measurement are used to assess feasibility and durability. In this [15] researchers derived MSE as well as the summation of performance of selected wavelet coefficients for image watermarking modification have a linear proportionality, and the link between MSE and the sum of performance of a specified wavelet coefficients for watermark embedding modification has been investigated. Discrete wavelet transformations are orthonormal, according to the first hypothesis. It is therefore improved for non-orthonormal wavelet kernels by using a weighting value based on the energy conservation theorems of wavelet frames. The aforementioned research is supported by simulation data for both non-blind

and blind watermarking methods. In this [16] discussed the poem examines and critiques a new verification secure conceptual model (CIA) standard in triplex cryptocurrency swarm optimization (PSO)-advanced encryption standard (AES) methodologies for patient proof of identity in health systems, revealing criticism and analysis of all attempts. There are three stages to discussion. To increase randomization, a novel hybrid model pattern based on radio frequency identification (RFID) and finger vein biometrics was first discussed. In order to accomplish this, researchers developed a new merging approach that blends RFID and finger vein features into a single hybrid and random device.

III. Proposed Methodology

The proposed methodology describes in two sections in first section describe the process of feature extraction based on wavelet transform and second section describe the process of ensemble based watermarking embedding.

The wavelet transform is derived from mother wavelet transform for the scaling of transform for the signal data decomposition. In process of wavelet transform get a finer low frequency resolution. Wavelet transform applied long time windows, in order to get high frequency data. the processing of wavelet transform is superior than FFT and STFT for texture feature extraction process[4,5,6].

Conder $f(x) \in L^2(R)$ relative to wavelet function $\psi(x)$ and scaling function $\phi(x)$

The DWT defined as

$$W_{\phi}(j0, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \phi_{j0,k}(x) \dots \dots \dots (1)$$

$$W_{\psi}(J, K) = \frac{2}{\sqrt{M}} \sum_x f(x) \psi_{j,k}(x) \dots \dots \dots (2)$$

Now

$$\begin{aligned} f(x) = & \frac{1}{M} \sum_K W_{\phi}(j0, k) \phi_{j0,k}(x) \\ & + \frac{1}{\sqrt{M}} \sum_{j=0}^{J-1} \sum_K W_{\psi}(j, K) \psi_{j,K}(x) \dots \dots \dots (3) \end{aligned}$$

In the value of M measure, the power of 2. The component of transform estimate M number of coefficients the maximum scale j-1 and minimum coefficient is 0, and detail coefficient define in equation 2.

The process of ensemble used the methods of boosting. In this method the main class of classifier is decision tree and variable classifier is KNN. The main classifier decides the classification predict of class based on KNN.

The decision tree classifier based on the entropy event of information. The classification predicts with the leaf node of tree. The branching of tree derived from the information gain; the value of maximum information gains the process of branch node converted into leaf node. The process of leaf node predicts the event of class. The building tree of algorithm based on ID3. Nearest neighbour classifiers are lazy classifier, but ability of this classifier based on similarity measure of nearest neighbour data points. The level of nearest based on the attribute value of class and measure the difference of class for non-overlapped data points[9,11,15].

The process of ensemble describes here

The naming of class $DT \leftarrow s$ and $KNN \leftarrow L$ the level of $M=2$

The mapping of sample feature of watermark image is $f(x)f(x) = D^R$ the represents the sample data and R measure the relation of data

$Dsample\{f1, f2, \dots, fn\};$

for $m \leftarrow 1$ *to* M *do*

$S \leftarrow l(f(x).f(x'));$

$em_class \leftarrow vote(S: x_{(:, :, m)}, L. y_{(:, :, m)});$

if $vote == True$ *or* $M == True$ *then*

$pridict \leftarrow class(S(f).L(f));$

$vote = vote + 1;$

return $pridict$

end

The process of watermark embedding

1. Select the area of watermark for embedding

The original image and symbol image pass through wavelet transform function and extract feature. The extracted features pass through ensemble classifier for optimization

2. Search the embedding position with factor level of ensemble M
3. After the training of source image data and symbol image data measure the pattern difference for the process of embedding
4. If the value of pattern difference $D \neq 0$
5. The process moves to training and final optimal location
6. Measure PSNR and NC
7. Terminate the process.

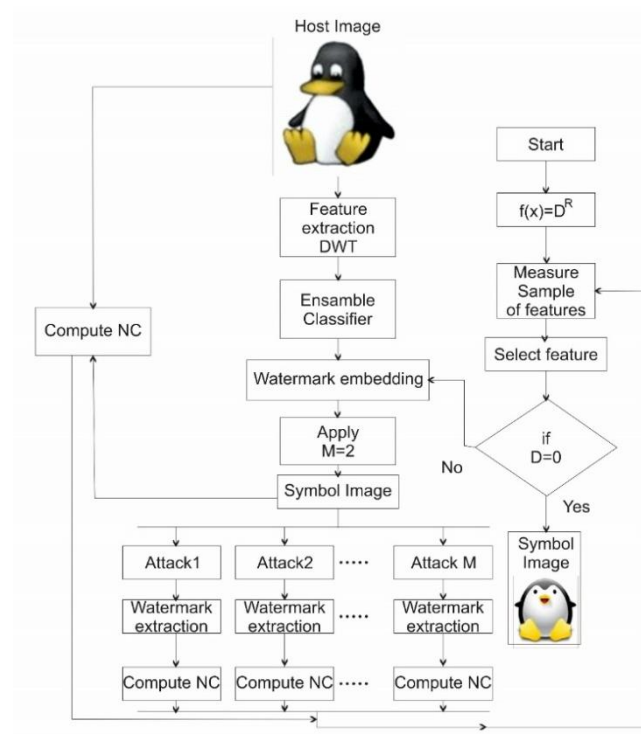


Fig. 1. Proposed model of ensemble based digital image watermarking model.

IV. Simulation Analysis

The proposed watermarking algorithm is tested on 300 color images of size (512 *512). The different class of images such as man, follower, peppers and other texture image. These images collected from CVG-UGR image dataset. All the analysis and experiment have been carried out in windows 10 based MATLAB 13. The hardware used for the simulation process is a Dell computer with intel core I7 processor and 8 GB Ram. For the evaluation of analysis used following formula as[19,20].

The value of RMSE indicates the error difference value of original image and final watermark image. The lower value of RMSE shows the good quality of watermark image and enhance the value of PSNR.

$$RMSE = \sqrt{\frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [O_{image}(i, j) - W_{image}(i, j)]^2} \dots\dots\dots(4)$$

where $m \times n$ is the size of the image, (i, j) is the pixel location, O_{image} is the original image, and W_{image} is the watermarked image. Then PSNR is defined as

$$PSNR = 20 \log_{10} \frac{\text{Max}(O_{image})}{RMSE} \dots\dots\dots(5)$$

The measure the value of robustness used this formula as

$$NC = \left(\frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W_o(i, j) - W_E(i, j)}{\sqrt{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W_o^2(i, j)} \times \sqrt{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W_E^2(i, j)}} \right) \dots\dots\dots(6)$$

where W_o is the original watermark and W_E is the extracted watermark. The time of encoding and Decoding measure by the MATLAB function TIC-TOC.

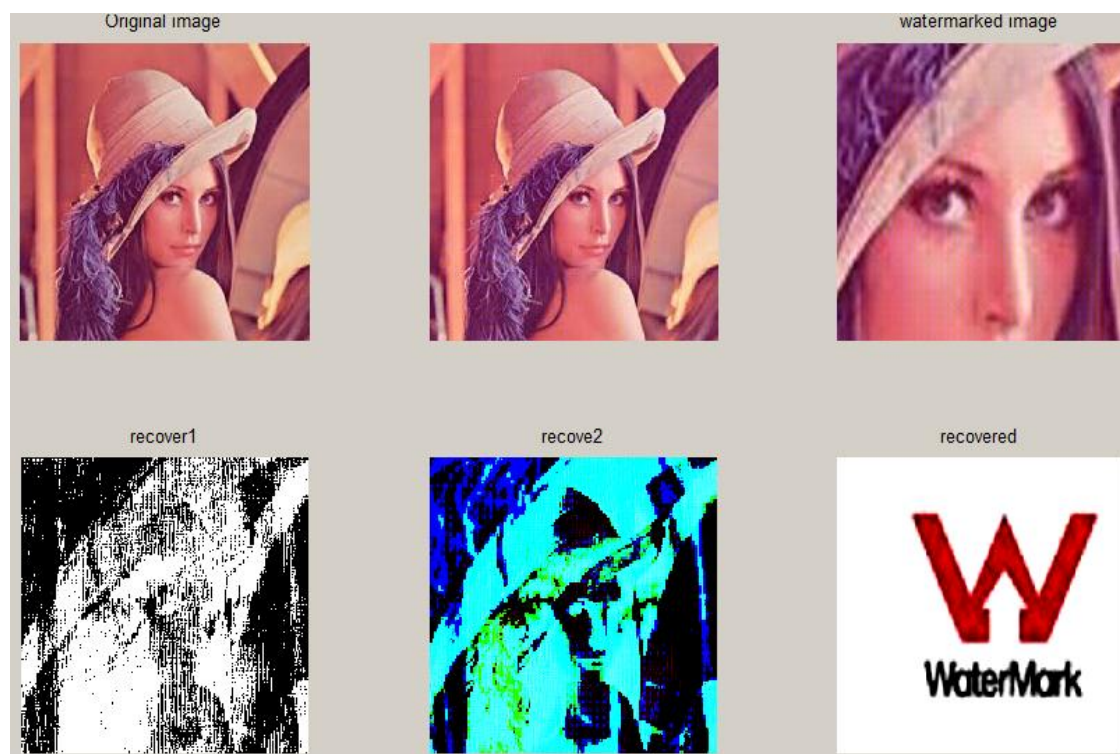


Fig. 2. Shows that the Lena image for Robust Digital image watermarking based on LWTML method on Cropping Attack.

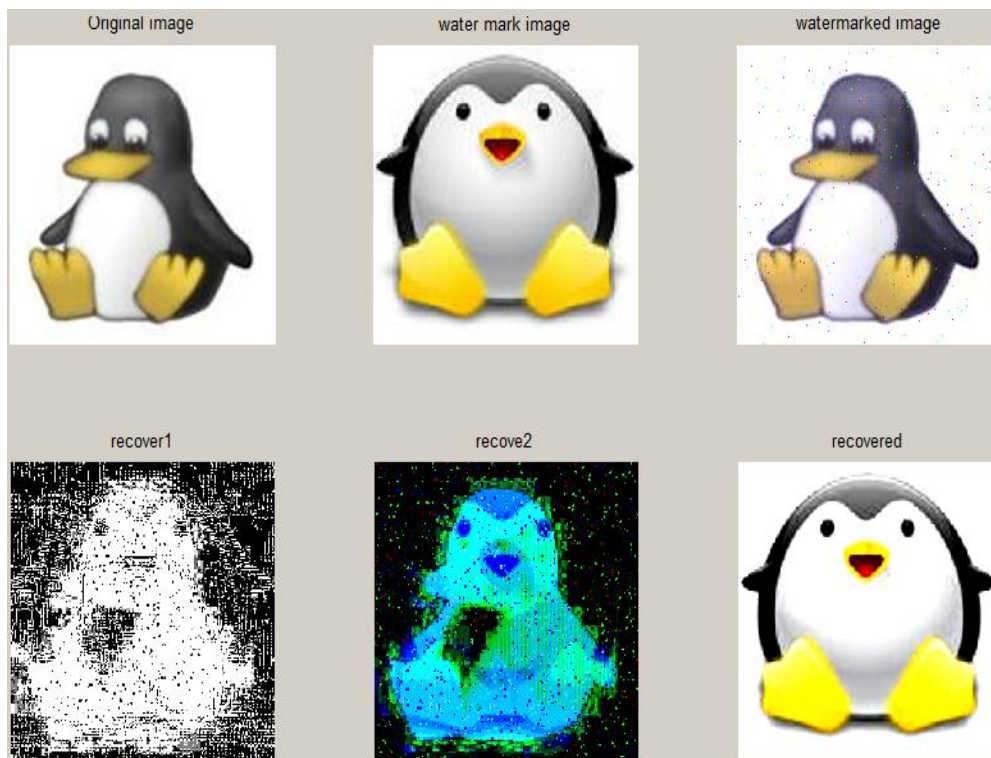


Fig. 3. Shows that the Penguin image for Robust Digital image watermarking based on Proposed method on Shear Attack.

TABLE I. SHOWS THE COMPARATIVE ANALYSIS OF DWT LWTML AND PROPOSED TECHNIQUES USING ATTACK RECOVERY TIME, PSNR AND NC THOSE PARAMETERS FOR LEENA IMAGE IN ROBUST DIGITAL IMAGE WATERMARKING.

Method	Types of Attack	Attack Recovery Time	PSNR	NC
DWT [6]	Cropping	11.4036	22.6285	0.5692
	Shear	8.0028	22.8389	0.1772
LWTML [15]	Cropping	10.3272	21.0920	0.5524
	Shear	6.9732	21.3860	0.1571
Proposed	Cropping	1.5444	25.0868	0.8308
	Shear	1.6380	24.8389	0.6108

TABLE II. SHOWS THE COMPARATIVE ANALYSIS OF DWT LWTML AND PROPOSED TECHNIQUES USING ATTACK RECOVERY TIME, PSNR AND NC THOSE PARAMETERS FOR PENGUIN IMAGE IN ROBUST DIGITAL IMAGE WATERMARKING.

Method	Types of Attack	Attack Recovery Time	PSNR	NC
DWT [6]	Cropping	11.8248	23.4145	0.4685
	Shear	7.2072	20.3699	0.7921
LWTML [15]	Cropping	8.2056	21.5758	0.4939
	Shear	6.8172	18.9171	0.7720
Proposed	Cropping	1.5132	25.0009	0.8041
	Shear	1.4976	22.3699	0.9274

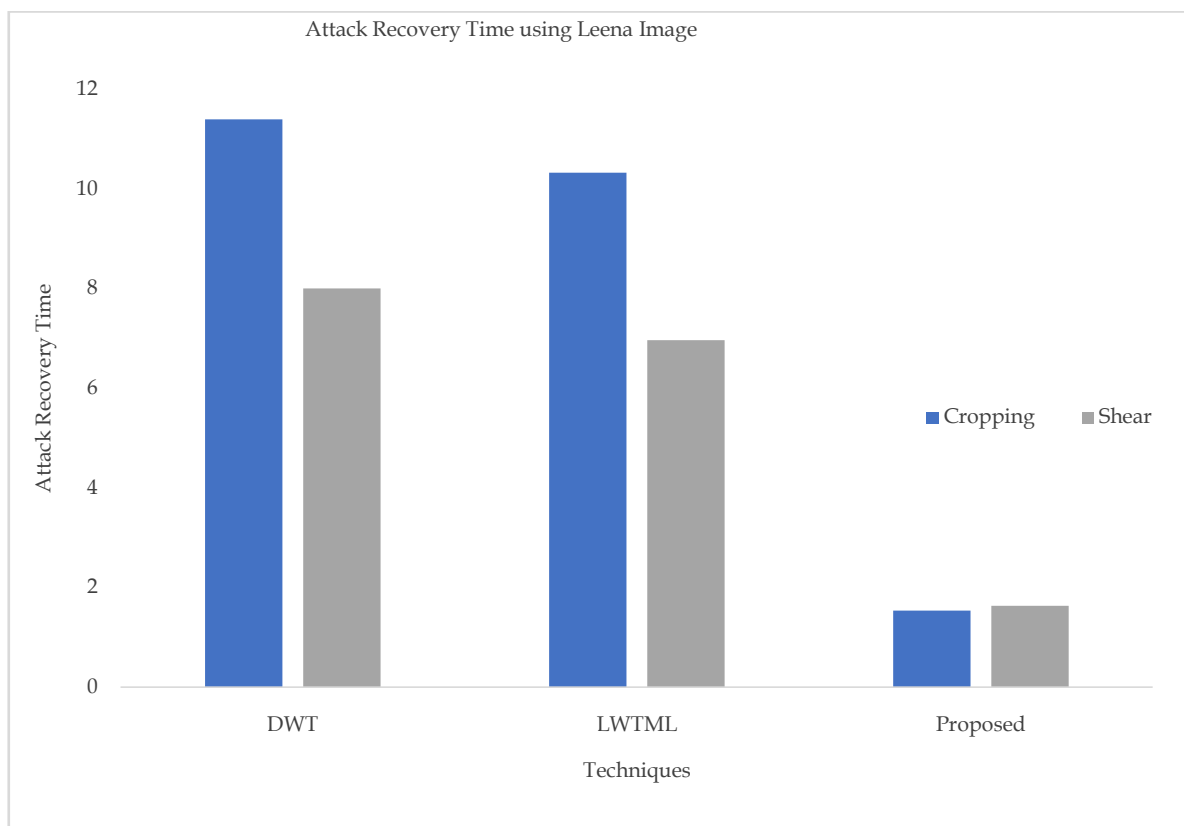


Fig. 4. Comparative performance analysis of attack recovery time using DWT, LWTML and proposed techniques with cropping and shear attack of Leena image.

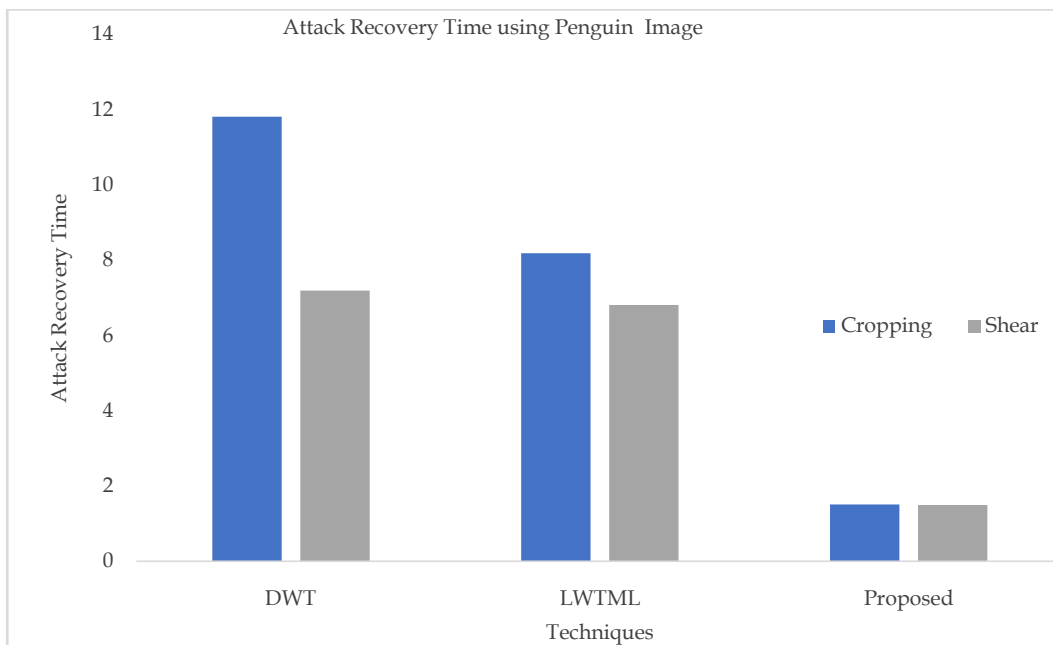


Fig. 5. Comparative performance analysis of attack recovery time using DWT, LWTML and proposed techniques with cropping and shear attack of penguin image.

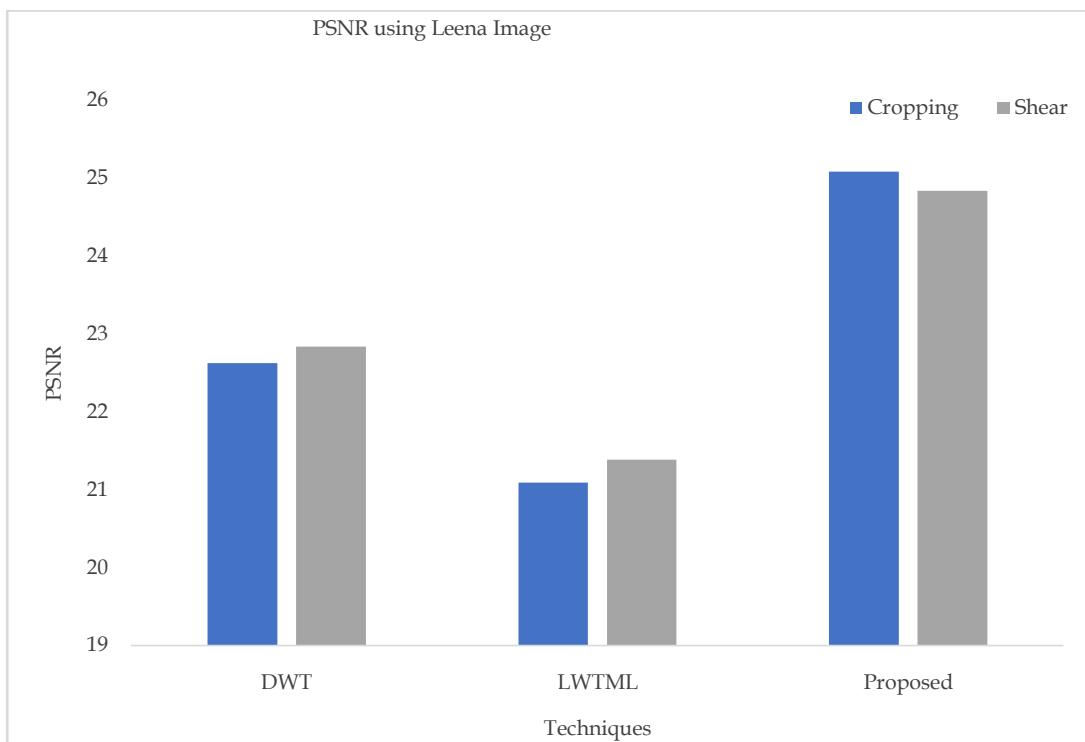


Fig. 6. Comparative performance analysis of PSNR using DWT, LWTML and proposed techniques with cropping and shear attack of leena image.

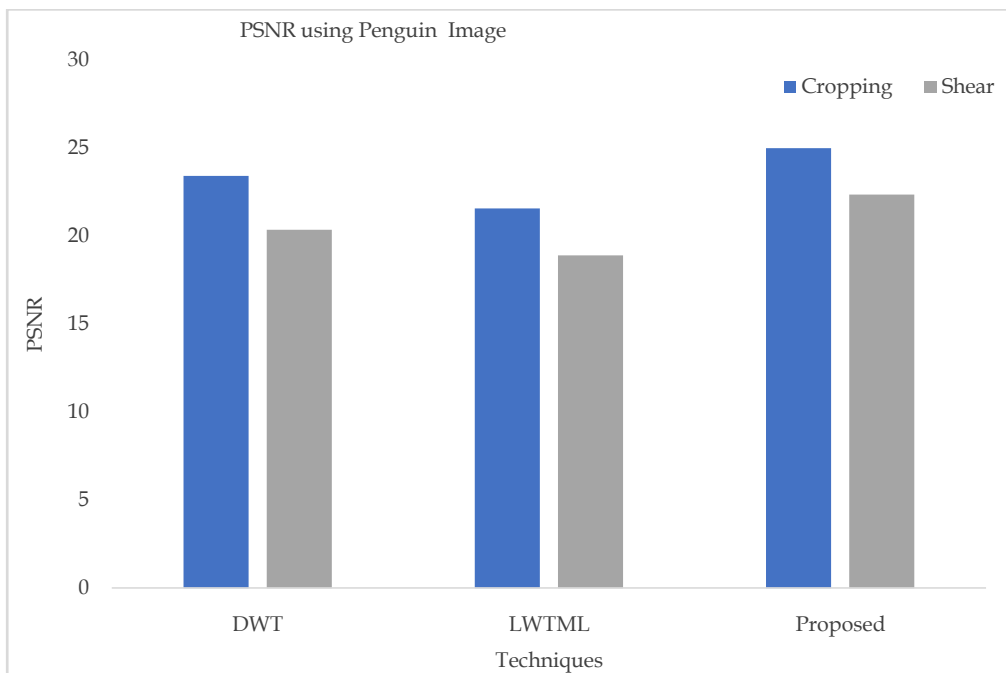


Fig. 7. Comparative performance analysis of PSNR using DWT, LWTML and proposed techniques with cropping and shear attack of penguin image.

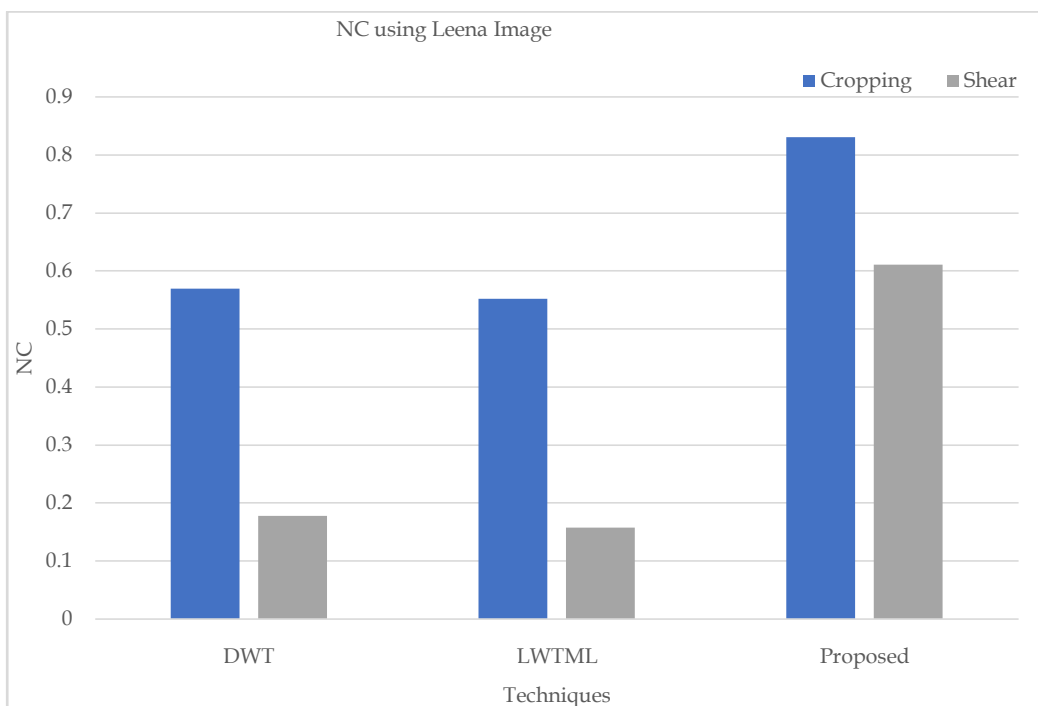


Fig. 8. Comparative performance analysis of NC using DWT, LWTML and proposed techniques with cropping and shear attack of Leena image.

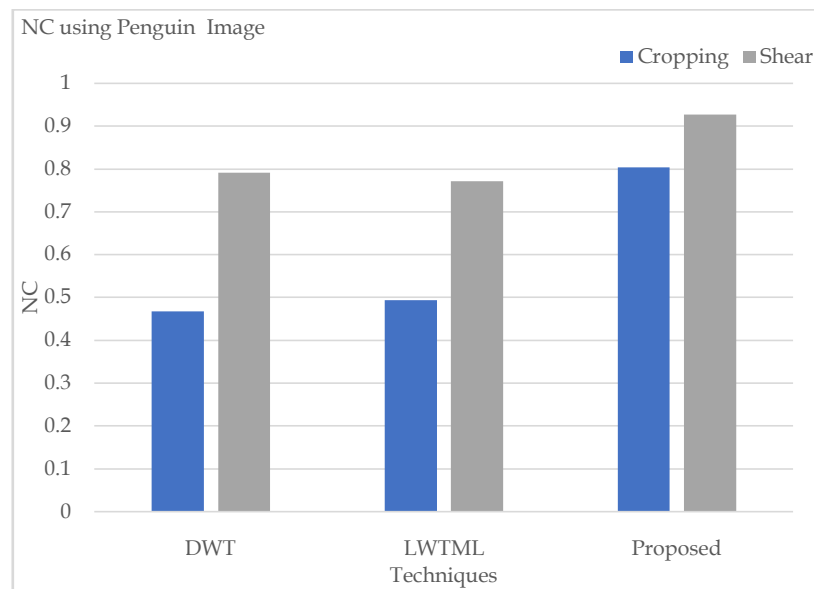


Fig. 9. Comparative performance analysis of NC using DWT, LWTML and proposed techniques with cropping and shear attack of penguin image.

V. Conclusion & Future Scope

Using water-marking systems applied to multimedia applications with a guaranteed quality requirement, we addressed a difficult design challenge in this research. By providing a unique fitness function to be used inside an ensemble classifier, a straightforward and efficient strategy for achieving high resilience under a restriction on the maximum distortion level was provided. The embedding strength settings were tuned to offer the most resilience within a predefined quality level limitation. The resilience and quality objectives are optimized individually in the proposed fitness function by decoupling the issue into two single-objective optimization sub-problems. Therefore, the weighting elements that are generally needed in traditional water-marking optimization systems are not necessary. A recent embedding technique was used, and the ABC algorithm with the suggested fitness function was then used to optimize it. Performance comparisons with commonly employed fitness functions based on the weighted sum technique were utilized to demonstrate the usefulness of the suggested fitness function. For comparison, recent watermarking methods were taken into account. The outcomes demonstrated how the watermarking scheme affected both quality and robustness. It is feasible to base the water-marking system's design on the maximum permitted distortion limit for the application in order to obtain the best level of resilience. The suggested method offers a way to regulate the quality level by changing a predetermined threshold. It was

found that the maximum value of the watermarking quality relies on the host picture, the embedding method, and the boundaries of the solution space.

References

- [1]. Abdelhakim, Assem Mahmoud, and Mai Abdelhakim. "A time-efficient optimization for robust image watermarking using machine learning." *Expert Systems with Applications* 100 (2018): 197-210.
- [2]. Liu, Shuai, Zheng Pan, and Houbing Song. "Digital image watermarking method based on DCT and fractal encoding." *IET image processing* 11, no. 10 (2017): 815-821.
- [3]. Huang, Xiaonan, Aijiao Cui, and Chip-Hong Chang. "A new watermarking scheme on scan chain ordering for hard IP protection." In *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1-4. IEEE, 2017.
- [4]. Khazraei, Amir, Hamed Kebriaei, and Farzad Rajaei Salmasi. "Replay attack detection in a multi agent system using stability analysis and loss effective watermarking." In *2017 American Control Conference (ACC)*, pp. 4778-4783. IEEE, 2017.
- [5]. Deeba, Farah, She Kun, Fayaz Ali Dharejo, and Hira Memon. "Digital image watermarking based on ANN and least significant bit." *Information Security Journal: A Global Perspective* 29, no. 1 (2020): 30-39.
- [6]. Ariatmanto, Dhani, and Ferda Ernawan. "An improved robust image watermarking by using different embedding strengths." *Multimedia Tools and Applications*: 1-27.
- [7]. Rakhmawati, Lusia, Wirawan Wirawan, and Suwadi Suwadi. "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability." *EURASIP Journal on Image and Video Processing* 2019, no. 1 (2019): 61.
- [8]. Huynh-The, Thien, Cam-Hao Hua, Nguyen Anh Tu, and Dong-Seong Kim. "Robust Image Watermarking Framework Powered by Convolutional Encoder-Decoder Network." In *2019 Digital Image Computing: Techniques and Applications (DICTA)*, pp. 1-7. IEEE, 2019.
- [9]. Valandar, Milad Yousefi, Milad Jafari Barani, and Peyman Ayubi. "A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map." *Soft Computing* (2019): 1-24.
- [10]. Cristin, Rajan, John Patrick Ananth, and Velankanni Cyril Raj. "Illumination-based texture descriptor and fruitfly support vector neural network for image forgery detection in face images." *IET Image Processing* 12, no. 8 (2018): 1439-1449.

- [11]. Kora, Padmavathi, Ch Usha Kumari, and K. Meenakshi. "Heart Arrhythmia Detection Using Wavelet Coherence and Firefly Algorithm." *Int. J. Comput. Appl* 975 (2018): 8887.
- [12]. Ronan, David, Zheng Ma, Paul Mc Namara, Hatice Gunes, and Joshua D. Reiss. "Automatic minimisation of masking in multitrack audio using subgroups." *arxiv preprint arxiv:1803.09960* (2018).
- [13]. Kumari, R. Radha, V. Vijaya Kumar, and K. Rama Naidu. "S-DWF: An Integrated Schema for Secure Digital Image Watermarking." In *Computer Science On-line Conference*, pp. 25-34. Springer, Cham, 2019.
- [14]. Abodena, Omar, and Mary Agoyi. "Colour Image Blind Watermarking Scheme Based on Fast Walsh Hadamard Transform and Hessenberg Decomposition." *Studies in Informatics and Control* 27, no. 3 (2018): 339-348.
- [15]. Bhowmik, Deepayan, and Charith Abhayaratne. "Embedding distortion analysis in wavelet-domain watermarking." *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 15, no. 4 (2019): 1-24.
- [16]. Mohsin, A. H., A. A. Zaidan, B. B. Zaidan, O. S. Albahri, A. S. Albahri, M. A. Alsalem, and K. I. Mohammed. "Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard." *Journal of medical systems* 43, no. 7 (2019): 192.
- [17]. Klaas, D. K. S. Y., M. A. Imteaz, I. Sudiyem, E. M. E. Klaas, and E. C. M. Klaas. "Novel approaches in sub-surface parameterisation to calibrate groundwater models." In *IOP Conference Series: Earth and Environmental Science*, vol. 82, no. 1, p. 012014. IOP Publishing, 2017.
- [18]. Alhumrani, Sultan A., and Mohammed J. Alhaddad. "ANN Model for Image Steganalysis Based on LSB." *International Journal of Computer Science and Information Security (IJCSIS)* 15, no. 7 (2017).
- [19]. Li, Jingyou, and Chaozhu Zhang. "Blind and robust watermarking scheme combining bimodal distribution structure with iterative selection method." *Multimedia Tools and Applications* (2019): 1-35.
- [20]. Bagade, Anant M., and Sanjay N. Talbar. "Intelligent Morphing and Steganography Techniques for Multimedia Security." In *Intelligent Techniques in Signal Processing for Multimedia Security*, pp. 47-64. Springer, Cham, 2017.