An Efficient Image Watermarking Approach based on Modified DWT Method to Improve the Performance

S.Markkandeyan[1], N Sengottaiyan[2], J.Vijayakumar[3], H.Senthil Kumar[4], P. Kalyanasundaram[5]

[1]*Professor, Department of Information Technology, KSR Institute for Engineering and Technology, Tiruchengode.*
[2]*Professor, Gopalan College of Engineering and Management, Whitefield, Bangalore.*
[3]*Associate Professor, Department of Electronics and Instrumentation, Bharathiar University, Coimbatore*
[4]*Assistant Professor, Department of Electronics and Communication Engineering,Gopalan College of Engineering and Management, Hoodi, Whitefield, Bangolore*
[5]*Professor, Institute of Electronics and Communication Engineering,Saveetha School of Engineering, SIMATS, Chennai.*
[1]*drsmkupt@gmail.com,* [2]*gcemprincipal@gmail.com,* [3]*vijayakumar@buc.edu.in,* [4]*halansenthil.ece@gmail.com,*
[5]*kalyanasundaramp.sse@saveetha.com*

Abstract.
In today's multimedia world, picture watermarking has become an essential component. Watermarking is a technique for securing information from tampering and ensuring integrity of data by injecting additional context to an original picture. Complicated and expensive, frequency transform domain methods diminish picture quality by reducing bit embedding. Uses the basic DCT technique with certain changes and applies it to the frequency ranges of DWT, as suggested. For embedding and extraction, the output is also employed in conjunction with a pixel alteration approach. An increase in efficiency in terms of time, imperceptibility, and stability is expected to be obtained.
Keywords. Watermarking; DCT; DWT; Embedding; Extraction; data integrity;

1. INTRODUCTION

As a signal-processing discipline, image processing is concerned with analyzing and processing images in order to produce the desired final picture, or to produce images that meet certain specifications. One must not overlook the importance of real material, as well. A digital picture's information should not be altered or duplicated throughout the digital processing of the image. Encryption, cryptography, digital signatures, and Steganography are some of the methods used to ensure the validity of material [1]. Both have their drawbacks. It is possible for a digital signature to identify changes to a picture, but it is not possible to determine the exact location of such changes. Information does not become yours when it is encrypted.
The employment of an image watermarking method [2] is one approach to provide validation, copyright, or ownership identity. Various algorithms are used to incorporate the appropriate watermark or brand into the original picture. In contrast to embedding, extraction typically goes the other way.
Digital information may be readily duplicated and manipulated because to the fast development of the Internet and digital multimedia capabilities. It is possible to leverage a watermark's security to stop material from being used illegally and to safeguard rights to intellectual property [3].
Figure 1 depicts the watermarking process. Four processes are involved: watermark creation, embedding, attacks, and recovery. Despite the attacker's best efforts, the watermark should remain hidden even if the host picture is rotated by a little amount.
Figure 2 depicts the fundamental steps involved in watermarking. Privacy via watermarking is a major problem because of a variety of attacks, including as rotation, translation, filtration, injecting noise, compression, etc. Copyrights mostly make use of frequency transform techniques [4]. Nevertheless, the integrity has worsened, thus additional bits cannot be inserted. Figure 3 depicts a picture with a watermark that may be seen. In tandem with pixel modification approaches, frequency domain approaches are incorporated, but they are time-consuming, complicated, not robust to diverse forms of assaults, and mostly capacity is lowered.

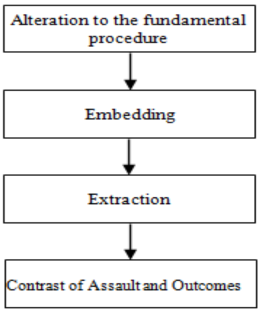


Figure 1. This is a simple watermarking framework.

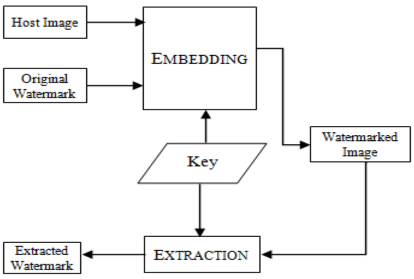


Figure 2: Process flow diagram for watermarking.

Figure 3. Watermarked image sample.

[5] In watermarking, the most essential aspect is to offer great resilience, safety, and scalability. Different forms of assaults must be thwarted by watermarking methods in the spatial and frequency transform domain. In a legal or medical matter, for example, a single photograph might be crucial evidence. Using technology such as Adobe, somebody may have made subtle modifications to the picture that would not be obvious to the naked eye. This would cause large alterations in such circumstances. Using fuzzy preprocessing is necessary if the photos are impacted by uncertainties and errors that influence the entire situation. Characterization of Watermarking Methods by kind of attack is shown in Figure 4.

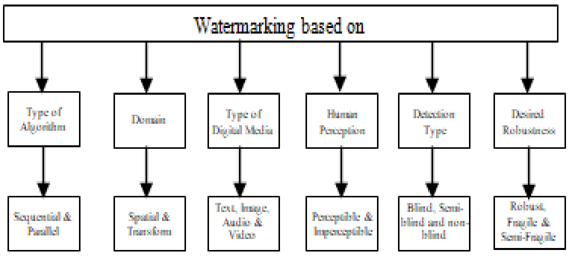


Figure 4: Techniques for watermarking categorization.

In this technique, improvements are made to the unifying framework and existing approaches are combined to create amethod for embedding and extraction. Then, a variety of assaults are used to evaluate the efficiency [6]. As a starting point, the fundamental goal of this study has been to provide a novel way for embedding and extracting data utilizing a hybrid method that includes modifications. It is therefore possible to compare the suggested technique's effectiveness with the efficiency of current solutions.

In this work, adjustments to DCT methodologies and mixtures of DWT, as well as modified approaches with pixel modification that remove the need of DCT for detecting DC parts in spatial domains, are implemented and analysed.

2. RELATED STUDY

Watermarking approaches for copyright and ownership recognition are covered in this area of the research. Watermarking is a popular approach for squaring the patient's relevant data for assessment in medical photographs. It has been determined that the effectiveness of an invisible watermark in a medical imaging application may be examined under a variety of assault scenarios. Nonetheless, most techniques fail to perform well when subjected to rotation assaults in copyrighting attacks. There is a test case of the medical photo watermarking approach for varying degrees of rotation assaults in this dissertation. Edge detection and dilatation methods are used in the construction of an undetectable watermarking approach for medical images. The dilated picture of the high frequency wavelet band is employed as a key for embedding by author [7]. Scaled As a watermark, dilated values are combined with a Gaussian noise template. The high frequency subband of the watermarked picture during the second level DWT decomposition is employed for watermark extraction during the redevelopment process.

Rebuilding quality is examined for various edge detector configurations and by adjusting scaling settings in conducted to test the technique's effectiveness against differing degrees of rotation assaults. Using the Canny edge operator and larger scaling variables under rotation attacks, it was shown to be the most effective method of obtaining the watermark during reconstruction. For various medical pictures, a parametric research is carried out using Mean Square Error and Signal to Noise Ratio. Copyright protection for digital goods is under significant threat as a result of the fast advancements in digital signal processing and computer network technologies. It is via the use of digital watermarking technology that copyright protection and content authentication are both made possible. A deep learning-based watermarking technique for color images is presented in publication [8]. The image's distinctive characteristics may be gleaned using the YUV color space, DCT, and binarization of the chrominance component. Testing results shows that the method is resistant to noise, compression, filtering and cropping, and successful copying assaults.

These days, many kinds of multimedia data, including text, images, music, and video, are created on a regular basis. Multimedia data security is the most important concern. Intruders have easy access to multimedia data and may quickly alter it. It is possible to safeguard multimedia data from illegal access by using watermarking and steganography methods. The data is hidden in the carrier signal via watermarking. Using Steganography, digital data (e.g. data files like audio, video, and text) may be hidden in another digital file. Maintaining watermark integrity is one of the primary goals of the watermarking process. As soon as an intruder attempts to corrupt or erase the watermark from the digital transmission, it's no longer usable. Different uses of watermarking, properties of watermarking, and the fundamentals of image processing are discussed in article [9]. In addition, the literature on digital picture watermarking is thoroughly reviewed in this research. We've also covered a few of the more advanced methods of optimization.

A new non-blind watermarking method for protecting personal information has been developed [10]. Using the signature of the document's owner as a watermark, the document's ownership and authenticity may be confirmed and preserved. Unlike other current approaches, the one we've described is dependable while also being almost undetectable. Relative and absolute findings reveal that the suggested strategy produces outstanding outcomes in experimental simulations and assessments. Multimedia data, such as digital photographs, are increasingly being used and produced as a result of the widespread usage of smart products and open networks. Although it has certain benefits, intellectual property violations have arisen as a result of this [11].

Watermarking digital images is a promising solution to these problems. When it comes to protecting intellectual property and improving the security of digital photographs, a new watermarking method is proposed in article [12] [13] that uses reversible data concealing with contrast enhancement. Reversible data hiding is used to hide a watermark logo in the spatial domain of the original picture such that the logo is exposed and the watermarked image is returned to its original form utilizing reversible functionality, which increases contrast and hides large amounts of data bits. Using the suggested method in a real-world setting has shown to be successful [14] [15]. The system's performance is compared to what is already available [16] [17].

3. METHODOLOGY

In both sectors, picture watermarking employs a variety of techniques. A wide range of picture watermarking techniques are utilised for both domains, including methods that alter the values of pixels, LSB-based watermarking, and DWT-based watermarking, among others. In all of these strategies, geometric and image processing assaults are not completely thwarted. DC components must be found using DCT in order to use these strategies.

Thus, the answer to this problem is a mechanism that modifies a fundamental procedure and removes the usage of DCT to discover DC components. Modifying DC and changing pixel values in the watermark is done as per the new approach, and then those watermark bits are replaced in the hosting file's DC components using the new approach. Figure 5 depicts the suggested methodology's process.

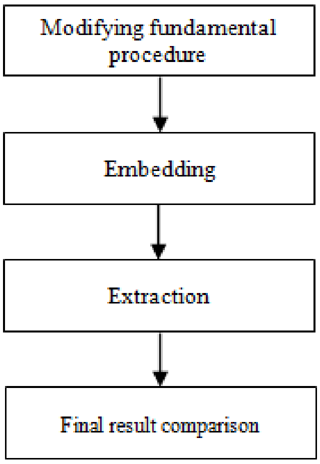


Figure 5. Proposed workflow.

Step I: Modifying fundamental procedure.

The LH band of the DWT technique is modified in the basic DCT technique to implement the alteration. DC values are updated and the frequency band is recalculated before further analysis is carried out. Figure 6 depicts the alteration of DC components. Tables 1 and 2 illustrate the embedding and extraction of DC coefficients that have been adjusted.

Block Image				
Pixel	1	2	3	4
1	52	52	50	54
2	50	53	55	55
3	53	52	54	56
4	53	57	54	50

Table 1. Calculation of DC Coefficient.

Resulted Image				
Pixel	1	2	3	4
1	56	56	54	58
2	54	53	55	55
3	57	52	54	56
4	56	57	54	50

Table 2. Updated DC Coefficient.

Attacks and Result Comparison.

To determine the actual and changed values, the operations were carried out on the host image. Next, a side-by-side comparison is carried out. Figure 6 depicts the whole process of embedding, extracting, attacking, and comparing results.

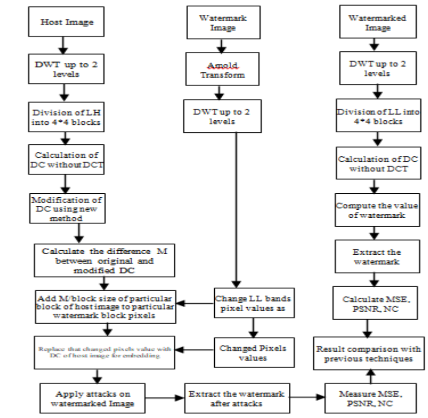
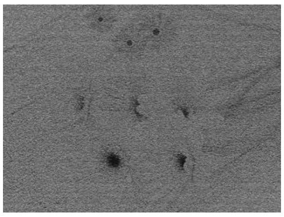


Figure 6. Proposed embedding, extraction algorithms, attacks, and result comparisons.

4. Results and Discussions

The following is how the initial change to the fundamental method is carried out here. When it comes to DC, there is no need for DCT or IDCT since it is immediately implemented in the spatial domain. Figure 7 shows a MATLAB simulation of a redesigned DC source.



Original Host Image DCT Image

Inverse DCT Result after modifying each pixel

Figure 7: Alteration based on DCT.

For the Block Image, the DC component is calculated using Tables 1 and 2.

4.1 Embedding and Extraction Process

Figure 8 depicts the end outcome of the watermark encoding and decoding process. Several assaults, including scaling, resizing, adaptive filtration and salt and pepper noise and Gaussian noise are presented in the following examples of watermark extraction. After scaling a picture to check for scaling assaults, the watermark is recovered in Figure 9. Using the suggested watermark extraction technique, Figure 10 shows how the first watermarked picture is clipped from all four edges and the watermark is then retrieved. An image-filtering assault is made to the watermarked picture in Figure 11 before the watermark is retrieved using a high-NC algorithm.

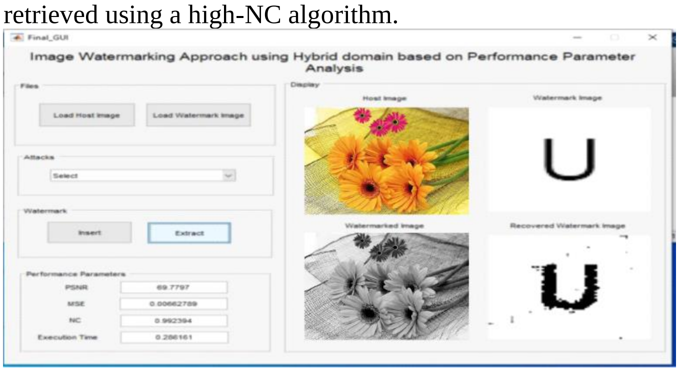


Figure 8: Embedding and extraction using the Suggested method.

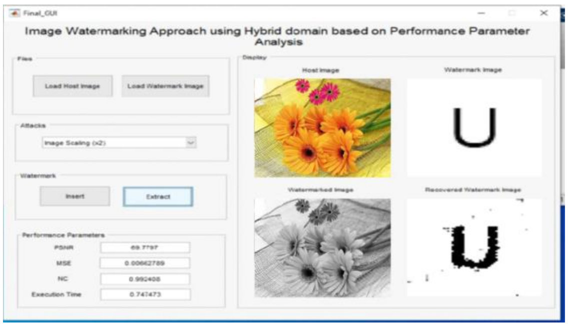


Figure 9: Image scaling attack and extraction of watermark after scaling of watermarked image.

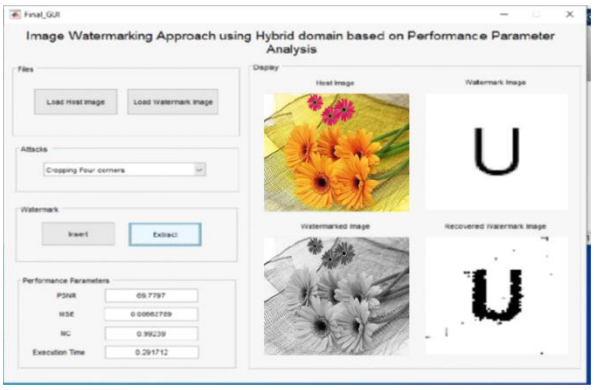


Figure 10: Cropping attack and extraction of watermark

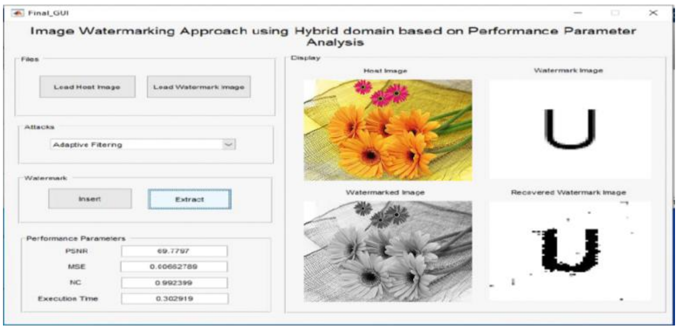


Figure 11: Adaptive filtering attack and extraction of watermark after filtering the watermarked image.

Salt and pepper noise is used to mask the watermark in Figure 12, and then the suggested approach is used to remove it. The normalized relationship is measured by comparing the original and retrieved watermarks. Table 3 compares the retrieved watermarks from various assaults with the original 64 x 64 watermark.

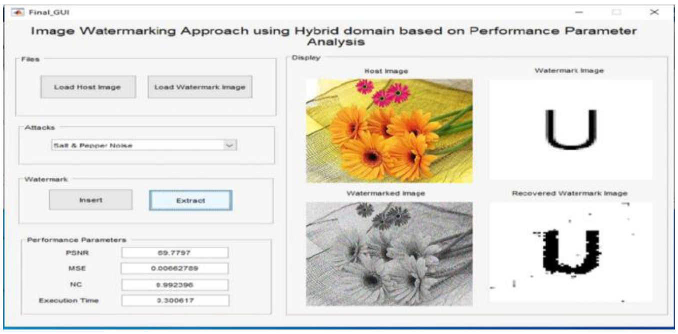


Figure 12: Injecting SP noise on the watermarked image

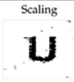
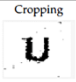
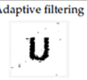
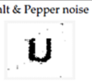
Original Watermark	Extracted Watermark			
	Scaling	Cropping	Adaptive filtering	Salt & Pepper noise
				

Table 3: Comparison of extracted watermark image of size 64 × 64.

4.2 A Real-Time Image Embedding and Extraction

Different resolution photos are utilized to measure the capacity. Images with watermarks are subjected to various assaults, which are subsequently used to remove the watermark. Histogram equalization, Gaussian noise, sharpening, and other methods are among the attack options. Using the suggested technology, watermarks may be embedded in real-time images as shown in Figure 13. An assault on a watermarked picture is shown in Figure 14, where the suggested approach is used to remove the watermark from it. Gaussian noise is applied to the watermark in Figure 15, and the watermark is retrieved after the noise is injected. Using the extraction process, a watermark may be removed from the picture in Figure 16.

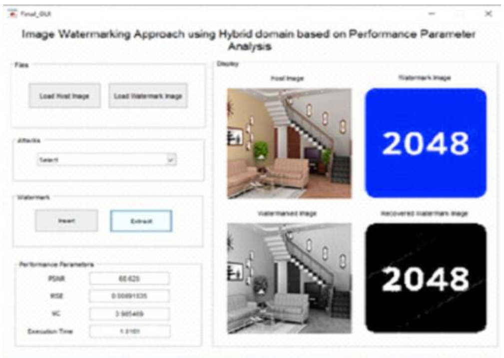


Figure 13: Embedding and Extraction using the proposed method for a real-time.

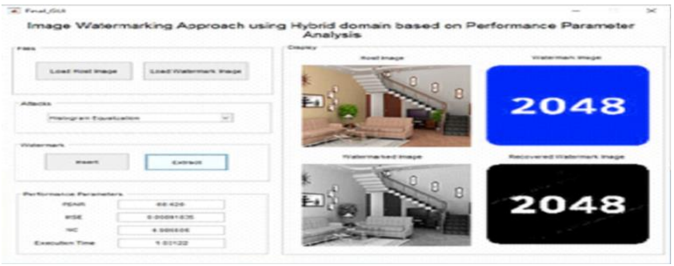


Figure 14: Applying histogram equalization

Figure 15: Injecting Gaussian noise

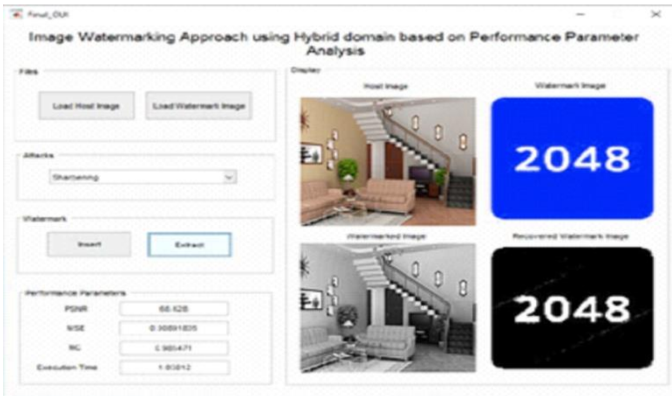


Figure 16: Sharpening watermarked image

Retrieved watermark is compared to original watermark in the following Table 4 to verify for resemblance and to measure normalized relationship, as shown

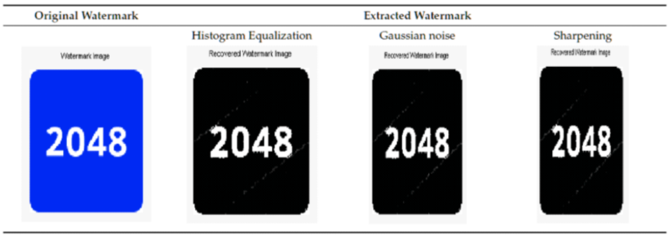


Table 4: Extraction of watermark Comparison

Existing and suggested methods are shown in Figure 17. NC should be as close to one as possible. This implies the technique is particularly resistant to a variety of assaults. Based on the graph, it can be determined that the suggested strategy is the most effective against all known forms of assaults. Increasing the size of the host and watermark images reduces the value of NC while also lengthening the time it takes to execute.

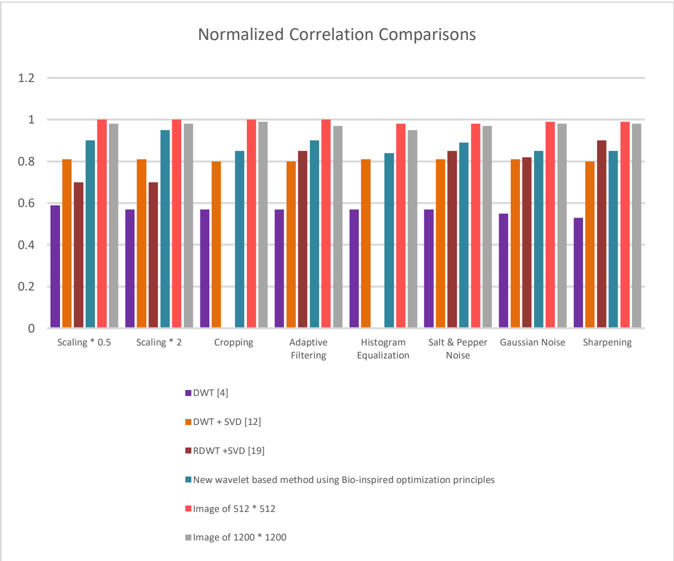


Figure 17: Comparison of Normalized correlation graph.

Figure 18 shows a comparison between the proposed technique and the current one based on PSNR, MSE, execution time, and NC value. Watermarking requires a high level of durability and resistance to deformation. DWT has been widely applied in earlier watermarking systems. Nevertheless, coefficients in the LL band frequency have strong resilience but poor distortion resistance, resulting in incorrect watermarking. DC coefficients are altered in the suggested technique, and then watermarking is carried out in the spatial domain, resulting in both high resilience and greater resistance to distortion. The suggested technique is more flexible and gives a better description of time and frequency. The drawbacks of utilizing DCT may be mitigated by not using DCT to locate DC, which increases execution time and MSE. The suggested technique may be used to a wide range of picture resolutions. The peak signal-to-noise ratio declines as the size of the base picture and watermark rises, but stability and runtime and mean square errors rise.

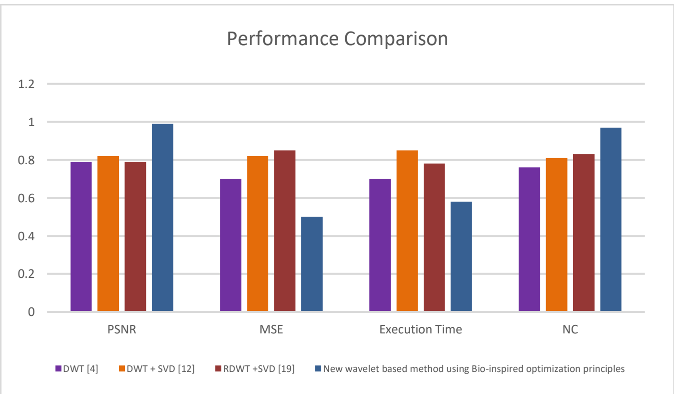


Figure 18: Performance Comparison Graph

5. CONCLUSION AND FUTURE SCOPE

Different watermarking methods are discussed in this paper. Additionally, other sorts of assaults on photographs have been addressed. The quality of the original picture should not be affected by the inclusion of a watermark. Work has been performed extensively to develop systems that are imperceptible, resilient, secure, and scalable. The primary goal of this project is to ensure long-term viability and high capacity. The basic technique is therefore altered, and embedding is carried out using a mixture of altered methodologies and established DWT methods; this cumulative approach is then used with pixel modifications, which improves capacity, reliability and imperceptibility while decreasing the overall execution time. MSE, PSNR, NC, and time are among the four metrics used to determine if the new approach improves on the old one. Instead of using SVD, RDWT, etc., DWT is used in this system. The same methodology may be utilized for video watermarking, and the same procedure can be employed.

6 REFERENCES

[1] N. Manohar and P. V. Kumar, "Data Encryption & Decryption Using Steganography," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 697-702, doi: 10.1109/ICICCS48265.2020.9120935.

[2] K. Hao, G. Feng and X. Zhang, "Robust image watermarking based on generative adversarial network," in China Communications, vol. 17, no. 11, pp. 131-140, Nov. 2020, doi: 10.23919/JCC.2020.11.012.

[3] Q. Yang, Y. Zhang, L. Wang and W. Zhao, "Watermark Image Reconstruction Based on Deep Learning," 2019 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC), 2019, pp. 739-743, doi: 10.1109/SDPC.2019.00140.

[4] Y. Vybornova, "Method for Image Copyright Protection Based on Construction of Highly Robust Watermarks," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116457.

[5] Y.Vybornova, "Method for Image Copyright Protection Based on Construction of Highly Robust Watermarks," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116457.

[6] D. Rosiyadi, H. Prasetyo, S. J. Horng and A. Indra Basuki, "Security Attack on Secret Sharing Based Watermarking Using Fractional Fourier Transform and Singular Value Decomposition," 2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 2020, pp. 343-347, doi: 10.1109/ICRAMET51080.2020.9298671.

[7] P. K. Shukla, P. Rawat, R. Singh and P. K. Dutta, "Efficient watermark reconstruction for medical images under rotation attacks using DWT," 3rd Smart Cities Symposium (SCS 2020), 2020, pp. 492-497, doi: 10.1049/icp.2021.0956.

[8] W. Jing, "Research on Digital Image Copying Watermarking Algorithm Based on Deep Learning," 2020 International Conference on Robots & Intelligent System (ICRIS), 2020, pp. 104-107, doi: 10.1109/ICRIS52159.2020.00034.

[9] L. Verma and S. Pratap Singh Chauhan, "A Review on Digital Image Watermarking Using Transformation and Optimization Techniques," 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020, pp. 1008-1012, doi: 10.1109/ICACCCN51052.2020.9362885.

[10] S. Sharma, J. J. Zou and G. Fang, "A Novel Signature Watermarking Scheme for Identity Protection," 2020 Digital Image Computing: Techniques and Applications (DICTA), 2020, pp. 1-5, doi: 10.1109/DICTA51227.2020.9363396.

[11] J. Sarabia-Lopez, D. Nuñez-Ramirez, D. Mata-Mendoza, E. Fragoso-Navarro, M. Cedillo-Hernandez and M. Nakano-Miyatake, "Visible-Imperceptible Image Watermarking based on Reversible Data Hiding with Contrast Enhancement," 2020 International Conference on Mechatronics, Electronics and Automotive Engineering (ICMEAE), 2020, pp. 29-34, doi: 10.1109/ICMEAE51770.2020.00013.

[12] S.Kannadhasan, R.Nagarajan and R.Banupriya, Performance Improvement of an ultra wide band antenna using textile material with a PIN diode, Textile Research Journal, DOI: 10.1177/00405175221089690journals.sagepub.com/home/trj

[13] P. Nirmala et al "An Effective Copyright Management Principle using Intelligent Wavelet Transformation based Water marking Scheme," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-7, doi: 10.1109/ACCAI53970.2022.9752516.

[14] M. Tamilselvi, et al, "A Novel Text Recognition Scheme using Classification Assisted Digital Image Processing Strategy," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2022, pp. 1-6, doi: 10.1109/ACCAI53970.2022.9752542.

[15] G Ramkumar, et al, “An Effectual Plant Leaf Disease Detection using Deep Learning Network with IoT Strategies”, Annals of the Romanian Society for Cell Biology, 2021, Vol.25, Issue.4, Page. 8876 – 8885. 1583-6258.

[16] G. Ramkumar, et al, “Experimental analysis of brain tumor detection system using Machine learning approach”, Materials Today: Proceedings, 2021, ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.01.246.

[17] Megalen Leo, A.Ranjith, R.Thandaiah Prabu, “Analysis of Mammogram Images using Active Contour Segmentation process & Level Set Method”, International Journal of Emerging Technology and Advanced Engineering, 2012, Vol.2, Issue.2, 2250-2459, ISBN:1472-1478.