

# Watermarking Approach based on Hybrid of DWT- SVD and ECC Algorithm

Gorkhnath Bhure  
Department of Electronics and  
communication Engineering  
Rabindranath Tagore  
University Raisen  
Madhya Pradesh, India

Laxmi Singh  
Department of Electronics and  
communication Engineering  
Rabindranath Tagore  
University Raisen  
Madhya Pradesh, India

Sanjeev Kumar Gupta  
Department of Electronics and  
communication Engineering  
Rabindranath Tagore  
University Raisen  
Madhya Pradesh, India

---

**Abstract:** Digital watermarking is the process of embedding a digital signal within digital media for copyright or authentication purposes. Digital image authentication is a major concern for the digital revolution because it is simple to alter any image. In the past few decades, ensuring the authenticity of digital images has been an imperative concern for researchers. Several suitable watermarking techniques have been developed based on the intended applications to address this concern. However, it is challenging to develop a watermarking system that is both robust and secure. This paper proposes digital watermarking techniques using DWT, SVD, and ECC algorithms with the random spread technique, which has been shown to enhance the output image quality. SVD-based watermarking modifies the singular values of the host image, whereas DWT-based watermarking modifies the coefficients of the high-frequency sub-bands of the host image. In contrast, ECC-based watermarking generates a digital secret using the owner's private key, which is then embedded in the watermark using a secret key. The DWT and SVD techniques offer excellent imperceptibility and robustness, whereas the ECC-based technique offers high security and authenticity. The simulation of these techniques is carried out using MATLAB, and the simulation results demonstrate their efficacy in terms of PSNR, MSE, and RMSE and normalized cross-correlation (NCC).

**Keywords:** Image watermarking SVD DWT, ECC, Haar transform, Digital watermarking.

---

## 1. INTRODUCTION

Image processing and the internet have made it much easier to copy, change, reproduce, and distribute digital photos at low cost and in almost real time, without losing the quality of the photos. This is possible because of how the two technologies work together. The development and improvement of network technology has happened so quickly that it puts the safety and privacy of data at risk. So, the authentication of content, the protection of copy rights, and the protection against duplication are all very important parts of the process of dealing with both the threats that are already here and the ones that will come up soon.[1] The process of digitally watermarking an image, also called digital image watermarking, is a simple way to make sure that the image can't be changed, that the owner owns all intellectual property related to the image, and that the image is real. Worries about how safe multimedia files are. Any kind of digital information, like photos, sounds, and movies, can be used to hide information. During the sending, processing, and storing of data, it is possible for digital content to be stolen, copied, and spread illegally through a physical transmission medium. This can happen in each of these three ways. Digital picture watermarking is the process of putting watermark data into a multimedia product and then getting that data out of the multimedia product or finding it in the multimedia product itself. These methods make sure that the image hasn't been changed, that it's been verified, that its content has been checked, and that it's been added [2-3]. If you want to get rid of a watermark, you can't just show the material that has been watermarked or change it into a different file format. Because of this, you can look at the watermark to find out what has

changed after an attack. It is important to know how digital watermarking differs from other technologies like encryption [4]. Digital picture watermarking techniques make it possible for a number of processes, such as going from digital to analogue, compression, changes in file format, re-encryption, and decryption, to be done without the watermark being destroyed. Because it can do all of these things, it can be used in place of cryptography or to help it.[5] Since the information is hard-coded into the text, it can't be taken out by using the text normally. The word "steganography" comes from the Greek word "steganos," which means "hidden." This method hides communication and changes an image in such a way that only the sender and the person to whom the message is meant can figure out what was sent.[6] This method makes it harder to find the person. Steganography is an alternative way to protect one's privacy and safety. Instead of encrypting communications, it can be used to hide them in other things that don't look like anything suspicious. Steganography can be used for both privacy and safety because of this. [7] On the other hand, steganography is a technology that can be used to share information and plan terrorist attacks. This is because of how quickly the internet and computer networks have grown.[8] Steganography is used to hide a cover image, while watermarking puts a message into the parts of a digital signal instead of the signal itself. So, a person who is listening in can't delete or change a message in order to get an output message. It is important to embed information into the original image so that content can't be seen by people who shouldn't be able to.[10] Steganography hides the existence of a cover image, while a watermarking technique embeds a message into the actual content of the digital signal within the

signal itself. Therefore, an eavesdropper cannot remove or replace a message to obtain an output message.[11] To protect content from unauthorized access, embedding information into the original image is essential. Digital image watermarking is imperceptible and hard to remove by unauthorized persons.[12]

### Image Watermarking Backgrounds and Frameworks

Due to the rapid growth of global computer networks, the internet, and multimedia systems, digital content can now be easily shared through many different channels of communication. By thinking of digital image watermarking as a research area, it is possible to build a platform for researchers. [13]This is done to protect digital information from being stolen, copied, changed, used, or shared illegally through physical transmission media during communications, processing of information, and data storage. [14]

**Random spread and non-random spread techniques** are two different methods used for embedding watermarks into digital media such as images, audio, and video. [15]

**Random spread technique:** In this technique, the watermark is spread randomly over the host media using a random key. The idea is to make it difficult for attackers to locate and remove the watermark. The random spread technique is typically used in conjunction with a secure encryption algorithm to provide additional security.[8]

**Non-random spread technique:** In this technique, the watermark is spread over the host media using a predetermined pattern. The pattern is designed to ensure that the watermark is imperceptible to the human eye while also being robust to common attacks such as compression, cropping, and filtering. The non-random spread technique is typically used in conjunction with a robust watermarking algorithm to provide additional robustness.[16]

## 2. PROPOSED WORK

In our work, we explore a new hybrid approach of DWT + SVD and ECC algorithm for security, for the improved quality of watermark insertion and extraction procedure. The DWT using Haar wavelets can be used to transform the input data into frequency components that can be analyzed and processed separately. SVD can then be used to reduce the dimensionality of the transformed data, while preserving important features. Finally, ECC can be used to encrypt the compressed data to protect it from unauthorized access this method is meant to improve the quality of the process of adding and removing watermarks. The benefit of this proposed method is that it is both hard to find and long-lasting, which are both good things to look for in an algorithm. When DWT and SVD are used together, they will

shed light on the possible mechanisms that are responsible for the owner's authenticity and resistance to different types of attacks. The suggested algorithm has two parts: the algorithm for embedding the watermark and the algorithm for getting the watermark out. The "Watermark Embedding Algorithm" and the "Watermark Extracting Algorithm" each have detailed explanations of both parts of the algorithm, as well as flowcharts for each. Embedding a watermark Figure 5, which can be found here, shows the steps that need to be taken to embed a watermark. The suggested method starts with picking a secret key, which is then used to make a random matrix, which is then used to put the watermark all over the image. The watermark is then changed by using DWT, and the DWT coefficients that are made as a result are changed by adding the spread watermark. The modified DWT coefficients are then inverse transformed using IDWT to obtain the watermarked image.

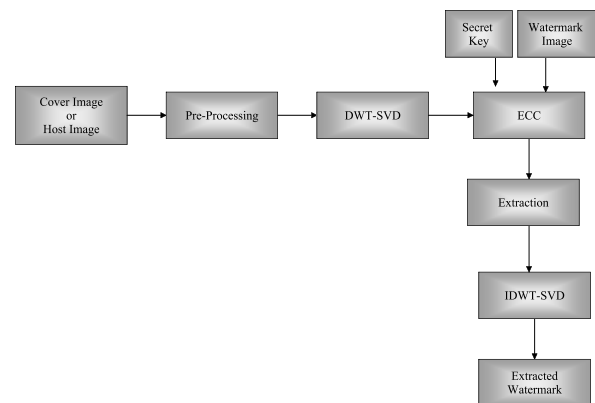


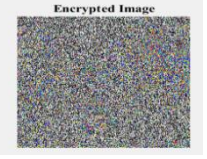
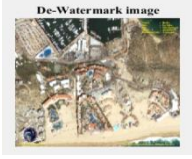



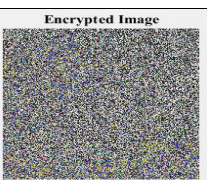
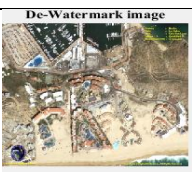

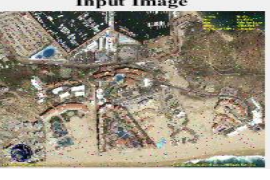


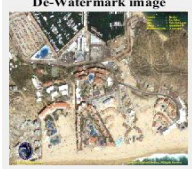

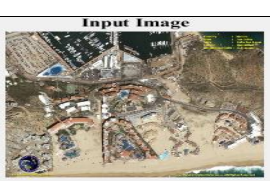

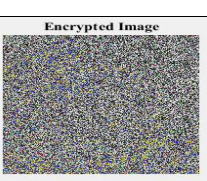




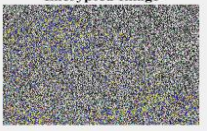
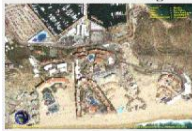



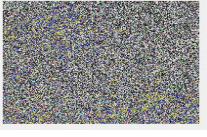














Fig.2 proposed flow diagram

## 3. RESULT DISCUSSION

Embedding time and extraction time are two important factors to consider when evaluating the performance of a watermarking algorithm. The noise attacks are common types of attacks used to test the robustness of watermarking algorithms. Salt and pepper noise adds random black and white pixels to the image, while Gaussian noise adds random values to each pixel based on a Gaussian distribution. Mean filtering is a common noise reduction technique that averages the values of neighboring pixels to reduce noise. JPEG compression is a lossy compression technique that can reduce the quality of an image, while cropping and scaling attacks modify the size and content of the image. Blur and unsharp attacks can also be used to alter the appearance of an image, potentially affecting the accuracy of watermark extraction.

Table 1 Visual results proposed approach for random spread technique

Types of attack	Input image	Watermark Image	Encrypted Image	De-Watermark Image	Extracted Image
No Attack					
JPEG					
Salt And Pepper					
Scaling					
Gaussian Noise					
Mil Filter					
Crop					
Blur					



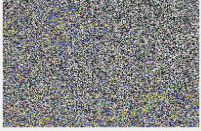










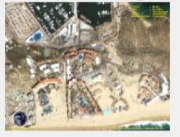






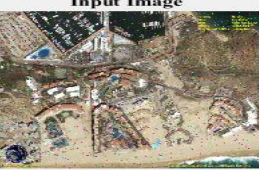






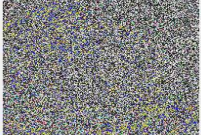


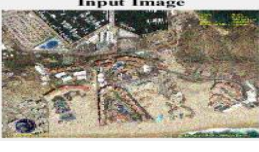

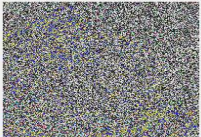


Unsharp					
Average					

Table 2 Visual results proposed approach for non-random spread technique

Types of attack	Input image	Watermark Image	Encrypted Image	De-Watermark Image	Extarcted Image
No Attack					
JPEG					
Salt And Pepper					
Scaling					
Gaussian Noise					








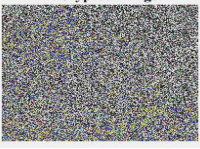




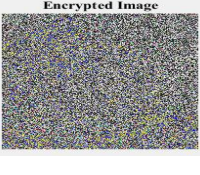




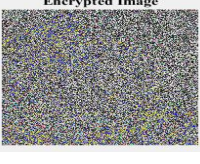




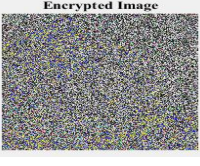


Mil Filter					
Crop					
Blur					
Unsharp					
Average					

Table 1 PSNR, MSE, RMSE performance of the proposed approach

#### 4. PERFORMANCE MEASURE

The table 1 above shows a comparison of different techniques used in image digital watermarking and their respective peak signal-to-noise ratio (PSNR) values. The PSNR metric measures the quality of the reconstructed image by comparing it to the original image. The results show that the proposed approach of DWT + SVD + ECC achieved the highest PSNR value of 52.36 dB, indicating better image quality compared to the other techniques.

#### 5. CONCLUSION

In this study, a strong and effective SVD, DWT, and ECC-based picture watermarking method is given to increase the

watermark while minimizing the impact on the image itself. Overall, your work seems to contribute to the development of more effective and secure digital watermarking techniques that can be useful in various applications.

Image	Random Spread			Non Random Spread		
	PSNR	MSE	RMSE	PSNR	MSE	RMSE
Image 1	50.0062	0.51	0.7182	48.48	0.57	0.88
Image 2	47.20	0.88	0.88	48.88	0.48	0.88
Image 3	48.17	0.86	0.82	50.58	0.47	0.86
Image 4	46.31	1.52	1.2	52.33	0.52	0.88
Image 5	52.12	0.87	0.85	48.22	0.51	0.87
Image 6	50.47	0.88	0.82	47.88	0.48	1.3
Image 7	48.17	0.72	0.88	48.40	0.46	0.88
Image 8	46.88	0.85	0.88	50.66	0.48	0.86
Image 8	51.36	0.88	0.84	51.38	0.57	0.88
Image 10	51.56	1.23	0.86	48.63	0.52	0.88

security level of the image. The scrambled watermark is added to the cover image using the SVD and three-level DWT algorithms. The suggested method was put to the test by putting watermarked photos through a series of attacks that got harder and harder. The results showed that the proposed method worked well and met the requirements for watermarking. This is because the method improves the capacity and security of embedded watermarks without hurting the quality of the cover image. This can be especially important in secure applications for telemedicine. By simulating them in MATLAB, different watermarking systems can be tested quickly to see how well they work. MATLAB has a number of built-in functions that can be used to create watermarking methods. It also lets users test how well the watermark holds up against different attacks, such as JPEG compression, cropping, and scaling. As part of this project, different, easier methods will be tried out to improve the quality of the images that have been watermarked. An ECC algorithm is used to spread the copyright image when it is added to the image of the container. Using SVD, DWT, and ECC algorithms, you aim to improve the security of the

#### 5. REFERENCES

1. Sayoko Kakikura; Hyunho Kang; Keiichi Iwamura Collusion Resistant Watermarking for Deep Learning Models Protection 2022 24th International Conference on Advanced Communication Technology (ICACT)
2. Bharti, N., Kumar, M., & Gupta, K. (2017). Comparative analysis between image de-noising algo rithm based on wavelet transform. In 2017 2nd international conference on inventive computation technologies, Coimbatore.
3. Maloo, S., Kumar, M., Lakshmi, N., & Pareek, N. K. (2018). Robust digital image watermarking based on hybrid GWO-DWT technique. International Journal of Pure and Applied Mathematics, 118(12), 12868–12876.
4. Touma, H. J. (2016). Study of the economic dispatch problem on IEEE 30-bus system using

- whale optimization algorithm. *International Journal of Engineering Technology and Sciences (IJETS)*, 5(1), 11–18.
5. Reddy, P. D. P., Reddy, V. V., & Manohar, T. G. (2017). Whale optimization algorithm for optimal sizing of renewable resources for loss reduction in distribution systems. *Renewables: Wind, Water, and Solar*, 4(1), 3.
  6. . Sharawi, M., Zawbaa, H. M., & Emary, E. (2017). Feature selection approach based on whale optimization algorithm. In 2017 Ninth international conference on advanced computational intelligence (ICACI) (pp. 163–168). IEEE.
  7. Shihab, H. S., Shafe, S., Ramli, A. R., & Ahmad, F. (2017). Enhancement of satellite image compression using a hybrid (DWT–DCT) algorithm. *Sensing and Imaging*, 18(1), 30z
  8. Sushma Jaiswal; Manoj Kumar Pandey Robust digital image watermarking using LWT and Random-Subspace-1DLDA with PCA based statistical feature reduction 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA) -2022 |
  9. Shuai Li; Zhefan Chen; Yanan Xie; Zhao Tian; Shanfeng Wang; Yihang Li; Yan Li A DWT Digital Watermarking Algorithm Based on 2D-LICM Hyperchaotic Mapping 2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE) - 2022 |
  10. Zainab F. Makhrib; Abdulmir A. Karim Improved Fragile Watermarking Technique Using Modified LBP Operator 2022 International Conference on Computer Science and Software Engineering (CSASE) Year: 2022 |
  11. Alshoura, W. H., Zainol, Z., Teh, J. S., & Alawida, M. (2020). A new chaotic image watermarking scheme based on SVD and IWT. *IEEE Access*, 8, 43381-43406.
  12. Prasanth Vaidya Sanivarapu , Kandala N. V. P. S. Rajesh , Khalid M. Hosny and Mostafa M. Fouda Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques *Appl. Sci.* 2022, 12, 8724. <https://doi.org/10.3380/app12178724> *Appl. Sci.* 2022, 12, 8724
  13. Neha Gupta; Ashok Bhansali Embedding Color Watermark by Adjusting DCT using RGB Gray Scale Watermarking 2021 Emerging Trends in Industry 4.0 (ETI 4.0) -2021
  14. Yifang Duang; Yi Wang; Congjun Cao; Xiaolin Zhang Research on Digital Watermarking Algorithm Based on Discrete Cosine Transform 2022 15th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI) -2022
  15. Dharmika B; Ch. Rupa; Haritha D; Vineetha Y Privacy Protection of Digital Information using Frequency Domain Watermarking Technique 2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) - 2022
  16. Rajpal, A., Mishra, A., & Bala, R. (2017, May). Fast digital watermarking of uncompressed colored images using bidirectional extreme learning machine. In 2017 International Joint Conference on Neural Networks (IJCNN) (pp. 1361-1366). IEEE.