International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Robust Digital Watermarking: A Review of Techniques and Performance

Sanjay Patsariya[1], Mahendra Kumar Pandey[2], Anand Jha [3] ,[4]J.S. Pahariya, [5]Pratiksha Tomar

[1,3,4] Department of Information Technology, RJIT, Gwalior, MP, India
[2]Department of Electronics & Communication Engg., RJIT,Gwalior,MP,India
[5]Department of Information Technology, RJIT, Gwalior, MP, India

---

Abstract -Watermarking constitutes a method employed to discreetly integrate concealed information or metadata without causing substantial degradation in content quality. This concealed information, referred to as a "watermark" serves multiple purposes, encompassing copyright protection, authentication, and detection of tampering. It is extensively utilized in industries like photography, publishing, and entertainment to dissuade unauthorized reproduction and distribution of digital media. In essence, watermarking is a technique entailing the incorporation of concealed information within digital media to safeguard intellectual property, establish authenticity, and facilitate content tracking, all without significantly compromising the quality of the media. It stands as a valuable tool for protecting digital assets and upholding content integrity in the contemporary digital landscape.

Key Words:Copyright Protection, DCT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform), DWT (Discrete Wavelet Transform), IWT (Integer Wavelet Transform), Scrambling.

1. INTRODUCTION

Watermarking is a fundamental and versatile technique used in the field of digital media to embed hidden information or metadata within digital content, such as images, audio, video, and documents [1]. The core idea behind watermarking is to make subtle and imperceptible alterations to the digital media that do not significantly affect its quality but allow for the identification or verification of the content. It should also be resistant to common attacks like compression, noise addition, and cropping. Digital watermarking plays a significant role in protecting intellectual property rights, especially in the digital age when multimedia content can be easily duplicated and distributed [2]. Blind watermarking, also known as robust blind watermarking, allows the extraction of the embedded watermark without needing the original, un-watermarked content. Non-blind watermarking requires access to the original, un-watermarked content for watermark extraction.

2. WATERMARKING OBJECTIVE

The main goal of watermarking is to incorporate concealed information or metadata into digital media, encompassing images, audio, video, or documents, all while minimizing any significant decline in the quality of the content [3]. This embedded information, referred to as a "watermark," fulfills diverse functions, including:

2.1 Copyright Protection: Watermarking is frequently utilized to prevent unauthorized usage, distribution, and reproduction of digital media.

2.2 Authentication: Watermarks offer a way to validate the integrity and legitimacy of digital content. Users can ascertain that the media they are engaging with is authentic and has not undergone any modifications or manipulations.

2.3 Content Tracking: Watermarks facilitate the tracking and surveillance of media across different platforms.

2.4 Tamper Detection: Watermarks can identify any unauthorized modifications or changes made to digital media.

3. CATERGORIZATION OF WATERMARKING METHODS

Watermarking techniques can be classified according to different factors, such as visibility, robustness, application, and domain. Here are some prevalent classifications:

3.1 Transparency

Visible Watermarks: Usually, these watermarks are superimposed onto the content and can be seen by the human

eye. Visible watermarks act as a declaration of ownership and have the potential to discourage casual unauthorized use [4,5].

Invisible Watermarks: Imperceptible to the human eye, invisible watermarks are seamlessly integrated into the content. This type of watermark is frequently employed for enhanced copyright protection and content tracking, as it poses a greater challenge for unauthorized users attempting removal.

3.2 Domain (Spatial vs. Transform)

The spatial domain and transform domain are foundational principles in signal processing, encompassing areas such as image and audio processing [4-9]. Table 1 illustrates the difference between spatial and frequency domains using various parameters.

Table-1: Various attributes of spatial and frequency domain

Factors	Spatial Domain	Frequency Domain
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Computational Complexity	Low	High
Computational Time	Less	More
Capacity	High	Low

In the realms of images and signals, prevalent transformations encompass the Fourier transform and wavelet transform [7-9]. The difference among various domains is illustrated in Table 2.

Table-2: Attributes of various transform domain

Parameters	DCT	DFT	DWT	IWT
Application	Frequently employed in the compression of images and videos, especially in formats such as JPEG.	Employed in signal analysis, spectral analysis, and audio processing.	Extensively used in image compression and de-noising.	It is a variation of the DWT, and it is typically employed in image and video compression.
Characteristics	It exhibits energy compaction, consolidating the majority of the signal's energy into a limited number of coefficients.	Offering a comprehensive perspective on the frequency components of the signal, it proves valuable for analyzing periodic signals	Partition the image into distinct frequency components. Capture both time and frequency information, offering a more versatile.	Functions with whole number values, rendering it appropriate for applications involving lossless compression.
Imperceptibility	In certain situations, it is less perceptually transparent compared to DWT.	It is generally not employed in watermarking applications where the preservation of perceptual transparency is crucial.	Opt for situations where preserving perceptual quality holds Significance.	Employed for watermarking without causing any loss to the original content.
Robustness	May not exhibit the same level of robustness against specific types of attacks, particularly those involving scaling and rotation.	It may not demonstrate the same level of robustness as other techniques.	Exhibits greater robustness against a range of attacks, including compression, noise, and geometric transformations, in comparison to DCT and DFT.	It might not match the robustness of DWT, primarily because of its emphasis on lossless compression.

3.3 Robustness: robustness refers to the ability of the embedded watermark to withstand various distortions, attacks, or alterations while remaining detectable and recoverable [1-3]. Various methods are employed in digital watermarking to achieve robustness against attacks and signal processing operations.Table 3 illustrates the difference between fragile, semi-fragile, and robust watermarking.

Table-3: Difference between Various watermarking schemes

Parameters	Fragile Watermarking	Semi-Fragile Watermarking	Robust Watermarking
Purpose	Fragile watermarking is primarily used for content authentication and tamper detection.	Semi-fragile watermarking is used for both content authentication and some degree of robustness.	Robust watermarking is primarily used for copyright protection, ownership
Robustness	Fragile watermarks are intentionally not built to withstand typical signal processing operations, compression, or any form of manipulation. They exhibit high sensitivity, reacting to even minor alterations.	Semi-fragile watermarks are crafted to exhibit increased tolerance toward certain common signal processing operations or legitimate content transformations. However, they still maintain sensitivity to malicious alterations.	Designed to endure common signal processing operations, compression, noise, and certain deliberate attacks, robust watermarks are intended to stay detectable and recoverable even after undergoing these transformations
Use Cases	Fragile watermarking finds frequent application in scenarios where the preservation of content integrity and authenticity is paramount, notably in fields like legal document and image forensics	Semi-fragile watermarking is commonly employed in situations where content authentication is crucial, allowing for some permissible transformations. Examples of its application	Robust watermarking is widely employed in applications like digital rights management (DRM), tracking and monitoring, and asserting ownership and copyright.
Detection	The detection process of a fragile watermark is usually straightforward and can quickly identify any unauthorized changes in the content.	Detecting unauthorized changes is possible with semi-fragile watermarking, but it requires a more careful and nuanced approach compared to fragile watermarking.	Detecting the presence of a robust watermark can be challenging in the presence of various signal-processing operations.

4. LITERATURE SURVEY

A literature survey on digital watermarking reveals a wealth of research and development in this field, covering various aspects, techniques, and applications Many researchers focus on developing robust watermarking techniques that can withstand common signal processing operations, such as compression, filtering, and noise addition.

Chou et al.[10] projected a methodology grounded on the wavelet domain to locate an appropriate host signal for watermark embedding by modifying the wavelet coefficients. To bolster robustness, permutation, and repetition are employed before the watermark insertion process. Due to the utilization of a blind watermarking approach, it proves to be space-efficient.

Su et al.[11] proposed a blind method employing QR decomposition for non-overlapping pixel blocks in color images, showcasing resilience against diverse attacks. Each plane of the watermark undergoes encryption using the Arnold transformation to augment security, with the number of iterations serving as a private key.

Gupta et al.[12] suggested an approach grounded on SVD-DWT-ABC to optimize strength parameters for embedding watermarks in an uncorrelated color space. The effective utilization of all color channels is a crucial aspect of the proposed method; however, the desired security requirements were not achieved.

Pandey et al.[13] introduced a non-blind approach that relies on SWT and SVD. The Y channel is employed for embedding, with a single-level scrambling technique. Their hybrid approach is designed to fulfill the criteria of transparency, robustness, and security.

Pandey et al.[14]. introduced a non-blind methodology based on LWT-SVD. The Y sub-band was utilized for watermark embedding. GWO was employed to select an optimized strength factor. Their approach included single-level Arnold-based scrambling.

Patsariya et al.[15] introduced a watermarking scheme based on multilevel LWT-SVD using a lifting scheme and a Y channel serving as the focal point. Image scrambling is achieved through chaotic image encryption transforms.

Patsariya et al.[16] introduced a watermarking technique based on Entropy-SVD-LWT; their paper also employs a multilevel-multiple image scrambling approach based on a modified Arnold transform to bolster security.

5.RESULT ANALYSIS

5.1 Imperceptibility assessment

Imperceptibility is a crucial performance parameter in digital watermarking, referring to the ability of the embedded watermark to remain visually unnoticeable while preserving the quality of the host image. It is commonly evaluated using Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NC) values. Higher PSNR indicates better visual quality, while NC values closer to 1 signify accurate watermark extraction.

Based on the reported results, Patsariya et al. [15] achieved the highest PSNR value of 50.52 dB, indicating excellent imperceptibility with minimal distortion in the watermarked image. Other methods, such as Patsariya et al. [16] (41.00 dB) and Pandey et al. [14] (39.51 dB), also demonstrate strong visual quality while maintaining high NC values of 0.99, reflecting reliable watermark recovery. Similarly, Pandey et al. [13] (38.36 dB) maintains a good balance between imperceptibility and robustness.

In contrast, earlier methods like Gupta et al. [12] (35.61 dB), Su et al. [11] (36.52 dB), and Chou and Liu [10] (37.36 dB) show comparatively lower PSNR values, suggesting slightly higher perceptual distortion. Additionally, the absence of NC values in these methods limits the evaluation of extraction accuracy.

Overall, the analysis indicates that hybrid and optimized techniques significantly improve imperceptibility while ensuring accurate watermark detection.

5.2 Robustness analysis

Robustness in watermarking refers to the ability of a watermark to remain detectable or recoverable even after the watermarked content has undergone various transformations or attacks [17-20].

Robustness is a key performance metric that evaluates the ability of a watermarking scheme to withstand various attacks while maintaining accurate extraction, typically measured using Normalized Correlation (NC) values. Higher NC values (close to 1) indicate strong robustness.

From the analysis, Patsariya et al. [16] and Patsariya et al. [15] consistently demonstrate superior robustness across most attacks. Under salt and pepper noise, both methods maintain high NC values (≈0.99 at low density), although performance slightly degrades as noise density increases. Similarly, in Gaussian and speckle noise attacks, these methods outperform others, maintaining NC values above 0.90 even at higher variance levels, indicating strong noise resistance.

In the case of filtering attacks such as median, Gaussian low-pass, and Wiener filters, Patsariya et al. [15] achieves excellent performance (up to 0.98), while Patsariya et al. [16] shows moderate resilience. Earlier methods, particularly Chou et al. [10], exhibit significantly lower robustness (e.g., NC = 0.18 under median filtering), highlighting their limitations.

For geometric attacks, including resizing, rotation, scaling, and cropping, Patsariya et al. [15] again performs best, maintaining high NC values (e.g., 0.95 under resizing and up to 0.98 in scaling). Additionally, it shows resilience against motion blur and AWGN, where other methods lack reported results.

Overall, hybrid and multilevel techniques, especially those incorporating LWT-SVD and advanced encryption, significantly enhance robustness compared to earlier approaches.

6. CONCLUSIONS

Various digital watermarking techniques, including DCT, DFT, DWT, IWT, and entropy-based methods, offer distinct advantages depending on application requirements. The selection of an appropriate technique largely depends on the balance between key performance parameters such as imperceptibility, robustness, and embedding capacity.

Among these, DWT-based methods are widely preferred due to their ability to provide a good trade-off between visual quality and resistance to attacks. By operating in the time–frequency domain, DWT enables efficient embedding in perceptually significant regions, thereby enhancing both robustness and imperceptibility. IWT, as an extension of DWT, is particularly useful for lossless reconstruction and accurate watermark

extraction, making it suitable for applications where data integrity is critical.

On the other hand, DCT and DFT techniques are effective in frequency-domain processing and are commonly used in compression-related applications; however, they may offer limited flexibility compared to wavelet-based approaches. Entropy-based methods, though less frequently used, are advantageous in scenarios requiring enhanced robustness, as they focus on embedding watermark data in highly informative regions of the image.

REFRENCES

1.Patsariya, S., Dixit, M.: A Survey on Watermarking and Its Techniques. Algorithms for Intelligent Systems. 71–78 (2021). https://doi.org/10.1007/978-981-33-4893-6_7.

2.Pandey, M.K., Parmar, G., Patsariya, S.: An Effective Way to Hide the Secret Audio File Using High Frequency Manipulation. Communications in Computer and Information Science. 125–130 (2011). https://doi.org/10.1007/978-3-642-18440-6_15.

3.Begum, M., Uddin, M.S.: Digital Image Watermarking Techniques: A Review. Information. 11, 110 (2020). https://doi.org/10.3390/info11020110.

4.Anand, A., Singh, A.K.: Watermarking techniques for medical data authentication: a survey. Multimedia Tools and Applications. (2020). https://doi.org/10.1007/s11042-020-08801-0.

5.Singh, A.K., Sharma, N., Dave, M., Mohan, A.: A novel technique for digital image watermarking in spatial domain. 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing. (2012). https://doi.org/10.1109/pdgc.2012.6449871.

6.Patvardhan, C., Kumar, P., Vasantha Lakshmi, C.: Effective Color image watermarking scheme using YCbCr color space and QR code. Multimedia Tools and Applications. 77, 12655–12677 (2017). https://doi.org/10.1007/s11042-017-4909-1.

7.Singh, R.K., Shaw, D.K., Jha, S.K., Kumar, M.: A DWT-SVD based multiple watermarking scheme for image based data security. Journal of Information and Optimization Sciences. 39, 67–81 (2017). https://doi.org/10.1080/02522667.2017.1372153.

8.Parah, S.A., Sheikh, J.A., Assad, U.I., Bhat, G.M.: Realisation and robustness evaluation of a blind spatial domain watermarking technique. International Journal of Electronics. 104, 659–672 (2016). https://doi.org/10.1080/00207217.2016.1242162.

9.Agarwal, N., Singh, A.K., Singh, P.K.: Survey of robust and imperceptible watermarking. Multimedia Tools and Applications. 78, 8603–8633 (2019). https://doi.org/10.1007/s11042-018-7128-5.

10.Chun-Hsien Chou, Kuo-Cheng Liu: A Perceptually Tuned Watermarking Scheme for Color Images. IEEE Transactions on Image Processing. 19, 2966–2982 (2010). https://doi.org/10.1109/tip.2010.2052261.

11.Su, Q., Niu, Y., Wang, G., Jia, S., Yue, J.: Color image blind watermarking scheme based on QR decomposition. Signal Processing. 94, 219–235 (2014). https://doi.org/10.1016/j.sigpro.2013.06.025.

12.Gupta, M., Parmar, G., Gupta, R., Saraswat, M.: Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony. International Journal of Computational Intelligence Systems. 8, 364 (2015). https://doi.org/10.1080/18756891.2015.1001958.

13.Pandey, M.K., Parmar, G., Gupta, R., Sikander, A.: Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space. Microsystem Technologies. 25, 3071–3081 (2018). https://doi.org/10.1007/s00542-018-4162-1.

14.Pandey, M.K., Parmar, G., Gupta, R., Sikander, A.: Lossless robust color image watermarking using lifting scheme and GWO. International Journal of System Assurance Engineering and Management. 11, 320–331 (2019). https://doi.org/10.1007/s13198-019-00859-w.

15.Patsariya, S., Dixit, M.: A New Block Based Non-Blind Hybrid Color Image Watermarking Approach Using Lifting Scheme and Chaotic Encryption Based on Arnold Cat Map. Traitement du Signal. 39, 1159–1168 (2022). https://doi.org/10.18280/ts.390408.

16.Patsariya, S., Dixit, M.: Entropy Based Secure and Robust Image Watermarking Using Lifting Wavelet Transform and Multi-Level-Multiple Image Scrambling Technique.

Traitement du Signal. 39, 1751–1759 (2022). https://doi.org/10.18280/ts.390533.

17.Tao, H., Chongmin, L., Mohamad Zain, J., Abdalla, A.N.: Robust Image Watermarking Theories and Techniques: A Review. Journal of Applied Research and Technology. 12, 122–138 (2014). https://doi.org/10.1016/S1665-6423(14)71612-8.

18.Fatahbeygi, A., Akhlaghian Tab, F.: A highly robust and secure image watermarking based on classification and visual cryptography. Journal of Information Security and Applications. 45, 71–78 (2019). https://doi.org/10.1016/j.jisa.2019.01.005.

19.Zhang, H., Wang, C., Zhou, X.: A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain. Future Internet. 9, 45 (2017). https://doi.org/10.3390/fi9030045.

20.Kumar Pandey, M., Patsariya, S., Jha, A.: A Segmentation-Driven Non-Blind DWT Watermarking Framework Ensuring Robustness, Transparency, and Security. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. 10, 1–9 (2026). https://doi.org/10.55041/ijsrem58141.