International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Strong Digital Image Watermarking Techniques Using Transform-Domain Methods

Sunit Jana , Rakhi Biswas ,Disha Das, Deepshikha Chatterjee , Nikita Pal , Debasmita Basak ,Koushik Pal
Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology ,Kolkata ,India

Abstract - As digital content becomes more widely shared, protecting intellectual property through digital watermarking is essential. This paper offers a detailed review of watermarking techniques that use transform-domain methods, including Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD). These methods provide better resistance to common image processing attacks while maintaining high imperceptibility and supporting various application scenarios. By examining key contributions from recent studies, this article shows the development of hybrid watermarking schemes, compares their performance, and points out trends in colour watermarking and optimization-based methods. The findings are helpful for researchers and practitioners working on secure and durable watermarking systems.

Key Words: Digital Image Watermarking ,Transform-Domain Techniques ,Robustness ,Discrete Cosine Transform (DCT) ,Discrete Wavelet Transform (DWT) ,Singular Value Decomposition (SVD) , Hybrid Watermarking.

1.INTRODUCTION

The rapid growth of digital media and the ease of sharing content online have made protecting intellectual property a major concern. Digital images are especially at risk of being copied, altered, and redistributed without permission. This creates significant challenges in keeping ownership rights, authenticity, and integrity. To tackle these problems, digital watermarking has become an effective method for embedding hidden information in multimedia content. This serves purposes like copyright protection, tamper detection, and content authentication.

Digital image watermarking techniques are typically divided into two categories: spatial-domain methods and transform-domain methods. Spatial-domain techniques change pixel values directly to embed the watermark. However, they are often fragile and can easily be affected by standard image processing actions. In contrast, transform-domain watermarking uses mathematical transforms to adjust frequency components or coefficients of the image. This approach provides better protection against compression, filtering, noise, and geometric attacks.

Among various transform-based techniques, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT) are the most researched. They have strong theoretical support and practical uses. Some hybrid methods combine two or more transforms, such as DWT-DCT or DWT-SVD. These hybrids take advantage of the unique strengths of each transform, improving performance in robustness, invisibility, and capacity for data.

This paper offers a thorough review of the latest transform-domain watermarking techniques. It examines the basic principles, advantages, and weaknesses of each method. The review also discusses how hybrid approaches have developed to address the limitations of individual methods. The goal is to provide researchers and practitioners with an informative comparison of techniques while suggesting future paths for effective and strong digital watermarking in image processing.

2. IMPORTANCE OF ROBUSTNESS IN WATERMARKING

In digital watermarking, robustness means the ability of the embedded watermark to withstand intentional or unintentional changes to the host image. This includes compression, noise, filtering, cropping, rotation, scaling, and other processing actions. Robustness is crucial for watermarking systems, especially in copyright protection, ownership verification, and authentication. The integrity and retrievability of the watermark must remain intact under various conditions. Watermarked images often get compressed (e.g., JPEG), filtered, resized, or improved during transmission or storage. A robust watermark should survive these actions and remain detectable without significant loss of quality.

Attackers may try to remove or damage the watermark using methods like cropping, noise addition, histogram equalization, or collusion attacks. Robust watermarking ensures that the watermark cannot be easily removed or changed without greatly harming the image. In copyright disputes or legal situations, the watermark can act as digital proof of ownership. A weak watermark may fail with minor changes, which weakens its admissibility and reliability in court. For uses such as medical imaging, satellite imaging, and surveillance, the watermark must confirm that the content has not been altered. Robustness ensures accurate detection even if the image undergoes standard processing. In real-world situations, images are shared across different platforms, devices, and networks.

Robust watermarking works effectively across various formats and conditions. Trade-off with Imperceptibility and Capacity , achieving robustness often means making trade-offs. Embedding a strong watermark may make it visible. Increasing watermark strength might also lower the amount of information that can be embedded. Thus, designing a watermarking scheme requires balancing robustness with image quality and data capacity.

Transform-domain watermarking methods are commonly used to improve robustness. By embedding the watermark in frequency components that are less prone to image manipulation, these methods improve resistance to compression (e.g., DCT in JPEG), manage geometric attacks (e.g., DFT for rotation and scaling), provide better trade-offs between robustness and invisibility (e.g., DWT with multi-level decomposition).

3. BACKGROUND OF DIGITAL WATERMARKING

Digital watermarking embeds hidden information, called a watermark, within digital media like images, audio, or video. This process helps claim ownership, authenticity, or integrity. Unlike traditional encryption, which locks up the entire content, watermarking keeps the content accessible while still including ownership details that can be retrieved when needed. This is especially helpful for content distribution, enforcing copyright, and detecting tampering. The concept of watermarking goes back centuries. It comes from the use of visible signs, like seals or logos, on paper or currency. In the digital era, this idea has shifted to invisible digital marks. These marks are meant to be undetectable by the human eye yet identifiable by algorithms. Digital watermarking systems can be broadly classified based on several characteristics:

1. *Domain:* Spatial-domain techniques change pixel values to insert the watermark. Transform-domain methods embed the watermark within the image's frequency components using mathematical transforms such as DCT, DWT, and DFT.

2. *Perceptibility:* Visible watermarking, like logos, is meant to be noticeable. Invisible watermarking hides the watermark within the host image without changing how it looks.

    - *Robustness:* Robust watermarking is built to endure common image processing attacks, including compression, filtering, and resizing. Fragile watermarking is sensitive to changes, making it good for tamper detection and authentication.

A typical digital watermarking system has two main processes: embedding and extraction. In embedding, the watermark is added to the original image, creating a watermarked image. In extraction, the watermark is retrieved, either without the original image (blindly) or with it (non-blindly). The effectiveness of a watermarking scheme is evaluated based on three main criteria:

1. *Imperceptibility:* The watermarked image should look the same as the original.

2. *Robustness:* The watermark should survive common image alterations or attacks.

3. *Capacity*: The amount of data that can be reliably added and retrieved.

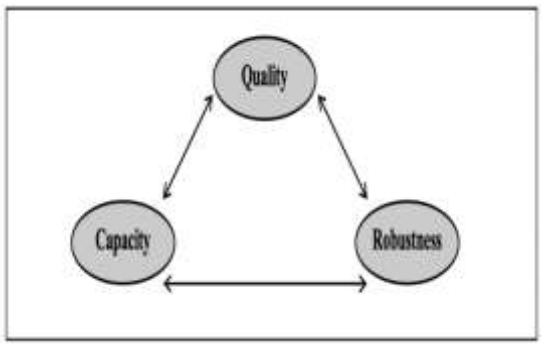

Fig1: Three requirements of Watermarking

As digital watermarking technologies improve, transform-domain methods have gained attention in research because of their better performance in robustness and invisibility. These approaches work with frequency components rather than raw pixels, making them less likely to degrade during normal signal processing tasks. The following sections will explore these transform-based techniques, their principles, and their relative strengths.

4. BASIC PRINCIPLE OF DIGITAL IMAGE WATERMARKING

Digital image watermarking is the process of embedding a hidden signal, known as the watermark, into a host image. The goal is to make the watermark invisible to human vision while still allowing for later detection or extraction for verification, authentication, or copyright protection. Several main principles guide the watermarking process. These principles determine how and where the data is embedded, how it is retrieved, and how well it can withstand different conditions.

A. Components of a Watermarking System

A typical watermarking system includes the following major components:

1. *Host Image (Cover Image):* The original image used to embed the watermark.
2. *Watermark (Payload):* The information to be embedded, such as a logo, ID, or binary string.
3. *Watermarking Algorithm:* The mathematical method used to insert or extract the watermark.
4. *Key (optional):* A secret key that secures the embedding and extraction processes for added security.
5. *Watermarked Image:* The output image after embedding the watermark, which should look almost identical to the original.

B. Watermark Embedding Process:

The embedding process changes the host image by inserting watermark information into selected regions or transform coefficients.

1. *Transform (Optional):* Convert the host image to a different domain, like DCT or DWT, to improve invisibility and strength.
2. *Selection of Embedding Region:* Choose where to embed the watermark, whether in spatial or transform coefficients, such as middle-frequency DCT coefficients or DWT LL sub-band.
3. *Embedding Rule:* Modify the selected coefficients based on the watermark data, which may involve adding, quantizing, or altering the sign.
4. *Inverse Transform (if used):* Convert the modified coefficients back to the spatial domain.
5. Output: The final watermarked image, which should look nearly identical to the original.

5.TRANSFORM DOMAIN WATERMARKING TECHNIQUES

Transform-domain techniques, also known as frequency-domain methods, are some of the most effective and common approaches in digital image watermarking. These techniques embed watermark data into the transformed coefficients of the host image instead of its pixel values. By taking advantage of the frequency characteristics of the image, these methods improve imperceptibility and resilience against common image processing attacks like compression, filtering, and noise.

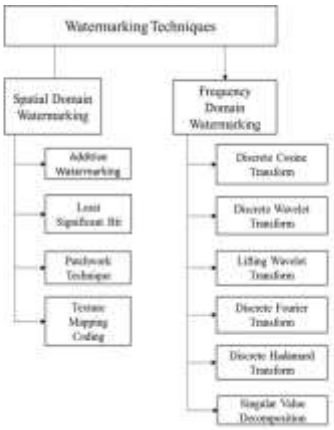

Fig 2: Watermarking techniques

A. Discrete Cosine Transform (DCT)

JPEG and other image compression formats widely use the DCT. It separates an image into parts with different frequencies, concentrating most energy in low-frequency components.

1. *Watermarking Process:*
   - Divide the image into 8×8 blocks.
   - Apply DCT to each block.
   - Include watermark bits in mid-frequency coefficients to balance resilience and imperceptibility.
   - Apply inverse DCT to get the watermarked image.
2. *Strengths:*
   - High robustness against JPEG compression.
   - Low visual distortion.
3. *Limitations:* Less resistant to geometric distortions like scaling or rotation.

B. Discrete Wavelet Transform (DWT)

The DWT analyzes the image at multiple resolutions by breaking it into four sub-bands: LL (approximate), LH, HL, and HH (details).

1. *Watermarking Process:*
   - Apply DWT to decompose the image.
   - Place a watermark in a few selected sub-bands, usually LL or LH.
   - Perform inverse DWT to reconstruct the image.
2. *Strengths:*
   - Excellent imperceptibility and robustness.

- Suitable for multiresolution and scalable watermarking.

3. *Limitations:* Slightly higher computational complexity.

C. *Discrete Fourier Transform (DFT)*

DFT represents the image in terms of sinusoids with different frequencies. It offers rotation, scaling, and translation invariance, making it useful against geometric attacks.

1. *Watermarking Process:*
   - Apply DFT to the entire image.
   - Embed the watermark into the magnitude (not phase) of selected frequency components.
   - Apply inverse DFT.
2. *Strengths:*
   - Robust to geometric distortions.
   - Suitable for watermarking under affine transformations.
3. *Limitations:*
   - Poor spatial localization.
   - Requires careful handling to avoid distortions.

D. *Singular Value Decomposition (SVD)*

An image matrix can be divided into three parts using the SVD matrix factorization technique: U, Σ (singular values), and V^t.

1. *Watermarking Process:*
   - Decompose the image matrix using SVD.
   - Modify the singular values with the watermark.
   - Reconstruct the image using the altered singular values.
2. *Strengths:*
   - High robustness and stability.
   - Minor changes in singular values do not significantly affect visual quality.
3. *Limitations:*
   - Computationally expensive.
   - Less intuitive embedding process.

E. *Hybrid Transform Techniques*

Hybrid methods combine two or more domain techniques, like DWT-DCT, DWT-SVD, or DCT-SVD, to leverage the strengths of multiple transforms.

1. *Example:* DWT-DCT Method
   - Apply DWT to obtain sub-bands.
   - Perform DCT on a sub-band (for example, LL).
   - Embed the watermark in DCT coefficients.
   - Apply inverse DCT and then inverse DWT.
2. *Strengths:*
   - Enhanced robustness and imperceptibility.
   - Resistance to a broader range of attacks.
3. *Limitations:* Increased complexity and processing time.

6.CHALLENGES

Despite significant progress, digital image watermarking, especially using transform-domain techniques, still struggles with several key challenges that limit its widespread use and effectiveness:

1. *Trade-off Between Imperceptibility and Robustness*

Boosting robustness often results in visible distortion in the image. On the other hand, improving imperceptibility can weaken the watermark's resistance to attacks. Finding the right balance remains a constant challenge.

2. *Vulnerability to Geometric Attacks*

Transform-domain methods, like DCT and DWT, are often sensitive to rotation, scaling, cropping, or affine transformations. While techniques like DFT or hybrid approaches provide partial solutions, achieving full invariance is tough.

3. *High Computational Complexity*

Complex algorithms, such as multi-level DWT-SVD, need a lot of processing time and memory, making them unsuitable for real-time or resource-limited applications like IoT or embedded systems.

4. *Lack of Standardization*

There is no universal standard for watermark embedding, detection, or evaluation. This leads to inconsistency in benchmarking and comparing different methods.

5. *Fragility to Combined Attacks*

A single watermarking method may stand strong against one type of attack, like JPEG compression, but be weak against

another, such as median filtering with rotation. Robustness under combined or unknown attack scenarios is still an issue.

6. *Security and Authentication Issues*

Attackers can forge, remove, or tamper with watermarks using signal processing or machine learning tools. Ensuring tamper detection and secure embedding without degrading image quality is still a developing area.

7.SOLUTIONS

1. *Balancing Robustness and Imperceptibility*

- *Problem:*

  Improving robustness might lower image quality, while enhancing imperceptibility can make watermarking less resilient.

- *Solutions:*

  a. Adaptive Embedding Strength: Adjust watermark strength based on local image features like texture complexity or edge density.

  b. Human Visual System (HVS) Models: Place watermarks in areas that the human eye finds less sensitive, using models that replicate how we see contrast and brightness.

  c. Multi-domain Watermarking: Use both spatial and frequency domain embedding methods, such as DWT-DCT or DWT-SVD, to balance quality and robustness.

2. *Countering Geometric Attacks*

- *Problem:*

  Transform-domain techniques can be affected by rotation, scaling, translation (RST), and cropping.

- *Solutions:*

  a. Invariant Feature Point Detection: Employ SIFT, SURF, or Harris corner detectors to embed watermarks in locations that withstand geometric changes.

  b. Template Embedding: Add synchronization patterns to identify and fix geometric distortions before extracting the watermark.

  c. Log-Polar Mapping + DFT: These transforms change geometric transformations into shifts, enhancing the watermark's resistance to RST attacks.

3. *Reducing Computational Complexity*

- *Problem:*

  Complicated watermarking methods are not practical for real-time or embedded applications.

- *Solutions:*

  a. Lightweight Transform Selection: Choose faster transforms like DCT or integer-based wavelet transforms instead of heavier ones such as SVD or FFT.

  b. Parallel Processing: Use GPUs or FPGA-based accelerators for watermarking to cut down processing time.

Selective Embedding: Only add watermarks to chosen blocks of interest to reduce processing demands

8.FUTURE SCOPE

1. *Deep Learning-Based Watermarking*

Future Direction: Combine deep learning techniques like CNNs, GANs, and autoencoders to create smart watermarking systems.

- Learn the best ways to embed and extract watermarks.
- Improve strength through adversarial training.
- Adjust to different image content and types of attacks.

2. *Robust Watermarking for Emerging Media*

Future Direction: Expand watermarking techniques to support new types of content such as:

- 3D models
- Medical images (DICOM)
- Augmented and Virtual Reality (AR/VR) content
- Holographic displays and 360° images

3. *Real-Time and Resource-Constrained Applications*

Future Direction: Develop lightweight, real-time watermarking solutions for:

- IoT devices
- Surveillance systems
- Mobile and embedded platforms

4. *Multi-Watermarking and Layered Embedding*

Future Direction: Embed multiple watermarks for various applications:

- Ownership verification
- Tamper detection

- Content tracking

Fig 3: Future Applications of Watermarking

9. CONCLUSIONS

Digital image watermarking has become an essential tool for protecting intellectual property, verifying digital content, and preventing unauthorized distribution in the digital age. Among various techniques, transform-domain methods like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), and hybrid combinations have shown to be especially effective because of their strength and compatibility with compression standards such as JPEG.

This review has covered the basics of digital watermarking, important requirements such as invisibility and strength, and the key role of transform-domain techniques in creating strong watermarking systems. We have looked at different transform-based methods, their advantages, disadvantages, and how well they perform against various types of attacks, including geometric changes, filtering, and compression-related distortions.

Additionally, the paper has emphasized the need for strong evaluation metrics, discussed common issues that current watermarking systems face, and suggested practical ways to enhance performance regarding security, speed, and flexibility. The review also pointed out future research directions, focusing on AI-based watermarking, watermarking for new media formats, integration with blockchain, and the importance of creating standard evaluation methods.

In summary, while current transform-domain watermarking techniques provide a good starting point, there is still much room for improvement in real-world applications, scalability, and resistance to complicated attack scenarios. Future watermarking systems will probably become more intelligent, combined with various techniques, and more closely linked to changing digital environments, offering better protection, verification, and tracking of digital content.

REFERENCES

[1]. Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673, 1687, 1997.

[2]. Barni, M., Bartolini, F., and Piva, A. "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking," IEEE Transactions on Image Processing, vol. 10, no. 5, pp. 783, 791, 2001.

[3]. Liu, R., & Tan, T. "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121-128, 2002.

[4]. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom "Digital Watermarking and Steganography," Morgan Kaufmann, 2nd Edition, 2007.

[5]. Christian S. Collberg and Jasvir Nagra "Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection," Addison-Wesley, 2009.

[6]. Frank Y. Shih "Digital Watermarking and Steganography: Fundamentals and Techniques," CRC Press, 2007.