RESEARCH PAPER

Intellectual Property Right Protection of Image Data Using DCT and Spread Spectrum-Based Watermarking

Dr. Heba Saad Alsaleh[1], Prof. Dr. Deevanshu Shrivastava[2]

[1] Assistant Professor of Law, Gulf University, Bahrain. ORCID: 0009-0002-8859-2399. Email: dr.hebaalsaleh@gulfuniversity.edu.bh

[2] Professor of Law, National University of Study and Research in Law, Ranchi, India. ORCID: 009-0007-3016-3440. Email: deevanshu.shrivastava@nusrlranchi.ac.in

Received: 20th Feb, 2026 | **Revised:** 4th Mar, 2026 | **Accepted:** 25th Mar, 2026 | **Available Online:** 10th Apr, 2026

ABSTRACT

The exponential growth of digital imaging technologies has fundamentally altered how visual content is produced, disseminated, and consumed. While this transformation has enabled greater access and innovation, it has also intensified concerns surrounding unauthorized reproduction, distribution, and misuse of digital images. Traditional intellectual property enforcement mechanisms have struggled to adapt to the scale and speed of digital environments. In this context, digital watermarking has emerged as a critical technological tool for safeguarding ownership rights. This chapter examines the use of Discrete Cosine Transform (DCT) and spread spectrum-based watermarking techniques as effective methods for protecting image data. It explores the theoretical underpinnings of these approaches, their practical implementation, robustness against common attacks, and their legal relevance. The chapter also situates these techniques within broader intellectual property frameworks, incorporates a deeper literature review, and critically evaluates their limitations and future potential. By bridging technical and legal perspectives, this study demonstrates how watermarking can play a central role in strengthening digital copyright protection.

Keywords: Digital watermarking, DCT, spread spectrum, intellectual property rights, copyright protection, image security.

How to cite this article: Alsaleh HS, Shrivastava D. Intellectual Property Right Protection of Image Data Using DCT and Spread Spectrum-Based Watermarking. Int J Drug Deliv Technol. 2026;16(30s):61-74. DOI: 10.25258/ijddt.16.30s.6

Source of support: Nil.

Conflict of interest: The authors declare no conflict of interest.

1. Introduction

Digital images have moved from being static artefacts to dynamic assets that circulate continuously across platforms. A photograph taken on a phone can be uploaded, reshared, edited, and repurposed within minutes. For creators, this reach is valuable. For rights protection, it creates a persistent vulnerability. The same mechanisms that enable visibility also enable uncredited reuse and commercial exploitation.

Here's the tension at the core of the problem. Copyright law assumes that ownership can be asserted, proven, and enforced. Digital networks, on the other hand, are built for frictionless copying and distribution. Once an image is released into this environment, it becomes difficult to distinguish the original from its copies. Attribution can be stripped, metadata can be altered, and the image can be embedded into derivative works with little trace of the source.

Enforcement through traditional legal routes is often reactive and slow. Takedown procedures, platform policies, and cross-border litigation provide some relief, but they rarely restore control to the creator in a meaningful way. By the time a claim is resolved, the image may have already reached a wide audience, reducing both its economic value and the practical benefit of enforcement.

This is why technological protection measures have become central to contemporary copyright strategy. Digital watermarking, in particular, introduces a shift in approach. Instead of relying entirely on external enforcement, it embeds identifying information within the image itself. The image carries a persistent marker of ownership that can be detected even after distribution and modification.

Among the available watermarking techniques, those based on the Discrete Cosine Transform (DCT) combined with spread spectrum methods are especially relevant. They align with widely used compression standards, distribute watermark information in a resilient manner, and maintain visual quality. This

combination makes them suitable for real-world deployment across platforms that routinely compress and transform images.

The objective of this chapter is to examine how DCT and spread spectrum-based watermarking can be used as a practical tool for intellectual property protection. It brings together technical design, performance considerations, and legal relevance. The aim is not just to explain how these techniques work, but to show how they fit into a broader framework of rights protection in digital environments.

2. Intellectual Property Rights and Digital Images

Intellectual Property Rights are intended to ensure that creators retain control over the use of their work. In the context of digital images, copyright protection arises automatically upon creation, without the need for formal registration. The author is granted exclusive rights over reproduction, distribution, communication to the public, and adaptation.

In theory, this framework is comprehensive. In practice, digital environments introduce structural challenges that weaken its effectiveness.

2.1 Structural Challenges in Digital Environments

Digital images differ from traditional media in several important ways.

First, replication is perfect. A copied image is indistinguishable from the original. There is no degradation that might signal duplication. This makes it difficult to establish provenance based on the artefact itself.

Second, dissemination is instantaneous and global. Platforms allow users to share content across jurisdictions without friction. This raises questions about applicable law, enforcement mechanisms, and jurisdictional competence.

Third, attribution is fragile. Metadata containing author information can be removed intentionally or lost during platform processing. Once attribution disappears, reconnecting the image to its creator becomes difficult.

Fourth, users can remain anonymous or operate under pseudonyms. This complicates enforcement, as identifying the infringer becomes a separate and often resource-intensive task.

These factors collectively undermine the practical enforceability of copyright. The legal right exists, but the ability to assert it effectively is constrained.

2.2 Technological Protection Measures and Their Role

To address these gaps, technological protection measures have been developed. These include encryption, access control systems, and watermarking.

Encryption restricts access to content, making it suitable for controlled distribution environments. However, it is less useful in open ecosystems where visibility is necessary, such as social media or public galleries.

Watermarking operates differently. It does not prevent access. Instead, it embeds information within the content itself. This allows the image to circulate freely while retaining a traceable link to its origin.

From a rights management perspective, this is a significant advantage. It enables creators to maintain a level of control without limiting exposure. It also creates a technological layer that complements legal protection.

2.3 Evidentiary Value of Embedded Information

One of the most important functions of watermarking is its evidentiary value. In a dispute, the ability to demonstrate ownership is critical. Traditional evidence may include original files, timestamps, or witness testimony. These forms of evidence can be challenged or may not always be available.

A robust watermark provides embedded evidence that is directly linked to the image. If the watermark can be reliably detected and verified, it strengthens the claim of authorship. It can also indicate that the alleged infringer had access to the original work.

However, for watermarking to be legally persuasive, it must satisfy certain conditions. The embedding process must be consistent and reproducible. The detection method must be reliable. The system must be resistant to tampering. Without these qualities, the evidentiary value of the watermark may be questioned.

2.4 Indian Legal Context

In India, the Copyright Act, 1957 governs the protection of artistic works, including photographs and digital images. The Act recognises the rights of authors and provides remedies for infringement, including injunctions and damages.

At the same time, the Information Technology Act, 2000 and related rules address issues of digital evidence and electronic records. Courts have increasingly accepted electronic evidence, subject to conditions of authenticity and integrity.

Watermarking fits into this framework as a supporting mechanism. It does not replace legal proof but strengthens it. By embedding ownership information within the image, it provides an additional layer of verification that can be presented in legal proceedings.

2.5 Practical Implications for Creators and Platforms

For creators, watermarking offers a way to assert ownership without altering the visual appeal of their

work. It can be integrated into workflows at the point of creation or distribution.

For platforms, watermarking can support content management systems, help track distribution, and assist in resolving disputes. Stock image providers, for instance, often rely on watermarking to protect their catalogues and monitor usage.

What emerges is a hybrid model of protection. Legal rights provide the foundation. Technological tools like watermarking enhance enforceability. Together, they offer a more resilient approach to protecting digital images in a networked environment.

3. Fundamentals of Digital Watermarking

Digital watermarking is the process of embedding auxiliary information into a host image in a manner that is largely imperceptible to the human eye but can be reliably detected or extracted using computational techniques. At its core, watermarking sits at the intersection of signal processing, information theory, and security. It is not just about hiding information. It is about doing so in a way that survives transformation, manipulation, and potential adversarial removal.

3.1 Conceptual Framework

A watermarking system can be understood through three primary components:

- **Host signal (I):** The original image into which data is embedded
- **Watermark signal (W):** The information to be embedded, which may represent ownership, authentication data, or tracking information
- **Embedding function (E):** The algorithm that inserts W into I to produce a watermarked image I'

Mathematically, this can be expressed as:

$I' = E(I, W, K)$

where K represents a secret key used to control embedding and detection.

At the detection stage, a corresponding function D is used:

$W' = D(I', K)$

The goal is to ensure that W' closely matches W, even after the image has undergone transformations.

3.2 Design Requirements and Trade-offs

Designing a watermarking system involves balancing several competing requirements.

Imperceptibility requires that the watermark does not degrade image quality in a noticeable way. This is typically evaluated using perceptual metrics such as PSNR or structural similarity.

Robustness ensures that the watermark remains detectable after common image processing operations such as compression, filtering, resizing, and noise addition.

Capacity refers to the amount of information that can be embedded. Higher capacity often comes at the cost of reduced imperceptibility or robustness.

Security ensures that unauthorized users cannot detect, extract, or modify the watermark. This is usually achieved through key-based embedding and pseudo-random sequences.

What this really means is that watermarking is always a balancing act. Increasing embedding strength improves robustness but risks visible distortion. Reducing it preserves quality but weakens resilience.

3.3 Types of Watermarks

Watermarks can be categorised based on visibility, robustness, and function.

Visible watermarks are directly perceptible, such as logos or text overlays. They act as a deterrent but can often be removed through editing.

Invisible watermarks are embedded within the image data. They are not visible but can be detected algorithmically. These are more suitable for forensic and legal purposes.

Fragile watermarks are designed to break under modification. They are useful for tamper detection and authentication.

Robust watermarks are designed to survive processing and attacks. These are the focus of copyright protection systems.

Semi-fragile watermarks strike a balance. They tolerate benign transformations like compression but break under malicious modification.

3.4 Spatial Domain Techniques

Spatial domain watermarking modifies pixel values directly. A common method is Least Significant Bit (LSB) substitution, where watermark bits replace the least significant bits of pixel intensities.

While these methods are simple and computationally efficient, they are highly vulnerable to attacks. Even minor image processing operations can destroy the watermark.

For example, basic compression or noise addition can alter pixel values enough to remove embedded information. This limits the applicability of spatial domain methods in robust copyright protection.

3.5 Frequency Domain Techniques

Frequency domain watermarking involves transforming the image into a different representation before embedding the watermark. Common transforms include:

- Discrete Cosine Transform (DCT)
- Discrete Wavelet Transform (DWT)

- Fourier Transform (FT)

These methods embed watermark data into frequency coefficients rather than raw pixels.

The advantage here is structural alignment. Many image processing operations, especially compression, operate in the frequency domain. By embedding the watermark in this domain, the system becomes inherently more resistant to such operations.

Frequency domain techniques also allow selective embedding. Instead of modifying the entire image uniformly, specific frequency bands can be targeted to optimise imperceptibility and robustness.

3.6 Blind, Semi-Blind, and Non-Blind Watermarking

Watermark detection systems can be classified based on the information required during extraction.

Non-blind watermarking requires access to the original image during detection. While accurate, it is impractical for many real-world applications.

Semi-blind watermarking requires partial information, such as the watermark or key.

Blind watermarking requires only the key. It does not rely on the original image, making it more suitable for large-scale deployment.

DCT spread spectrum watermarking is often implemented as a blind or semi-blind system, enhancing its usability in distributed environments.

3.7 Attacks on Watermarking Systems

Understanding potential attacks is essential for designing robust systems. Attacks can be classified as:

Signal processing attacks: compression, noise addition, filtering

Geometric attacks: rotation, scaling, translation

Collusion attacks: combining multiple copies to remove watermark

Forgery attacks: inserting a false watermark

A strong watermarking system must anticipate these threats and incorporate resilience at the design stage.

3.8 Evaluation Metrics

Performance evaluation is critical to assessing watermarking systems.

Peak Signal-to-Noise Ratio (PSNR): Measures the quality of the watermarked image compared to the original. Higher values indicate better imperceptibility.

Structural Similarity Index (SSIM): Evaluates perceptual similarity based on luminance, contrast, and structure.

Normalized Correlation (NC): Measures similarity between original and extracted watermark. Values close to 1 indicate successful detection.

Bit Error Rate (BER): Indicates the proportion of incorrectly extracted bits.

These metrics provide a quantitative basis for comparing different watermarking techniques.

3.9 Practical Workflow Integration

In real-world applications, watermarking is rarely a standalone process. It is integrated into broader content workflows.

For instance, a photographer may embed a watermark at the point of export. A platform may apply additional watermarking during upload. Detection systems may operate at scale to identify unauthorized use across the web.

This layered approach increases effectiveness. Even if one watermark is removed, others may remain.

3.10 Relevance to DCT and Spread Spectrum Techniques

The concepts discussed in this section form the foundation for understanding DCT and spread spectrum watermarking. Frequency domain embedding addresses robustness, while spread spectrum techniques address distribution and security.

When combined, these approaches create a system that is not only technically sound but also aligned with real-world requirements of copyright protection.

4. Discrete Cosine Transform (DCT) in Depth

The Discrete Cosine Transform is one of the most widely used mathematical tools in image processing. Its importance comes from a simple but powerful idea: it represents an image not in terms of pixel intensities, but in terms of frequency components. This shift in representation allows more efficient manipulation, compression, and, importantly, watermark embedding.

4.1 Intuition Behind DCT

To understand DCT, it helps to think of an image as a combination of patterns. Some patterns change slowly across the image, such as smooth backgrounds. Others change rapidly, such as edges and textures. DCT separates these patterns into frequency components.

Low-frequency components capture the general structure of the image. High-frequency components capture fine details and abrupt changes. By isolating these components, DCT allows selective modification of the image in a controlled manner.

This is precisely what makes it suitable for watermarking. Instead of altering pixels directly, we can modify specific frequency components in a way that is less noticeable and more robust.

4.2 Mathematical Formulation

The two-dimensional DCT for an N × N image block is defined as:

$$C(u,v) = (2/N)\ \alpha(u)\alpha(v)\ \Sigma\Sigma\ f(x,y)\ \cos[(2x+1)u\pi/2N]\ \cos[(2y+1)v\pi/2N]$$

where:

- f(x,y) represents pixel values
- C(u,v) represents DCT coefficients
- α(u), α(v) are normalization factors

The inverse DCT reconstructs the image from these coefficients. The transformation is energy-preserving, meaning that no information is lost during the transform itself.

4.3 Block-Based Processing and JPEG Relevance

In practical applications, images are divided into blocks, typically 8 × 8 pixels. Each block is independently transformed using DCT.

This block-based approach is not arbitrary. It aligns directly with JPEG compression, where images are also processed in 8 × 8 blocks. This alignment is critical because it ensures that watermarking operates within the same framework as compression.

What this really means is that a watermark embedded in DCT coefficients is more likely to survive compression, since it is embedded in the same domain where compression decisions are made.

4.4 Energy Compaction and Its Importance

One of the defining properties of DCT is energy compaction. Most of the signal energy is concentrated in a small number of low-frequency coefficients.

This has two implications:

- Modifying low-frequency coefficients can significantly affect image quality
- High-frequency coefficients contain less perceptually important information

However, watermarking does not simply choose between low and high frequencies. Instead, it targets mid-frequency coefficients, which provide a balance between visibility and robustness.

4.5 Frequency Coefficient Regions

Within each DCT block, coefficients can be divided into three regions:

Low-frequency region: Located near the top-left corner of the coefficient matrix. These coefficients determine overall brightness and smooth variations.

Mid-frequency region: Located between low and high frequencies. These coefficients influence textures and moderate variations.

High-frequency region: Located toward the bottom-right corner. These coefficients capture edges and fine details.

Watermarking strategies typically focus on mid-frequency coefficients. This ensures that the watermark is not easily removed by compression (which often targets high-frequency components) while also avoiding visible distortion.

4.6 Embedding Strategies in DCT Domain

Several approaches exist for embedding watermark data into DCT coefficients.

Coefficient modification: Selected coefficients are slightly altered based on watermark bits. For example, one coefficient may be increased to represent a binary 1 and decreased to represent a binary 0.

Quantization-based methods: Watermark information is embedded by modifying quantization indices. These methods are often more robust to compression.

Differential embedding: Instead of modifying absolute values, relationships between coefficients are altered. This improves resistance to uniform changes such as brightness adjustment.

Each method involves trade-offs between robustness, imperceptibility, and computational complexity.

4.7 Imperceptibility Considerations

A key requirement is that watermark embedding should not degrade visual quality. Human vision is less sensitive to certain frequency changes, particularly in textured regions.

DCT-based watermarking exploits this property by embedding information in areas where changes are less perceptible. This ensures that the watermark remains invisible under normal viewing conditions.

Perceptual models can also be incorporated to adapt embedding strength based on local image characteristics.

4.8 Robustness to Compression and Noise

DCT-based watermarking is inherently robust to JPEG compression. Since both processes operate in the frequency domain, carefully embedded watermark data is less likely to be discarded.

Similarly, spreading watermark information across multiple coefficients increases resistance to noise. Even if some coefficients are altered, the watermark can still be detected through redundancy.

4.9 Limitations of DCT-Based Approaches

Despite its advantages, DCT-based watermarking has limitations.

- Block-based processing can introduce blocking artifacts if embedding is not carefully controlled
- Geometric transformations can disrupt coefficient alignment
- Fixed block size may not adapt well to all image types

These limitations are often addressed by combining DCT with other techniques, such as spread spectrum or wavelet transforms.

4.10 Role of DCT in Hybrid Watermarking Systems

In hybrid systems, DCT serves as the structural foundation. It provides access to frequency components and enables controlled embedding.

When combined with spread spectrum techniques, DCT allows watermark information to be distributed across multiple coefficients in a secure and robust manner.

This combination enhances both resilience and security, making it suitable for real-world intellectual property protection scenarios.

5. Spread Spectrum Watermarking in Depth

Spread spectrum watermarking borrows its core idea from communication theory. In wireless communication, spread spectrum techniques are used to transmit signals over a wide frequency band in a way that makes them resistant to interference, noise, and interception. When this idea is applied to watermarking, the watermark signal is not confined to a single location. Instead, it is distributed across many components of the host image.

This distribution is what gives spread spectrum watermarking its strength. Rather than relying on a few modified coefficients, the watermark is embedded in a dispersed and redundant manner, making it significantly harder to remove or destroy without degrading the entire image.

5.1 Conceptual Basis

At a conceptual level, spread spectrum watermarking treats the watermark as a low-power noise-like signal that is added to the host image. Because it resembles noise, it is difficult to distinguish or isolate without knowledge of the embedding key.

The key idea is simple: if the watermark is spread widely enough, even partial loss of information will not eliminate it completely. Detection then becomes a matter of identifying a statistical pattern rather than recovering exact data.

5.2 Mathematical Model

The embedding process can be expressed as:

$I' = I + kW$

where:

- I is the original image or its transformed representation
- W is the watermark sequence
- k is the embedding strength factor
- I' is the watermarked image

The watermark sequence W is typically generated as a pseudo-random sequence with values such as +1 and -1. This ensures that the watermark behaves like noise while still being reproducible using a secret key.

5.3 Role of the Secret Key

Security in spread spectrum watermarking relies heavily on the use of a secret key. The key is used to generate the pseudo-random sequence that determines where and how the watermark is embedded.

Without access to this key, an attacker cannot easily detect or remove the watermark. Even if the presence of a watermark is suspected, extracting it without the correct sequence becomes computationally difficult.

This key-based approach introduces a cryptographic dimension to watermarking, enhancing its suitability for intellectual property protection.

5.4 Embedding Strategies

There are multiple ways to implement spread spectrum embedding.

Additive embedding: The watermark is directly added to the host signal, as shown in the basic model. This is simple and widely used.

Multiplicative embedding: The watermark modifies the host signal proportionally. This can improve robustness under certain conditions.

Adaptive embedding: The embedding strength k is varied based on local image characteristics. For example, stronger embedding may be applied in textured regions where distortion is less noticeable.

Each approach offers a different balance between robustness and imperceptibility.

5.5 Detection and Correlation Analysis

Detection in spread spectrum watermarking is typically based on correlation. The detector computes the similarity between the suspected image and the pseudo-random watermark sequence.

The correlation value can be expressed as:

$\rho = \Sigma (I' \times W)$

If the computed correlation exceeds a predefined threshold, the watermark is considered present.

This approach has several advantages:

- It does not require exact reconstruction of the watermark
- It is robust to partial data loss
- It supports blind detection when the original image is unavailable

The threshold value plays a critical role. If set too low, false positives may occur. If set too high, genuine watermarks may be missed.

5.6 Robustness Characteristics

Spread spectrum watermarking is inherently robust due to its distributed nature.

Resistance to noise: Since the watermark is spread across many components, random noise affects only a portion of it.

Resistance to cropping: Even if parts of the image are removed, the remaining portions may still contain enough watermark information for detection.

Resistance to compression: When combined with frequency domain techniques like DCT, spread spectrum watermarking can survive lossy compression. This robustness makes it particularly suitable for real-world applications where images undergo multiple transformations.

5.7 Vulnerabilities and Limitations

Despite its strengths, spread spectrum watermarking is not immune to attack.

Collusion attacks: If multiple watermarked copies are available, attackers may combine them to estimate and remove the watermark.

Desynchronization attacks: Geometric transformations such as rotation or scaling can disrupt alignment between the watermark and detection sequence.

Estimation attacks: Sophisticated attackers may attempt to estimate the watermark signal statistically and subtract it.

These challenges highlight the need for combining spread spectrum with other techniques, such as DCT, to enhance robustness.

5.8 Trade-offs in Parameter Selection

The effectiveness of spread spectrum watermarking depends on parameter choices.

- Higher embedding strength improves robustness but increases visibility
- Longer watermark sequences improve detection reliability but increase computational cost
- Choice of threshold affects detection accuracy

Careful tuning is required to achieve an optimal balance.

5.9 Integration with Frequency Domain Techniques

Spread spectrum watermarking is often implemented in the frequency domain rather than directly on pixel values. This improves robustness and aligns with image processing operations.

When applied in the DCT domain, the watermark is embedded into selected frequency coefficients. This combination leverages both distribution (spread spectrum) and structural embedding (DCT).

5.10 Relevance to Intellectual Property Protection

From an intellectual property perspective, spread spectrum watermarking offers several advantages.

- It provides persistent ownership information
- It is difficult to remove without degrading the image
- It supports large-scale automated detection

What this really means is that spread spectrum watermarking transforms the watermark from a fragile tag into a resilient signal embedded within the image itself.

When combined with DCT, it forms a robust framework for protecting digital images in environments where copying and modification are inevitable.

6. Hybrid DCT and Spread Spectrum Framework

The integration of Discrete Cosine Transform (DCT) with spread spectrum watermarking represents a significant advancement in digital watermarking design. Individually, each technique addresses specific challenges. DCT provides a structured and perceptually aligned domain for embedding, while spread spectrum ensures distribution and robustness. When combined, they form a system that is both resilient and practical for real-world deployment.

6.1 Rationale for Hybridisation

Pure DCT-based watermarking can achieve good imperceptibility and moderate robustness, but it may be vulnerable to targeted attacks that manipulate specific coefficients. On the other hand, spread spectrum techniques offer strong robustness but may lack structural alignment with image compression standards when used in isolation.

The hybrid approach leverages the strengths of both methods. DCT provides access to frequency components that are stable under compression, while spread spectrum distributes the watermark across these components, increasing resistance to localized and global attacks.

6.2 Detailed Embedding Algorithm

The embedding process in a hybrid system typically involves the following steps:

1. **Pre-processing:** The input image is optionally converted to grayscale or a suitable colour space such as YCbCr. The luminance component is often selected for embedding, as it has greater perceptual importance.
2. **Block segmentation:** The image is divided into non-overlapping 8×8 blocks.
3. **DCT transformation:** Each block undergoes DCT to obtain frequency coefficients.
4. **Coefficient selection:** Mid-frequency coefficients are selected based on a predefined pattern or key.
5. **Watermark generation:** A pseudo-random sequence is generated using a secret key.
6. **Embedding operation:** The watermark sequence is embedded into selected coefficients using the spread spectrum model:

$C' = C + kW$

7. **Inverse DCT:** The modified coefficients are transformed back to the spatial domain.
8. **Reconstruction:** All blocks are combined to form the final watermarked image.

This process ensures that the watermark is both imperceptible and distributed across the image.

6.3 Extraction and Detection Algorithm

The extraction process mirrors the embedding process but focuses on detection rather than reconstruction.

1. Apply DCT to the received image
2. Extract the same set of coefficients using the key
3. Generate the pseudo-random sequence
4. Compute correlation between extracted data and watermark sequence
5. Compare with threshold to determine presence

This process can be implemented as a blind detection system, meaning that the original image is not required.

6.4 Parameter Selection and Optimisation

The performance of the hybrid system depends heavily on parameter choices.

- **Embedding strength (k):** Higher values improve robustness but risk visible distortion
- **Coefficient selection pattern:** Determines resistance to compression and filtering
- **Watermark length:** Affects detection reliability
- **Threshold value:** Influences false positive and false negative rates

Optimisation often involves empirical testing across different image types and attack scenarios.

6.5 Performance Evaluation

Hybrid systems are typically evaluated using multiple metrics.

PSNR: Measures visual quality. Values above 35 dB are generally considered acceptable.

NC: Measures similarity between original and extracted watermark. Values close to 1 indicate strong detection.

Robustness tests: Evaluate performance under compression, noise, cropping, and filtering.

Experimental studies consistently show that hybrid DCT-spread spectrum methods outperform standalone approaches in terms of robustness.

6.6 Advantages of the Hybrid Approach

- Improved robustness against compression and noise
- Better imperceptibility through frequency domain embedding
- Enhanced security through key-based spread spectrum
- Compatibility with existing image processing standards

These advantages make the hybrid approach particularly suitable for intellectual property protection in digital environments.

6.7 Limitations of Hybrid Systems

Despite their strengths, hybrid systems are not without challenges.

- Increased computational complexity
- Sensitivity to geometric transformations
- Need for careful parameter tuning

Addressing these limitations often requires additional techniques such as synchronization patterns or geometric correction algorithms.

7. Robustness and Attack Analysis

Robustness is one of the most critical requirements for any watermarking system. A watermark that cannot survive common image processing operations is of limited practical value. This section examines how hybrid DCT and spread spectrum watermarking performs under various attack scenarios.

7.1 Classification of Attacks

Attacks on watermarking systems can be broadly classified into the following categories:

Signal processing attacks: These include operations such as compression, noise addition, filtering, and sharpening.

Geometric attacks: These involve spatial transformations such as rotation, scaling, translation, and cropping.

Intentional removal attacks: These are designed specifically to eliminate or weaken the watermark.

Collusion attacks: Multiple watermarked copies are combined to estimate and remove the watermark.

7.2 Performance Under Compression

JPEG compression is one of the most common transformations applied to images. Since DCT is also used in JPEG, watermarking in this domain provides inherent resistance.

Hybrid systems maintain high detection accuracy even at moderate compression levels. This is because watermark data is embedded in coefficients that are less likely to be discarded.

7.3 Resistance to Noise and Filtering

Noise addition affects pixel values randomly. However, spread spectrum watermarking distributes information across multiple coefficients, ensuring that the watermark is not entirely lost.

Filtering operations, such as smoothing or sharpening, may alter certain frequencies but typically do not remove the watermark completely.

7.4 Cropping and Partial Data Loss

Cropping removes portions of the image. In a localized watermarking system, this could eliminate the watermark entirely. However, spread spectrum distribution ensures that watermark information remains in multiple regions.

Even after partial cropping, detection is often still possible.

7.5 Geometric Transformations

Geometric transformations present a greater challenge. Rotation, scaling, and translation can disrupt the alignment between the embedded watermark and the detection sequence.

This desynchronization reduces correlation and may lead to detection failure.

Solutions include:

- Embedding synchronization patterns
- Using invariant features
- Applying geometric correction algorithms

7.6 Collusion and Estimation Attacks

In collusion attacks, an attacker uses multiple watermarked versions of the same image to estimate the watermark signal. By averaging these images, the watermark can be weakened or removed.

Hybrid systems reduce this risk by using key-based pseudo-random sequences, making it difficult to isolate the watermark.

7.7 Experimental Observations

Empirical studies show that hybrid DCT spread spectrum watermarking maintains high NC values under:

- Moderate JPEG compression
- Gaussian noise
- Low to moderate filtering

Performance degrades under severe geometric distortion, highlighting an area for further research.

7.8 Practical Implications

From a practical standpoint, robustness determines whether watermarking is viable in real-world environments. Images shared online are routinely compressed, resized, and filtered.

A robust watermark ensures that ownership information persists despite these transformations.

7.9 Balancing Robustness and Imperceptibility

Increasing robustness often requires stronger embedding, which can affect image quality. The challenge lies in finding a balance where the watermark is both durable and invisible.

Hybrid DCT spread spectrum watermarking achieves this balance more effectively than many alternative methods.

8. Legal Relevance and Practical Application

Watermarking becomes meaningful for intellectual property protection only when it connects convincingly with legal standards of proof, attribution, and enforcement. This section examines how DCT and spread spectrum-based watermarking operates within legal frameworks and how it can be deployed in practice by creators, platforms, and enforcement agencies.

8.1 Watermarking as Evidence of Ownership

In copyright disputes, establishing authorship and priority is central. Traditional evidence includes original files, metadata, witness testimony, and publication records. Each of these can be challenged. Metadata may be stripped, timestamps can be manipulated, and access logs are not always available.

A robust, well-designed watermark adds a different kind of evidence. It is intrinsic to the image. If the watermark can be reliably detected and linked to a creator through a secure key or registry, it strengthens the evidentiary chain.

Courts generally assess digital evidence based on authenticity, integrity, and reliability. Watermarking contributes to all three:

- **Authenticity:** The watermark links the image to a specific creator or system
- **Integrity:** Persistence of the watermark across transformations suggests the image has not been fundamentally altered
- **Reliability:** A repeatable detection process supports consistency

8.2 Standards for Admissibility

For watermark evidence to be persuasive, certain technical conditions should be met:

- The embedding process must be documented and reproducible
- The detection algorithm must be verifiable and not ad hoc
- The key management process must be secure and auditable
- False positive rates must be demonstrably low

In practice, this means watermarking systems should maintain logs of embedding operations, keys used, and timestamps. This documentation can be critical in litigation.

8.3 Role in Infringement Analysis

Watermarking assists not only in proving ownership but also in demonstrating infringement.

If a watermarked image appears on an unauthorised platform, detection of the watermark can show that the infringing copy originated from the original work. In some cases, different watermark variants can be embedded for different licensees. This enables identification of the specific source of leakage.

This capability is particularly useful in cases involving stock image distribution, confidential visual assets, or pre-release promotional material.

8.4 Licensing, Tracking, and Rights Management

Beyond litigation, watermarking plays an operational role in managing rights.

- **License tracking:** Different watermarks can be assigned to different licensees
- **Usage monitoring:** Automated systems can scan the web for watermarked content
- **Royalty management:** Detection can inform compensation models based on usage

Platforms that host large volumes of images can integrate watermark detection into their moderation or compliance systems. This enables proactive identification of unauthorised content.

8.5 Indian Legal Context and Digital Evidence

Under the Copyright Act, 1957, photographs and digital images are protected as artistic works. Enforcement depends on proving ownership and unauthorised use.

The Information Technology Act, 2000 and the Indian Evidence Act (as amended to include electronic records) recognise the admissibility of digital evidence, subject to conditions such as authenticity and proper certification.

Watermarking complements this framework. It does not replace statutory proof requirements but strengthens them. When combined with proper documentation and certification, watermark detection can support claims of ownership and infringement.

8.6 Platform Responsibility and Intermediary Role

Digital platforms act as intermediaries in the dissemination of images. While they are often protected by safe harbour provisions, they are increasingly expected to implement reasonable measures to prevent infringement.

Watermarking can support these obligations. Platforms can:

- Detect known watermarks during upload
- Flag or block unauthorised content
- Assist rights holders in tracking misuse

This creates a collaborative enforcement model where both creators and platforms participate in protecting intellectual property.

8.7 Limitations from a Legal Perspective

Despite its value, watermarking is not definitive proof on its own. It can be challenged on several grounds:

- Allegations of false embedding or forgery
- Questions about reliability of detection methods
- Disputes over key ownership or control

Therefore, watermarking should be treated as part of a broader evidentiary framework rather than a standalone solution.

8.8 Practical Implementation Models

In real-world scenarios, watermarking is often implemented through layered systems:

- Creator-level embedding at the point of creation
- Platform-level watermarking during upload or distribution
- Monitoring systems that scan for watermarked content

This layered approach increases resilience and improves enforcement outcomes.

8.9 Strategic Value for Creators

For individual creators, watermarking provides a relatively low-cost method of asserting ownership. It can be integrated into existing workflows and does not require visible alteration of the image.

For organisations, it enables large-scale rights management, tracking, and enforcement. In both cases, it shifts the balance from reactive enforcement to proactive protection.

9. Bahraini legal perspective

From a Bahraini legal perspective, the protection of digital images through watermarking technologies such as DCT and spread spectrum methods fits coherently within the country's evolving intellectual property and digital evidence framework, though certain doctrinal and evidentiary nuances deserve closer attention. Bahrain's primary copyright regime is governed by Legislative Decree No. 22 of 2006 on the Protection of Copyright and Neighbouring Rights, as amended, which grants authors exclusive rights over reproduction, distribution, and communication to the public. Digital images fall squarely within "artistic works," and protection arises automatically upon creation, aligning with Berne Convention standards to which Bahrain is a party. What this really means is that, doctrinally, the legal right exists without friction; the challenge, much like in the Indian context discussed in the chapter, lies in enforceability within high-velocity digital environments.

Here's the critical point: Bahraini law does not explicitly regulate watermarking as a distinct legal category, but it implicitly accommodates it through two

adjacent legal domains—technological protection measures (TPMs) and electronic evidence. Under Article 39 of the Bahraini Copyright Law, the circumvention of effective technological protection measures is prohibited, particularly where such measures are designed to prevent or restrict unauthorized acts. While watermarking does not restrict access in the same way as encryption, courts can reasonably interpret robust watermarking systems as TPMs when they serve an authentication or rights-management function. This interpretive flexibility allows watermarking to acquire legal significance beyond its technical function.

On the evidentiary front, Bahrain's Law of Evidence in Civil and Commercial Matters (Legislative Decree No. 14 of 1996, as amended) and the Electronic Transactions Law (Legislative Decree No. 54 of 2018) provide the necessary infrastructure for admitting digital evidence. The latter explicitly recognises electronic records and signatures, provided their integrity and reliability can be established. This is where watermarking becomes strategically valuable. A properly implemented DCT-spread spectrum watermark, embedded at the point of creation and verifiable through a consistent detection algorithm, can strengthen claims of authorship by demonstrating continuity and integrity of the digital asset. As the chapter notes, watermarking enhances authenticity, integrity, and reliability—three pillars of admissibility in digital evidence regimes.

However, Bahraini courts, like many civil law jurisdictions, place significant weight on procedural certainty and expert validation. This introduces a practical constraint: watermark evidence will rarely be self-sufficient. It must be supported by technical documentation, expert testimony, and demonstrable chain-of-custody practices. Without these, opposing parties may challenge the possibility of false embedding, key compromise, or manipulation of detection processes. In other words, watermarking strengthens evidence, but does not conclusively establish it.

Another dimension worth noting is Bahrain's position as a regional financial and digital hub. With increasing reliance on digital platforms and cross-border data flows, enforcement often intersects with jurisdictional complexity. Watermarking, particularly when combined with licensing differentiation (unique watermark variants per licensee), can assist in tracing the source of infringement—an approach that is especially relevant for media, advertising, and fintech sectors operating in Bahrain.

That said, regulatory gaps remain. Bahrain lacks detailed guidelines or standards on watermarking practices, which may affect uniform judicial treatment. There is also limited jurisprudence directly addressing watermark-based claims, meaning outcomes will depend heavily on judicial discretion and expert interpretation.

In sum, the Bahraini legal framework is sufficiently flexible to accommodate advanced watermarking techniques as evidentiary and protective tools, but their effectiveness ultimately depends on how rigorously they are implemented and contextualised within broader legal proof structures.

9.2 Movement from implicit accommodation of watermarking technologies

From a Bahraini legal standpoint, the immediate priority is to move from implicit accommodation of watermarking technologies to explicit doctrinal recognition. At present, watermarking operates in a legal grey zone, indirectly supported through provisions on technological protection measures and electronic evidence. A more precise statutory clarification—either through amendment to Legislative Decree No. 22 of 2006 or through interpretive guidelines—would strengthen its legal status. Specifically, Bahrain could recognise robust digital watermarking as a form of rights management information (RMI), aligning with international standards under the WIPO Copyright Treaty. This would allow courts to treat the removal or alteration of watermarks as a standalone infringement, rather than forcing claimants to rely solely on traditional copyright violations.

Equally important is evidentiary standardisation. Bahraini courts already accept electronic records under the Electronic Transactions Law, but watermark-based claims would benefit from structured admissibility criteria. This includes requiring demonstrable reliability of the embedding algorithm, secure key management protocols, and documented workflows showing when and how the watermark was inserted. The introduction of judicial or regulatory guidance on digital forensic standards—possibly through the Ministry of Justice or specialised commercial courts—would reduce uncertainty and improve consistency in adjudication.

9.3 Need for strong Institutional Support

There is also a strong case for institutional integration. Bahrain could encourage platforms, stock image repositories, and media companies operating within its jurisdiction to adopt interoperable watermarking systems. This would not only facilitate enforcement but

also support automated detection of infringement. A regulatory sandbox approach, led by entities such as the Economic Development Board, could allow testing of watermarking technologies in controlled environments, particularly in sectors like fintech, digital media, and advertising where image misuse is commercially significant.

From an enforcement perspective, watermarking should be positioned as part of a layered compliance model rather than a standalone solution. Rights holders should combine watermarking with contractual safeguards, platform monitoring, and licensing audits. In parallel, Bahrain could explore integrating watermark detection into intermediary liability frameworks, encouraging platforms to take reasonable measures in identifying and flagging watermarked content used without authorization.

9.4 Hybrid Model

Finally, there is room for forward-looking reform. Bahrain is well placed to experiment with hybrid models that combine watermarking with blockchain-based registries for timestamping and ownership verification. While not yet doctrinally settled, such integration could address persistent challenges around provenance and cross-border enforcement. The broader point is this: Bahrain does not need to reinvent its legal framework—it needs to calibrate it to recognise that in digital environments, proof of ownership is increasingly embedded within the asset itself, not merely documented outside it.

10. Limitations and Critical Evaluation

While DCT and spread spectrum-based watermarking offer significant advantages, it is not a complete solution to the problem of digital image protection. A critical evaluation is necessary to understand its boundaries and practical constraints.

10.1 Trade-offs Between Core Requirements

Watermarking systems operate under inherent trade-offs.

- Increasing robustness often reduces imperceptibility
- Increasing capacity may weaken security
- Enhancing security may increase computational complexity

There is no universal configuration that optimises all parameters simultaneously. System design must therefore be context-specific.

10.2 Vulnerability to Advanced Attacks

Although hybrid watermarking is robust against common attacks, sophisticated adversaries can still pose challenges.

- **Geometric attacks** can disrupt synchronisation
- **Collusion attacks** can weaken watermark signals
- **Machine learning-based attacks** can potentially estimate and remove embedded patterns

These threats require continuous adaptation and improvement of watermarking techniques.

10.3 Computational and Implementation Costs

Hybrid watermarking systems involve multiple processing steps, including transformation, embedding, and detection. At scale, this can introduce computational overhead. For large platforms handling millions of images, efficiency becomes a critical factor. Real-time watermarking and detection require optimisation and resource allocation.

10.4 Lack of Standardisation

There is no universally accepted standard for watermarking implementation. Different systems use different embedding strategies, keys, and detection methods. This lack of standardisation creates interoperability issues. A watermark embedded by one system may not be detectable by another. Standardisation could improve adoption and legal acceptance.

10.5 Dependence on Key Management

The security of watermarking systems depends heavily on key management. If the embedding key is compromised, the watermark can be forged or removed.

This introduces a layer of operational risk that must be managed through secure storage, access control, and auditing.

10.6 Limitations in Legal Acceptance

While watermarking strengthens evidence, courts may still require additional proof. The technology must be explained in a way that is understandable and credible. Expert testimony may be required to establish reliability. This adds cost and complexity to litigation.

10.7 Ethical and Privacy Considerations

Watermarking raises certain ethical concerns.

- Embedding tracking information may raise privacy issues
- Use in surveillance contexts may be contested
- Lack of transparency in watermarking systems may affect user trust

Balancing protection with ethical considerations is essential.

10.8 Over-Reliance on Technology

There is a risk of viewing watermarking as a complete solution. In reality, it is one component of a broader protection strategy.

Effective intellectual property protection requires:

- Legal enforcement mechanisms
- Platform governance
- Awareness and compliance by users

Watermarking enhances these systems but does not replace them.

10.9 Scope for Improvement

Future improvements may address current limitations through:

- Adaptive and AI-driven watermarking
- Robust geometric-invariant techniques
- Integration with blockchain for ownership verification

These developments indicate that watermarking will continue to evolve as part of a larger technological ecosystem.

11. Conclusion

Protecting digital images in contemporary networks requires more than formal legal rights. It requires embedding resilience into the image itself. This chapter has examined how Discrete Cosine Transform (DCT) and spread spectrum-based watermarking together offer a technically grounded and practically viable approach to intellectual property protection. The analysis shows that DCT provides a perceptually aligned frequency domain where modifications can be made with minimal visual impact, while spread spectrum techniques ensure that watermark information is distributed, redundant, and difficult to remove. When combined, these methods address two central requirements of watermarking systems: imperceptibility and robustness.

At the same time, the discussion makes it clear that watermarking is not a complete solution. Its effectiveness depends on careful parameter selection, secure key management, and resistance to evolving attack models. From a legal perspective, watermarking strengthens evidentiary claims but does not replace the need for supporting documentation, procedural compliance, and judicial scrutiny. What emerges is a layered model of protection. Legal frameworks establish rights. Technological tools such as watermarking enhance enforceability. Platforms and intermediaries contribute through detection and compliance mechanisms. Together, these layers create a more resilient system for protecting digital images.

The broader implication is that intellectual property protection in digital environments is no longer purely a legal question. It is equally a design question. Systems must be built with protection in mind from the outset. DCT and spread spectrum watermarking represent one of the most effective ways of doing this today. As digital ecosystems continue to evolve, the role of such hybrid techniques will only become more central. They do not eliminate infringement, but they change the terms of engagement. Ownership becomes harder to erase, easier to prove, and more difficult to ignore.

References

1. Abd El-Latif, A. A., et al. (2025). *Digital forensics and cyber crime investigation: Recent advances and future directions*. Springer.
2. Agilandeeswari, L. (2023). Digital image and video watermarking: Methodologies, attacks, applications and future directions. *Multimedia Tools and Applications*.
3. Al-Khulaifi, A. (2021). "Digital Evidence and Its Admissibility in GCC Courts." *Journal of Law and Technology*.
4. Al-Saleh, Y. (2019). "Legal Framework of E-Commerce in Bahrain." *Arab Law Quarterly*, 33(2).
5. Anam, R. K. (2025). Robustness and imperceptibility analysis of hybrid spatial-frequency domain watermarking. *arXiv preprint*.
6. Arora, M., & Neetu. (2024). Legal framework of watermarks for copyright protection. *ShodhKosh Journal*.
7. Barni, M., Bartolini, F., & Piva, A. (2001). Improved wavelet-based watermarking through pixel-wise masking. *IEEE Transactions on Image Processing*, 10(5), 783–791.
8. Chaudhary, H., & Vishwakarma, V. P. (2024). Digital image watermarking: Recent trends and techniques—A survey. *Journal of Information & Optimization Sciences*.
9. Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673–1687.
10. Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). *Digital watermarking*. Morgan Kaufmann.
11. Gonzalez, R. C., & Woods, R. E. (2018). *Digital image processing* (4th ed.). Pearson.
12. Hartung, F., & Kutter, M. (1999). Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7), 1079–1107.

13. Indian Journal of Integrated Research in Law. (2024). Cross-jurisdictional analysis of digital watermarking and copyright protection.
14. Kundur, D., & Hatzinakos, D. (1999). Digital watermarking for telltale tamper proofing and authentication. *Proceedings of the IEEE*, 87(7), 1167–1180.
15. Langelaar, G. C., Setyawan, I., & Lagendijk, R. L. (2000). Watermarking digital image and video data. *IEEE Signal Processing Magazine*, 17(5), 20–46.
16. Ma, R., et al. (2022). Towards blind watermarking: Combining invertible and non-invertible mechanisms. *arXiv preprint*.
17. Moore, A. (2011). *Intellectual property and digital media*. Cambridge University Press.
18. Pagnotta, G., Hitaj, D., Hitaj, B., Perez-Cruz, F., & Mancini, L. V. (2022). TATTOOED: A robust deep neural network watermarking scheme based on spread-spectrum channel coding. *arXiv preprint*.
19. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A survey. *Proceedings of the IEEE*, 87(7), 1062–1078.
20. Piva, A., Barni, M., Bartolini, F., & Cappellini, V. (1997). DCT-based watermark recovering without resorting to the uncorrupted original image. *Proceedings of IEEE International Conference on Image Processing*.
21. Podilchuk, C. I., & Delp, E. J. (2001). Digital watermarking: Algorithms and applications. *IEEE Signal Processing Magazine*, 18(4), 33–46.
22. Reedy, P. (2023). Interpol review of digital evidence (2019–2022). *Forensic Science International*.
23. Swanson, M. D., Zhu, B., & Tewfik, A. H. (1998). Robust data hiding for images. *Proceedings of IEEE Digital Signal Processing Workshop*.
24. Voloshynovskiy, S., Pereira, S., Herrigel, A., Baumgaertner, F., & Pun, T. (2001). Generalized watermark attack based on watermark estimation and perceptual removal. *Proceedings of SPIE*.