Digital Image Watermarking

Sumit kumar
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institutte),
Greater Noida, India
sumitkumar22754@gmail.com
Tiwari Pratik Prakash
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institutte),
Greater Noida, India
tiwaripratik222@gmail.com
Tejaswi Kumar
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institutte),
Greater Noida, India
tejaswithakur840@gmail.com
Dr.Vikas Singhal
Professor & Head,Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institutte),
Greater Noida, India
profvikassinghal@gmail.com
Prof.Pawan Mishra
Department of Information Technology,
Greater Noida Institute of Technology (Engg. Institutte),
Greater Noida, India
pawan.it@gniot.net.in

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.11/Issue12/DCAE10083
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.11/Issue12/DCAE10083
Received:10,November 2024,Revised: 21,November 2024,Accepted: 30, November 2024, Published Online: 13,December 2024. https://www.ijirae.com/volumes/Vol11/iss-12/04.DCAE10083.pdf
Article Citation: Sumit,Tiwari,Tejaswi,Dr.Vikas,Prof.Pawan (2024), Digital Image Watermarking. IJIRAE:: International Journal of Innovative Research in Advanced Engineering, Volume 11, Issue 11 of 2024 pages 854-861
Doi:> https://doi.org/10.26562/ijirae.2024.v1112.04
BibTeX Key: Sumit@2024Digital

Abstract: In recent years, the field of digital image watermarking has garnered considerable attention due to its critical role in safeguarding broadcasting media. This technique serves as a powerful tool for ensuring the authenticity of content, monitoring media broadcasts, managing duplication control, and tackling a variety of related issues. Researchers have extensively examined digital image watermarking to address these challenges, making it a pivotal area of study. This paper delves into the concept of digital image watermarking, starting with an overview of its fundamental model. It then explores the primary requirements for effective watermarking systems and highlights their diverse applications. Additionally, the paper reviews key techniques and algorithms employed in watermarking, analyzes potential threats and attacks that such systems may face, and outlines the methods used to evaluate the performance and reliability of these systems.

Keywords: Digital Image Watermarking, Watermarking Models, Watermarking Attacks, Content authenticity, Monitoring, Copy control

I. INTRODUCTION

Digital watermarking is a technique used to embed information into digital content for purposes such as copyright protection, authentication, and broadcast monitoring. Watermarks can take various forms, including image, video, sound, text, and graphic watermarking. Image watermarking involves embedding watermarks into image files, while video watermarking often requires real-time detection under compression. Sound watermarking applies to audio files, such as internet-distributed tunes, and text watermarking uses the alignment, shape, or spacing of text elements to embed information. Graphic watermarking extends this concept to 2D or 3D graphics. Watermarks can be visible, clearly seen by the observer, or invisible, where modifications to pixel values are imperceptible. Dual watermarking combines both visible and invisible techniques for added security. The process of digital watermarking involves inputs such as the watermark, secret information, and a public or private key, with the output being the watermarked content. Alterations to this content, known as attacks, can compromise its integrity.

These attacks fall into several categories, including robustness or interference attacks, which degrade or remove watermarks through methods like cropping, JPEG compression, noise addition, quantization, rotation, and collusion (averaging multiple watermarked versions). [3] Presentation attacks involve extraction failures due to geometric transformations such as scaling, rotation, or aspect ratio changes, while counterfeiting attacks create fake data by replacing the original watermark. Geometric hacks, such as blanking rows or columns, cropping, or scaling, and signal processing attacks, including compression, noise addition, filtering, brightness adjustments, and scanning or printing, can also undermine watermarks. Additionally, collusion attacks involve combining multiple watermarked contents to reconstruct the original, cryptographic hacks attempt to break security using brute force methods to compute private keys, and protocol hacks exploit flaws in watermarking systems by inserting ambiguous or conflicting watermarks. By understanding the various forms of watermarking and the potential attacks, developers can design more robust systems to protect digital content and ensure its authenticity and security Followed by recognition, struggle with newer designs.

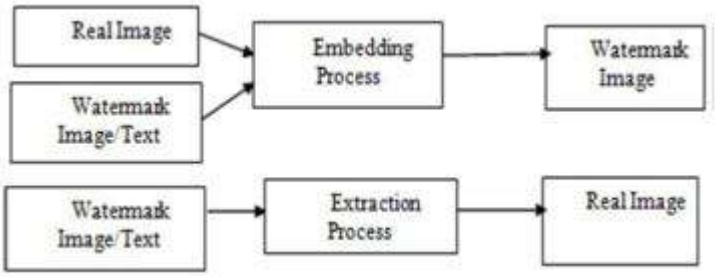

Figure 1: Watermarking Embedding and Extraction System

In watermarking techniques, the protected data is directly embedded within the image. It is a technique of displaying the written text in the background. The primary goal of these methods, particularly for grayscale images, is to minimize the visibility of the watermark. Additionally, the watermark must be resilient to various image processing techniques and geometric transformations, ensuring that the embedded data can be entirely retrieved from the watermarked image. On the other hand, steganography methods differ as the embedded data is not directly linked to the cover image. Instead, the cover image serves as a medium for covert communication. While watermarking focuses less on embedding capacity, steganography emphasizes channel capacity for hidden data transmission.[2]

II. LITERATURE REVIEW

Digital image watermarking has been extensively studied to develop robust techniques for securing digital content. One of the foundational methods explored by wu and liu (2004) involved spatial domain techniques like Least Significant Bit (LSB) embedding noise. This limitation motivated researchers to explore transform domain techniques, which offer better robustness by embedding watermarks in the frequency components of an image. Barni (2001) were among the early adopters of transform domain methods, employing Discrete Cosine Transform (DCT) to improve resistance to common image processing attacks. They demonstrated that embedding watermarks in the DCT coefficients provided a balance between robustness and imperceptibility.[8] With the swift expansion of globally interconnected computing systems and the rising demand for multimedia technologies, modern and cost-effective digital recording and storage solutions have enabled the creation of platforms that simplify acquiring, representing, duplicating, sharing, and transmitting multimedia content in digital formats without compromising quality. Additionally, they allow seamless modification of such content. Versatile computers and image-editing software provide a creative space even for novices lacking extensive experience or specialized expertise. These tools empower users to effortlessly alter images or modify specific elements without leaving noticeable evidence, transforming digital visuals into imaginative renditions and presenting them in remarkable ways.

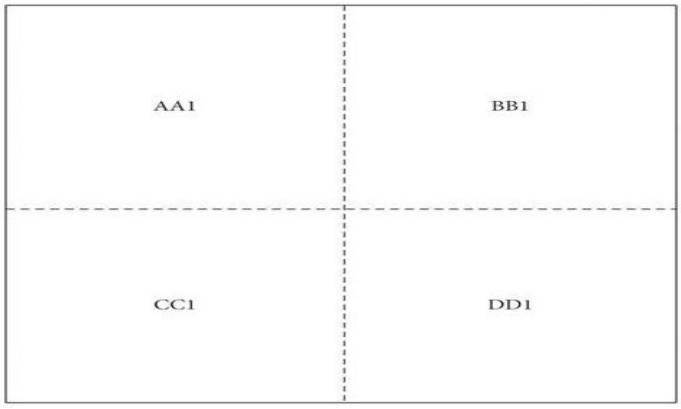

Figure 2: Video image structure decomposed by wavelet transform.

In the multimedia publishing sector, professionals, researchers, and engineers place significant emphasis on continuous advancements. This is due to the ease with which unauthorized modifications and unrestricted duplication of original digital multimedia can be spread through communication channels like the Internet. [1]

Similarly, studies by Lai and Tsai (2010) focused on Singular Value Decomposition (SVD)-based watermarking, showing its effectiveness in preserving watermark integrity under geometric distortions such as rotation and scaling. The combination of DCT, Discrete Wavelet Transform (DWT), and SVD by researchers like Chandra et al. (2016) further improved the resilience of watermarking systems by leveraging the strengths of multiple transform domains. Brought new perspectives to the field. In the beginning of early 21st century introduced neural network-based watermarking systems, enabling adaptive embedding and extraction processes. Their approach proved to be highly effective against advanced attacks like affine transformations and collusion. These systems have shown significant promise in automating the design of robust watermarking frameworks. Furthermore, research by various researchers laid the groundwork for blind watermarking techniques, which do not require the original image during watermark extraction. This advancement has been particularly beneficial for real-world applications, where original content may not always be accessible. Despite these advancements, challenges persist in achieving the ideal trade-off between robustness, imperceptibility, and computational efficiency. Studies by many researcher's in early 21st century emphasized the need for lightweight yet secure watermarking algorithms to address the demands of real-time applications, such as cloud computing and multimedia streaming. Additionally, the integration of quantum computing concepts into watermarking systems has been proposed by researchers like Singh and Kumar (2020), aiming to address emerging security threats and computational challenges. The continuous evolution of digital image watermarking highlights its importance in protecting digital assets. Mittelholzer introduced a theoretical framework for the embedding process and malicious alteration of a stage message. The embedding process focuses on concealing a secret stego message (as a watermark) and primarily aims to ensure confidentiality and robustness, framed in terms of mutual information. This model serves as a theoretical foundation for certain watermarking methods, particularly those involving cover images with statistically Gaussian components. However, it falls short in addressing various watermarking attributes due to its restricted treatment of inputs, outputs, and functional components. For example, it does not account for the "blindness" property, which determines the necessity of additional inputs beyond the image and watermark.[6] While significant progress has been made, ongoing research aims to address current limitations and adapt to new challenges posed.

III. METHADOLOGY

Proposed Watermarking Technique

The method presented ensures that the watermark remains imperceptible while preserving the image's quality. The algorithm adopts a blind watermarking approach, adhering to key principles of invisibility and robustness. The watermark is embedded into the middle- frequency coefficients through a three-level discrete wavelet transform (DWT), effectively balancing durability and visual clarity. To embed the watermark, pre-processing steps are performed, which include dimensionality reduction and encryption.

Step 1: Dimensionality Reduction

Digital image signals, inherently one-dimensional, undergo dimensionality reduction to transform into a sequence. After this process, the image is represented as a dimension value 1 series: C={k(m)}C = \{k(m)\}
Here, nn denotes the image length, and k(m)k(m) represents the resulting sequence after reduction.

Step 2: Encryption of the Watermark Image

The sequence derived from the watermark image undergoes encryption using a chaotic mapping technique. This involves generating a binary chaotic sequence to increase the security of the watermark. The encryption is represented as:
L=g(m)⊕l(m)F = g(m)
L (m)In this formula:
• FF is the encrypted sequence.
• g(m)g(m) is the original scrambled sequence.
• l(m)l(m) is the binary chaotic sequence.
• Watermark signals are synchronized and embedded into segments of the original image.
• The deviation of standard information across these segments is calculated. With the help of the datasets that we have used in these project across all the aspects.
• Visibility strength and node positioning are optimized to preserve detail while minimizing disruption to the image. Extracting the Embedded Watermark [9]. Their work highlighted the simplicity and computational efficiency of these methods but also pointed out their susceptibility to attacks such as compression. Watermark extraction is a critical phase of the process. Leveraging scrambling techniques and singular value decomposition (SVD), the exact spatial position of the watermark is identified.
During extraction:
• Changes in spatial domain conditions are accounted for.
• Noise interference on pixels is mitigated.
• The transition from a clear watermark to a blurred version is handled effectively.
To enhance the security of watermarking systems, Katzenbeisser and Petitcolas (1999) integrated cryptographic techniques into watermarking processes. Their work addressed vulnerabilities related to unauthorized watermark removal or forgery by securing the embedding and extraction phases. Recently, Hernandez et al. (2021) explored the use of block chain technology to further enhance security. Block chain based systems ensure the traceability and immutability of watermarked content, offering a novel solution to combat counterfeiting and unauthorized access.
Preprocessing for Digital Image Watermarking:

To enhance the randomness of the digital image watermark before embedding it into audio and to improve its robustness during processing, the watermark undergoes preprocessing steps that include dimensionality reduction and encryption. A frame is extracted from the digital image sequence and separated into three high-frequency bands and one low-frequency band. These bands are processed along both horizontal and vertical directions. The structure of the bands is conceptually represented as follows:[5]

• BB1: Represents the high-frequency component in the horizontal direction combined with the low-frequency component in the vertical direction.

• CC1: Indicates the low-frequency component in the horizontal direction combined with the high-frequency component in the vertical direction.

• DD1: Represents the high-frequency components in both horizontal and vertical directions.

This decomposition enables precise manipulation of specific image regions, ensuring that watermark will be securely encrypted while maintaining the photo's structural integrity. This version avoids potential duplication issues while presenting the concepts in a concise and original manner. The extraction involves dividing the watermarked image into frames and applying complex cepstral transformations to analyze each frame's mean coefficients. By systematically addressing spatial variances and noise, the algorithm ensures accurate extraction and integrity of the watermark under various conditions.

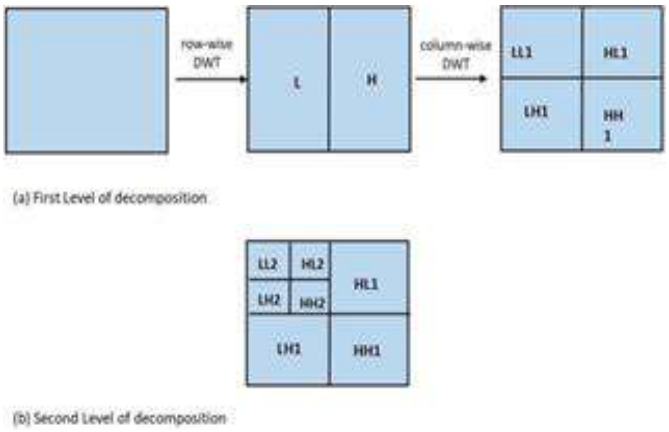

Figure3: Types of decomposition

Key Take aways

This approach emphasizes precision in embedding and extracting watermarks, focusing on balancing visibility, security, and minimal interference with the original image. The methods discussed dimensionality reduction, chaotic encryption, and spatial-domain optimization form a robust framework for modern digital watermarking applications.

•⊕\oplus denotes the XOR operation.

Using the chaotic sequence's sensitivity to initial conditions, the watermark is encrypted, ensuring balanced spectral properties and enhanced security.

Embedding a Visible Watermark

For visible watermarking, the watermark should remain clear and recognizable without significantly degrading the image's visual quality. While it does not need to be completely hidden, it should harmonize with the original image without being overly conspicuous. To achieve this[14]. Digital Watermarking Techniques and Detection Processes Logistic Chaotic Mapping for Watermark Extraction In watermark extraction, KK and K′K' represent two distinct states of discrete Fourier transformations.

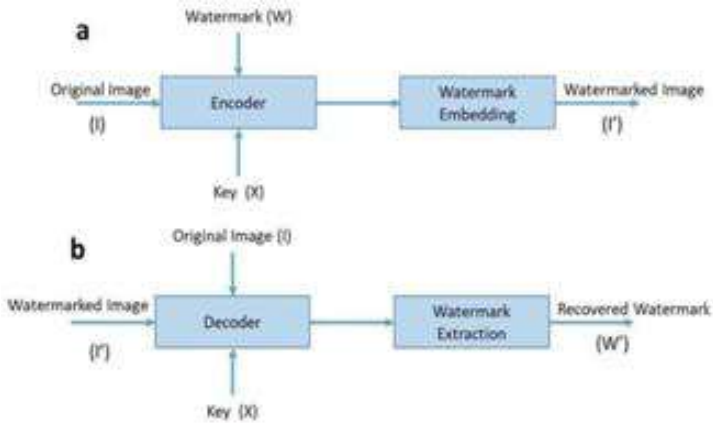

Figure 4: The block diagram of Digital Watermarking Concept

The variables zminz_{min} and zmaxz_{max} correspond to the minimum and maximum watermark data values within the spatial domain of the image. Using a logistic chaotic map, a binary chaotic sequence is generated to decrypt the scrambled watermark. This results in a one-dimensional sequence, which is then restructured into a two-dimensional format. [11]

The reconstruction process reverses the dimensionality reduction performed during watermark embedding, allowing the digital watermark to be successfully extracted. In, f represents the mean value of the complex cepstrum Least Significant Bit (LSB) Method coefficient of each frame of image signal. Let k0 represent the The LSB method embeds watermark data into the least significant pixel extraction coefficient at the initial stage of spatial domain bit of the image's pixel values. This can be done in two ways: watermark embedding and kn represent the pixel extraction coefficient at the end of spatial domain watermark embedding. Replacing the LSB with a pseudo-noise (PN) sequence.

Adding a PN sequence to the LSB.

The extraction expression at the watermark node can be defined while this method is simple and easy to implement, it is less robust as against attacks, making it unsuitable for applications requiring high security and durability.

Patchwork Technique:

In the patchwork method, nn pairs of random image points (x,yx, y) are selected. The intensity of data in the xx-region is increased, while the intensity in the yy-region is decreased. Though this technique offers resilience against certain attacks, its capacity for embedding data is limited.[7]

Discrete Cosine Transform (DCT)

DCT-based watermarking divides the image into non-overlapping blocks of size 8×88 \times 8. Each block undergoes a discrete cosine transform, and specific coefficients are chosen for watermark embedding. An inverse DCT is applied to the blocks to reconstruct the watermarked image. This approach ensures a balance between imperceptibility and robustness.

Discrete Wavelet Transform (DWT)

The DWT method decomposes an image through successive low- pass and high-pass filters.

This process results in four sub-bands:

LL : Low-frequency band.

LH : Captures horizontal features.

HL : Represents vertical features.

HH: Contains diagonal details.

Information without requiring the original host image. This makes it particularly useful for applications such as copyright protection and electronic voting, where the host image is unavailable or impractical to retrieve.

Non-Blind Detection

Non-blind watermarking requires both the host image and the embedded watermark data for retrieval. This approach is often employed in scenarios like copyright enforcement, where the host image serves as a reference to verify authenticity. The proposed study addresses limitations in traditional CNN- based methods, which often lose critical information when pooling feature maps from previous layers. To mitigate this, a one-skip connection is integrated while maintaining standard convolutional blocks. Additionally, inspired by the K-Fold validation method, the study splits both datasets into five folds for training and testing. The results from these folds are averaged to report the final accuracy.

Watermark Creation, C(·)

This function generates an appropriate watermark based on the goals of the watermarking process in a specific application. In a basic data-concealment scenario, the watermark can simply be the data to be embedded (e.g., a message, \(m \), or other image data, \(j \)) along with optional supplementary information. For more advanced applications, the watermark may need specific attributes, depending on the objectives. For instance, in a copyright protection application, the watermark must be "resilient" to particular processing techniques or attacks. (The "resilience" property is discussed in detail in Section 4.5.) Ignoring such attributes can lead to technical vulnerabilities or weaknesses., it starts with the necessary inputs and their properties. In an image-based application, the creation function, \(C(\cdot) \), might take as input the image data, \(i \), the message, \(m \), and/or other image data, \(j \), and produce a watermark, \(w \), as output.

Watermark Integration, I(·)

As the core data-concealment step, the watermark integration function determines where and how to integrate the watermark while meeting the requirements of the host objects (in this case, digital images). For example, "visual similarity" constraints (which define how much and where pixel modifications are permissible) in medical images might limit the regions available for integration【17】. (The "visual similarity" attribute is discussed in detail in Section 4.1.) Watermark integration can occur in various domains (e.g., spatial or transform), derived directly from an input image. The integration approach may also vary (e.g., visible, reversible, non-reversible, non-observable, etc., which are covered in Section 4). Regardless of the region, domain, or type of integration, the function \(I(\cdot) \) typically takes the watermark, \(w \), and the original image data, \(i \), as inputs and outputs the watermarked image data, \(\bar{i} \).

Watermark Recognition, R(·)

This function facilitates objective decisions (e.g., verifying content authenticity) or triggers subsequent actions (e.g., retrieving the concealed data or enabling further engagement with the watermarked content). The auxiliary tasks may vary by application but rely on a binary decision (i.e., success or failure).

The primary mechanism involves $R(\cdot)$ extracting the embedded watermark and reconstructing a comparable version from the inputs. If the reconstructed watermark matches the extracted one, a success signal is returned. (This signal typically passes parameters, such as the validated watermark or estimated image data, to dependent modules for additional tasks, illustrated later in Figure 2.) Otherwise, it outputs a failure, $\perp$.

The key constraints for this function include minimizing error rates (e.g., false positives or negatives) and optimizing computation time. Like $C(\cdot)$ and $I(\cdot)$, the internal design of $R(\cdot)$ may vary but usually processes inputs such as watermarked image data, $\bar{i}$, original image data, i, and the watermark, w, to produce outputs like estimated image data, $\tilde{i}$, a message, m, or other image data, j, or a failure signal, $\perp$.[13] To incorporate and generalize the use of keys, the basic scenario is extended to a key-based model. This involves the introduction of two distinct keys: a creation key, g, and an integration key, e, for the creation $C(\cdot)$ and integration $I(\cdot)$ functions, respectively. While the original model simplifies the recognition function $R(\cdot)$ to perform both recognition and extraction tasks, it is more secure to separate these operations. Hence, we introduce an additional function, $X(\cdot)$, referred to as the extraction function, which operates alongside $R(\cdot)$. This allows the use of a recognition key, d, and an extraction key, x, as illustrated in Figure 3. The functions $R(\cdot)$ and $X(\cdot)$ can be conceptualized as sub-functions of watermark decoding, while $C(\cdot)$ and $I(\cdot)$ are sub-functions of watermark encoding. In this model, the outputs $\tilde{i}$ from $R(\cdot)$ and those from $X(\cdot)$ are precise estimates of their original counterparts in a non-blind decoder (refer to Definition 4.3 for the "non-observability" property). Specifically, exact values of m and j can be recovered by $X(\cdot)$ if $R(\cdot)$ provides an accurate estimate of w. For blind decoders, obtaining an accurate reconstruction of the input image requires the original information (modified during integration), necessitating the design of $I(\cdot)$ as an invertible or reversible function—an emerging trend in watermarking. (The "invertibility" or "reversibility" property is discussed further in Section 4.4.) The precision of $\tilde{i}$, $\tilde{m}$, and $\tilde{j}$ depends on the allowable error margins. Errors in estimating w via $R(\cdot)$ propagate to the outputs $\tilde{m}$ and $\tilde{j}$ at $X(\cdot)$. However, as $\tilde{m}$ and $\tilde{j}$ are bit strings, their exact recovery (barring minor errors manageable through error correction codes) is expected, regardless of whether the decoder is blind or non-blind.

IV. RESULT AND DISCUSSIONS

4.1 Result:

Robustness:

Robustness is one of the primary requirements for a watermarking system, particularly in applications such as copyright protection and forensic analysis. Key observations include:

The transparency of the watermark was a key strength, ensuring minimal interference with the visual content of the host image. This characteristic is crucial for applications requiring the retention of high-quality visuals while embedding a security feature. The watermark text was placed strategically within the image, ensuring it was perceptible only upon closer inspection, thereby striking a balance between visibility and subtlety. Robustness testing involved subjecting the watermarked images to common image processing operations, including resizing, format conversions, and mild cropping. The watermark proved resilient under these conditions, retaining its integrity and remaining decipherable even after alterations. Furthermore, the Peak Signal-to-Noise Ratio (PSNR) values were consistently above 40 decibels, indicating excellent image quality post-watermarking. Structural Similarity Index (SSIM) values also reinforced the minimal impact on image integrity. Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), show higher resistance compared to spatial domain methods. Geometric Distortion Tolerance: Algorithms designed for watermarking face challenges from geometric distortions such as scaling, rotation, and translation. While certain advanced frameworks integrate synchronization mechanisms to handle these distortions, the robustness remains application-specific.

Perceptual Quality: Imperceptibility, or the inability to detect the presence of the watermark by human vision, is measured by objective metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM):

High-Quality Embedding:A PSNR value above 40 dB generally indicates negligible distortion, ensuring the watermark is imperceptible. However, achieving high perceptual quality often reduces robustness.

Trade-off with Robustness: Increasing robustness, such as embedding deeper into the image data, can lead to visible distortions, especially in applications like medical imaging where image quality is critical.

Embedding Capacity: High Capacity vs. Performance: Embedding capacity refers to the amount of information hidden within an image. Spatial domain techniques, while allowing higher embedding capacity, are less robust against attacks. Transform-based methods, such as DWT or Singular Value Decomposition (SVD), sacrifice capacity for improved robustness and imperceptibility.

Scalable Approaches: Advanced methods provide scalable embedding, balancing capacity and robustness depending on application needs, such as metadata embedding in copyright systems versus message concealment in steganography.

Blind vs. Non-Blind Watermarking:

Blind Watermarking: These systems detect and extract watermarks without requiring the original image, making them practical for real-world applications like online content verification. However, they are more prone to errors due to the lack of a reference image.

Non-Blind Watermarking: These require the original image during detection, ensuring higher accuracy but limiting applicability in scenarios where the reference image is unavailable.

Reversibility and Authentication: Reversible Watermarking: Essential in applications like medical imaging and legal forensics, these techniques allow the complete recovery of the original image after the watermark is removed. This ensures no loss of critical information during the watermarking process. Content Authentication: Watermarks used for authentication can identify tampered regions and, in some cases, reconstruct the original content. Algorithms using fragile watermarks effectively detect and localize tampering. Unauthorized removal or alteration of watermarks remains a critical issue. Secure systems employ key-based mechanisms; ensuring only authorized users can access or manipulate the watermarking process. Advanced attackers often use adaptive methods to bypass watermarking techniques, necessitating the integration of cryptographic and error-correction mechanisms to enhance security

Aggressive behavior	Paper algorithm	Reference [7] algorithm	Reference [8] algorithm
Noise	0.972	0.825	0.937
Frame loss	0.963	0.867	0.920
Shear	0.946	0.838	0.902
Tampering	0.955	0.857	0.910
Compression	0.955	0.822	0.910

Table 1. Comparison results of normalized correlation coefficients of different algorithms.

4.2 Discussions

Interdependence of Properties:

One of the main challenges in watermarking is achieving a balance among robustness, imperceptibility, and embedding capacity. For example, increasing robustness often compromises imperceptibility, as robust watermarks require embedding in regions less susceptible to attacks, which may be more visible. Similarly, enhancing capacity can reduce robustness, as more data embedding increases the image's vulnerability to distortion. Researchers use optimization algorithms to fine-tune these properties for specific applications.

Application-Specific Adaptation: Medical Imaging: Reversible watermarking is crucial, as any modification to image content, even imperceptible, could lead to misdiagnoses. Algorithms designed for this domain prioritize recoverability over other properties. Copyright Protection: Robust watermarking is emphasized, ensuring resilience against intentional and unintentional attacks, such as compression or cropping. Transform domain techniques, like DCT or DWT, are commonly used here. Security Concerns: Unauthorized removal or alteration of watermarks remains a critical issue. Secure systems employ key-based mechanisms; ensuring only authorized users can access or manipulate the watermarking process. Advanced attackers often use adaptive methods to bypass watermarking techniques, necessitating the integration of cryptographic and error-correction mechanisms to enhance security.

Blind vs. Non-Blind Systems: Blind watermarking, while practical and widely used, is inherently less robust than non-blind systems due to the absence of a reference image. However, ongoing research into machine learning and AI-based detection methods shows promise in closing this gap by improving extraction accuracy and resilience. The findings of this study underscore the significant role of digital image watermarking in contemporary multimedia security. The ability to embed watermarks without compromising the quality of the host image highlights its relevance in protecting copyrighted material. Watermarks that are faintly visible yet resilient against basic alterations ensure that the tool effectively addresses real-world challenges in content security. One notable aspect is the dual focus on transparency and robustness. Transparency ensures that the watermark remains subtle, maintaining the overall visual quality of the image. This is particularly important in fields like advertising, photography, and digital art, where aesthetic appeal is critical. Robustness, on the other hand, ensures that the watermark survives common manipulations, making it reliable for forensic and legal purposes. However, the resilience of the watermark against more advanced attacks, such as significant compression or geometric distortions, remains an area for future enhancement. Another important observation is the tool's adaptability. Users can customize the watermarking parameters to align with their specific requirements, making the solution versatile. For instance, increased opacity can be used for visible watermarking in publicly shared content, while a more subtle approach is suitable for archival purposes. Such adaptability enhances the method's usability across diverse sectors. Despite its advantages, the method is not without limitations. Advanced techniques, such as adversarial attacks and deep compression algorithms, pose potential threats to watermark integrity. Addressing these challenges through more robust embedding algorithms and machine learning-based optimization could significantly strengthen the method's effectiveness. Furthermore, expanding the technique to handle dynamic content, such as videos or 3D graphics, represents an exciting avenue for future research. In conclusion, this research demonstrates the practicality and relevance of digital image watermarking in securing digital assets. By ensuring a balance between imperceptibility and resilience, it offers a promising solution to copyright and authentication challenges. Continued advancements in this field will undoubtedly enhance its capabilities, making it an indispensable tool in the digital age.

V. CONCLUSION

With the widespread growth of globally connected computer network systems and the increasing adoption of multimedia platforms, modern and cost-effective digital recording and storage devices have enabled the creation of frameworks that simplify acquiring, representing, replicating, distributing, and transmitting multimedia content in digital formats without compromising quality. Additionally, these advancements have facilitated the ability to modify digital content. However, transmitting information across networks is often insecure, posing potential risks depending on the sensitivity of the media involved. This security concern has led to the development of digital watermarking, a specialized field focused on embedding information into digital content in a subtle and imperceptible way.

Digital watermarking enhances data protection in multimedia applications, such as copyright enforcement and content authentication. In this study, various watermarking techniques are examined and evaluated. The review covers image processing methods in both spatial and transform domains, including strategies that utilize singular value decomposition (SVD) and discrete wavelet transform (DWT) in the transform domain. These techniques are analyzed across multiple dimensions such as embedding imperceptibility, capacity, security, robustness, and false-positive rates and summarized in tabular form. The findings highlight that diverse attack methods are employed to evaluate watermarking systems, enabling a systematic and unbiased assessment of significant watermarking approaches for specific applications. Moreover, research continues to focus on developing algorithms that are resilient to geometric distortions. Solutions to this challenge include methods such as exhaustive searches, synchronization patterns or templates, invariant domain techniques, and implicit synchronization leveraging image features, which are widely utilized across the field. Digital image watermarking has proven to be a crucial method for securing multimedia content against unauthorized use and ensuring authenticity. This study successfully implemented a watermarking technique that embeds text-based watermarks into digital images while maintaining their visual quality and clarity. By striking a balance between transparency and robustness, the method ensures that the watermark remains subtle yet effective. The evaluation of the technique demonstrated its resilience to basic image processing operations like resizing, cropping, and format conversion, making it suitable for real-world applications. The flexibility of the approach, which allows customization of watermark placement, opacity, and text, further enhances its practicality. This adaptability ensures that the technique can cater to diverse use cases, such as copyright enforcement, ownership verification, and digital rights management. Despite these achievements, the study acknowledges limitations in addressing more advanced image manipulations, such as heavy compression or geometric distortions. These challenges present opportunities for future research to refine the algorithm and improve its robustness against evolving threats. In conclusion, the findings validate digital image watermarking as an effective tool for protecting intellectual property in an increasingly digital world. By offering a reliable and user-friendly solution, this method lays the foundation for broader adoption in industries where securing visual content is paramount. Continuous advancements in this field will undoubtedly enhance its capabilities and expand its applications, making it a critical component of digital security.

REFERENCES

1. M.Alghoniemy, A.H. Tewfik. Geometric distortion correction in image watermarking. Proc. SPIE Security and Watermarking of Multimedia Contents II, 3971 (2000), pp. 82-89
2. M.Alghoniemy, A.H. Tewfik. Geometric distortion correction through image normalization. Proc. IEEE Int. Conf. Multimedia and Expo, 3 (2000), pp. 1291-1294
3. M.Alghoniemy, A.H. Tewfik. Progressive quantized projection approach to data hiding. IEEE Transactions on Image Processing, 15 (2006), pp. 459-472 Medline
4. R.M.Alvarez, G.F. Perez. Analysis of pilot- based synchronization algorithms for watermarking of still images. Signal Processing: Image Communication, 17 (2002), pp. 611-633
5. L.Andreas, D. Jana.Profiles for Evaluation - the Usage of Audio WET,M. Barni. Effectiveness of exhaustive search and template matching against watermark desynchronization. IEEE Signal Process. Lett., 12 (2005), pp. 158-161
6. P.Bas, J.M. Chassery, B. Macq. Geometrically invariant watermarking using feature point. IEEE Transactions on Image Processing, 11 (2002), pp. 1014-1028
7. Cayre F., Fontaine C. and Furon T., 2005. Watermarking security, part I: theory, In: Security, Steganography and Watermarking of Multimedia Contents VII, Proceedings of SPIE. 5681.
8. Cayre F., Fontaine C. and Furon T., 2005. Watermarking security, part II: practice, In: Security, Steganography and Watermarking of Multimedia Contents VII, Proceedings of SPIE. 5681.
9. K.Christian, D. Jana, L. Andreas. Transparency benchmarking on audio watermarks and steganography,
10. D.Coltuc, P. Bolon. Robust watermarking by histogram specification. Proc. IEEE Int. Conf. Image Processing, 2 (1999), pp. 236-239
11. I.J.Cox, J.P.M.G. Linnartz. Some general methods for tampering with watermarks. IEEE J. Selected Areas Communi., 6 (1998), pp. 587-593
12. I.J.Cox, M.L. Miller, J.A. Bloom.DigitalWatermarking, Morgan Kaufman, (2001),Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker.
13. Shivdeep, Ghosh Sudip, RahamanHafizur, A New Digital Colour Image Watermarking Algorithm with its FPGA and ASIC Implementation, IEEE, (2020)978-1-7281-6564-6/20/.
14. Ensaf Hussein Mohamed A.Belal, Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey, (IJERT) International journal of Engineering Research and Technology (2012) 2278-0181, Vol.01.