International Journal of Data Informatics and Intelligent Computing (IJDIIC)
Vol. 4, No. 1, March 2025, pp. 54~72
DOI: 10.59461/ijdiic.v4i1.160

A Comprehensive Study on Digital Watermarking for Security Threats and Research Directions

Sambhaji Marutirao Shedole[1], V. Santhi[1]
[1]School of Computer Science and Engineering, Vellore Institute of Technology, Tamil Nadu, India

Article Info

Article history:

Received November 29, 2024
Revised February 27, 2025
Accepted March 18, 2025

Keywords:

Digital Image Watermarking
Steganography
Artificial Intelligence
Information hiding
Security

ABSTRACT

With the growing popularity of the Internet of Things (IoT) and the proliferation of AI-powered smart devices, a vast amount of digital data is being stored and shared on public platforms such as LinkedIn, Facebook, Twitter, Flickr, and other social media websites. Among these, digital images are the most commonly used medium for data sharing. Recent reports indicate that Google Photos stores over a billion images per week. Additionally, digital images play a crucial role in various applications, including social media, smart healthcare, intelligent transportation systems, industrial automation, robotics, the film industry, legal systems, news and insurance industries, and business sectors. However, the misuse of these images raises significant concerns regarding privacy and security. Identity theft, a growing issue in the 21st century, is a primary contributor to fraud in India and other countries. Thus, ensuring the security of digital images is a critical challenge that needs to be addressed. Currently, watermarking algorithms offer the most cost-effective solution for securing digital images. Watermarking involves embedding hidden marks within digital content to enhance its security. The key benefits of watermarking include: 1. Reducing bandwidth and storage demands, 2. Preventing copyright infringement and ownership disputes, 3. Protecting against tampering, and 4. Serving as an authentication keyword. Watermarking has gained significant traction in various fields, including cybersecurity and e-governance; given the growing importance of digital watermarking from a security perspective, this study aims to provide a comprehensive analysis of watermarking techniques and their evaluation methods across different applications. The findings of this extensive study are presented in this paper. Social media and healthcare. The primary objective of watermarking research is to enhance robustness, watermark capacity, and invisibility—an intricate trade-off among these factors. However, many existing watermarking techniques lack adequate security measures. Various approaches are available for both implementing and evaluating digital watermarking algorithms.

Corresponding Author: V. Santhi (e-mail: vsanthi@vit.ac.in)

1. INTRODUCTION

1.1. Overview

The evolution of computer networks and telecommunications has made data transmission easier and faster. However, the availability of numerous tools and software has also increased vulnerability to various attacks [1]. Securing digital photos and other multimedia data with copyright protection is becoming increasingly challenging, necessitating the development of an effective mechanism to address this issue. A variety of security mechanisms, including cryptography, steganography, and digital watermarking, must be used to protect multimedia data [2][3]. Cryptography employs encryption to secure text and graphic data and decryption to restore them to their original form. While this enables secure communication between two parties, the data remains unprotected once decrypted. In general, cryptographic methods transform messages

in a way that allows anyone who intercepts them to understand their content. In this paper, we present various modality-based watermarking schemes. The contributions of this work include: (1) a detailed overview of watermarking along with its characteristics, type of watermarking, embedding and recovery procedure, evaluation metrics and current applications; (2) a comprehensive survey of the different algorithms along with their merits and limitations; and (3) a summary of each of the algorithms in detail, including objectives, goals, embedding location, evaluation metrics, and weaknesses, and a discussion of recent challenges and their possible solutions.

The rest of the paper is structured as follows: Section 2 discusses different types of watermarks. Section 3 outlines the watermark embedding and extraction processes. Section 4 explores the key characteristics of watermarking, while Section 5 presents notable objective evaluation measures. Section 6 reviews related algorithms in both conventional and computational intelligence approaches and highlights state-of-the-art watermarking techniques. In Section 7, we identify potential challenges in the field and propose research directions along with possible solutions. Finally, Section 8 concludes the paper with a brief summary.

1.2. Background

Steganography can be used for discreet communication with a small payload between trusted parties. It is a technique that embeds secret data within cover images to ensure covert communication. Typically, a key is required for embedding the data; without this key, it becomes difficult for an unauthorized party to detect or remove the hidden information. The image containing the embedded data is known as the steganographic image. However, steganography must be resilient to attacks, data modifications, and potential alterations during transmission, storage, or format conversion, as it is primarily designed to protect sensitive information. Steganography and watermarking serve as complementary techniques rather than competing methods [4].

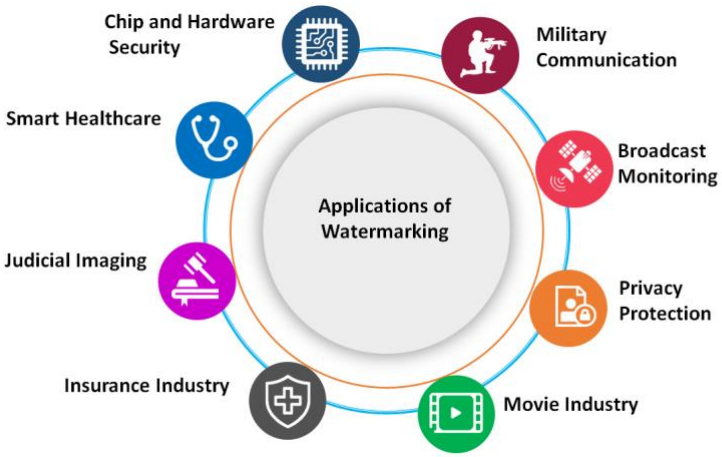

Figure 1. The various watermarking applications

Table 1. The Distinction between similar concepts

Related Approaches	Goal	Objectives	Limitations
Cryptography	Reach the primary security elements.	To prevent unauthorized individuals from understanding data or information.	High availability, lengthy running times, and intricate key management, particularly in public key infrastructure
Steganography	One-on-one secret communication	Invisibly conceal secret data in cover media from unlawful users.	Insufficiently resilient to assaults
Digital Watermarking	Covert communication from one to many	Robust and undetectable ownership verification of a media organization	Because of its fragility, image processing could destroy Mark.

Digital watermarking has been proposed as an effective method for identifying the source, creator, owner, retailer, or authorized user of an image or other digital data. It is one of the most reliable strategies for

protecting the copyright of digital multimedia content. This approach involves embedding permanent and unalterable marks within images to prevent unauthorized recognition or misuse [5][6]. The study of digital watermarking encompasses multiple disciplines, including communication theory, computational signal processing, multimedia coding, information theory, cryptography, mathematics, and computer science. This interdisciplinary nature makes watermarking applicable to various practical domains, such as chip and hardware security, insurance, the film industry, intelligent healthcare, legal imaging, military communication, privacy protection, and monitoring of military broadcasts [7][8]. A standard group of watermarking real-time applications are displayed in Figure 1. Limitations of related approaches are discussed in Table 1.

2. TYPES OF DIGITAL WATERMARKING

Digital watermarking embeds a distinct marker into electronic content, such as music, video, or image files, to identify the creator or copyright owner. Watermarks are classified into several types, including perceptual, visible, invisible, public, and private. Invisible watermarks can be further categorized into three types: robust, semi-robust, and fragile. Watermarking techniques are generally divided into two categories based on their operational domains: spatial and transform domains. Among these, transform domain techniques offer greater robustness compared to spatial domain-based methods. Figure 2 illustrates the Types of Watermarks. Table 2 lists the important categories of watermarks.

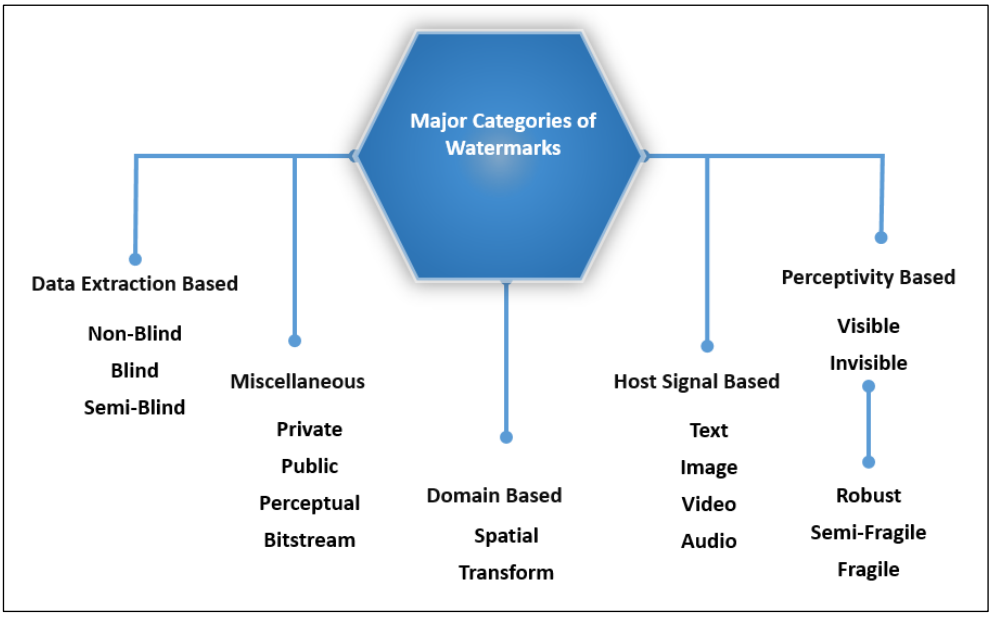

Figure 1. Types of digital watermarks

Table 1. A list of prominent watermarks

Type of watermark	Description	Prominent applications	Impediment
Non-blind	It calls for original media, which can occasionally be challenging to get by. Their use is restricted by the demand for original media.	Copyright protection, surreptitious communication	Need a greater space for storage to keep the carrier signal
Blind	Both original data and watermark information are not necessary.	Copyright protection, Healthcare, Remote education, tampering Detection etc.	The cost and computational complexity of the methods are high.
Semi-blind	Original data is not required; only a watermark or some supplementary information is required.	CAD model privacy and copyright protection, image authentication, etc.	To keep the additional information and key, more storage space is required.

Spatial domain	By directly altering the value of a pixel, bit, or code, secret information is added to the host signal.	Teleconferences, the media sector, watermarking in videos, and fingerprinting	Less resistant to many types of attacks.
Transform domain	The secret data is concealed in the frequency domains when the host signals are transformed to it.	Healthcare, image authentication, and copy protection	The cost and computational complexity of the methods are high.
Visible watermarks	Visual signals such as pictures and movies are appropriate targets for this kind of watermark. They are imprinted on the picture and are translucent.	Movie Industry	Decrease in image quality and enable detection using visual methods without the need for image processing
Invisible watermarks	Data, signals, or designs may contain a hidden, encoded message that is only visible to or observable by authorized parties after undergoing specific logical processing.	Healthcare, Copy-protection	The data, signal, or design may be subject to additional overhead.
Robust watermarks	It is resistant to general operations like compression, noise addition, filtering, A/D or D/A conversion, and geometric attacks like rotation, scaling, translation, shearing, and so forth.	Healthcare, image authentication, and copy protection	Watermarks have the potential to deter people from viewing or downloading images by making them appear amateurish and of poor quality.
Semi-Fragile watermarking	Strong enough to withstand appropriate content-preserving modifications and semi-fragile watermarks (compression, enhancement, etc.)	Copyright protection, Healthcare, Remote education, tampering Detection etc	The semi-fragile watermarking algorithm is not impervious to all types of attacks and is unable to discern between legitimate image processing operations and intentional manipulation.
Fragile Watermarking	Fragmentary watermarking techniques seek to be sensitive to any alterations to identify and pinpoint these changes.	Copyright protection, Healthcare, Remote education, tampering Detection etc	Brutality: If an image element is altered, some watermarks vanish.

3. THE PROCESS OF EMBEDDING AND EXTRACTING A TRADEMARK

Digital watermarking methods consist of two phases: embedding and extraction. The embedding phase involves concealing confidential information within cover data, while the extraction phase retrieves the hidden information. Cover material can include text, music, video, logos, or images [9]. Secret keys are used during embedding to insert watermarks into host images and during extraction to retrieve the embedded watermark. Figure 3 illustrates the complete process of watermark embedding and extraction.

Cover media is denoted as CV in the embedding system, while watermark is denoted as WT (wt1, wt2, wt3, etc.). The symbol for the embedding function is embedding (). The embedding process yields the watermarked picture WT'. Eq. (1) describes the embedding function mathematical equation.

$$\text{Embedding}(\text{CV}, \text{WT}) = WT' \quad (1)$$

Finally, the receiver side receives the watermarked media as the extraction is being done. When the watermark is extracted, the original watermark is recovered. The received watermarked image is designated as RW in the extraction procedure, and the extraction function is designated as extraction (). The

watermarked picture that was received is designated as RW in the extraction procedure, and the extraction function Eq. (2) is designated as extraction.

$$\text{Extraction } (\text{WT}') = RW \tag{2}$$

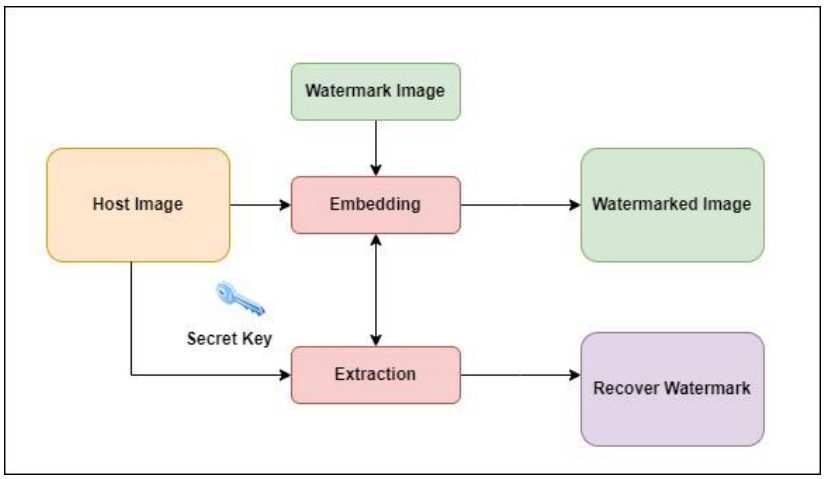

Figure 1. Watermarking Embedding and Extracting Procedure

4. CHARACTERISTICS OF DIGITAL WATERMARKING

To ensure authenticity and protect copyright holders from unauthorized use of their content, digital image watermarking techniques embed a watermark into multimedia data. It is also important to define the key features of the watermarking technique discussed in the following subsections. Figure 4 illustrates some of the most essential characteristics of watermarks [3][9]. Table 3 lists the important Characteristics of watermarks.

Figure 1. Characteristics of Watermarking Technique

Table 1. Features of digital watermark

Characteristics	Details
Imperceptibility	The degree to which the original and watermarked photographs resemble each other, as measured.
Robustness	The resistance of the hidden watermark to attacks and modifications of any kind is measured.
Security	The cover material and the watermark shouldn't be accessible to unauthorized parties or changed in any way.
capacity	A multimedia cover's ability to obscure a certain amount of information while maintaining its Imperceptibility.
Computational cost	Costs associated with watermarking, such as those associated with adding and removing digital watermarks on cover media.
False positive	The probability is that an un-watermarked section of the multimedia may be

	interpreted for a watermarked cover during the extraction process.
Key restrictions	The data or information for the watermark is generated from the cover multimedia, together with the key and its length.
Tamper resistance	By preventing any kind of alteration or substitution of the watermarked content, the validity and integrity of the digital watermarking system are safeguarded.

5. PERFORMANCE METRICS OF DIGITAL WATERMARKING

The following are some of the performance metrics mentioned in Table 4 that are used to gauge how well the suggested algorithm performs:

Table 4. Performance metrics of digital watermark

Performance Parameters	Formula	Descriptions
Peak Signal Noise Ratio (PSNR)	$PSNR = 10log\frac{(255)^2}{MSE}$ $Where,\ MSE = \frac{1}{a\times b}\sum_{i=1}^{a}\sum_{j=1}^{b}\left(X_{ij}-Y_{ij}\right)^2$ X_{ij} And Y_{ij} pixel value of novel and marked data of size $a \times b$, respectively.	Calculate the invisibility, better image quality is produced by a higher PSNR value. A good watermarking algorithm should provide PSNR value ≥ 30 dB
Normalized Correlation (NC)	$\mathrm{NC} = \frac{\sum_{i=1}^{a}\sum_{j=1}^{b}\left(X_{org_{ij}}\times Y_{rec_{ij}}\right)}{\sum_{i=1}^{a}\sum_{j=1}^{b}\left(X_{org_{ij}}\times Y_{org_{ij}}\right)}$ Where $X_{org_{ij}}$ and Extracted watermark data of size a*b and $Y_{rec_{ij}}$ a pixel of carrier data, respectively.	Measure the extracted mark's robustness attributes. Good watermarking algorithm Should provide NC value ≥ 0.7.
Bit Error Rate (BER)	$BER = \frac{(\text{Number of incorrect bits at receiver end})}{(\text{The overall amount of bits})}$	Compares the original and recovered marks for similarity. It ought to be close to zero.
Number of Pixel Change Rate (NPCR), or number of change pixel rate Average change intensity that is unified (UACI)	$X(c,d) = \begin{cases}0, if\ Z^1(c,d) = Z^2(c,d)\\1, if\ Z^1(c,d) \neq Z^2(c,d)\end{cases}$ $NPCR: N(Z^1,Z^2) = \sum_{p,q}\frac{X(c,d)}{T}$ $UACI: U(Z^1,Z^2) = \sum_{p,q}\frac{[Z^1(c,d)-Z^2(c,d)]}{F.T}$ where Z^1 is encrypted, Z^2 is decrypted media, F is the maximum pixel value, $and\ T$ is the complete number of pixels value of cypher-text media.	Used to evaluate how well defences respond against different attackers, NPCR (Number of Pixels Change Rate) values should ideally be close to 100%, and UACI (Unified Average Changing Intensity) values should be around 33.3%
Structural Similarity Index (SSIM)	$SSIM = f\left(l(c,d)m(c,d)n(c,d)\right)$ Where, $f(c,d), m(c,d), and\ n(c,d)$ Are the functions for comparing structure, contrast, and brightness, respectively	SSIM is used to compare watermarked and original images for resemblance. The resultant SSIM value close to 1 indicates perfect similarity

5.1. Problem Statement

The growing demand for secure digital content has driven the widespread use of watermarking techniques. However, maintaining an optimal balance between robustness, capacity, and invisibility remains challenging. This study explores various digital watermarking techniques and evaluation methods to enhance security across diverse applications.

6. LITERATURE REVIEW

In the subsequent section, various approaches used in watermarking multimedia data under two broad categories namely conventional approaches and computational approaches.

6.1. Conventional Approaches

A study [10] proposes a fragile watermarking scheme for concealing images, enabling coherent image tamper detection and self-recovery. A secret key-based pseudo-random binary sequence is used as a fragile watermark for detecting modifications. Additionally, a secret key is employed to store recovery data in a randomized manner. During the embedding process, each RGB image channel is separated and divided into non-overlapping 24-pixel blocks. Each block is watermarked using a 9-base notation system through Least Significant Bit (LSB) replacement. The proposed method achieves approximately 99% accurate tamper detection and significant image recovery, even at an 80% tampering rate. Comparative results demonstrate the effectiveness and relevance of this approach.

Using a quantization technique, [11] developed a watermarking method that embeds a binary image into the wavelet coefficients of a carrier image. The method employs the Otsu thresholding approach to extract the embedded bits from the watermarked image. Experimental results indicate strong resilience and Imperceptibility. However, the computational cost is high due to the Otsu method.

Quaternion Fourier transform (QFT) was used to build copy protection [12], which utilizes the Quaternion Fourier Transform (QFT) for copy protection. The RGB colour components of the carrier image are extracted, and each is processed using the wavelet packet transform. Security is enhanced through scrambling and encryption of the watermark image before embedding it into the carrier image using QFT. Experimental results confirm the algorithm's effectiveness.

In 2020, Study [13] introduced a watermarking method for High Dynamic Range (HDR) images in specific spatial transform domains, ensuring perceptual invisibility. The approach integrates imperceptible watermarking for ownership verification and visible watermarking for content integrity. The HDR encoding Transfer Function (TF) uses a Luma Variation Tolerance (LVT) curve to ensure optimal watermark embedding. Experimental and analytical studies on HDR images demonstrate robustness against tone mapping, lossy compression, and common signal processing operations while maintaining high Imperceptibility.

The study in [14] presents a quantum watermarking technique based on the Flexible Representation of Quantum Images (FRQI), embedding a 2n×2n2^n \times 2^n2n×2n watermark image within a 2n×2n2^n \times 2^n2n×2n grayscale carrier image. The watermark image influences the diagonal wavelet coefficients, which can be retained or modified. The watermark is extracted accurately due to the reversible nature of quantum operations. Performance evaluations highlight the effectiveness of this approach in preserving the similarity between the watermark and carrier images. The author proposes [15] four evaluation metrics for visible watermarking algorithms: global visibility, global prominence, local prominence at image edges, and overall image quality after watermarking. The evaluation results confirm the reliability of these metrics in assessing watermarking effectiveness under different conditions.

Introduces a block-based watermarking strategy utilizing entropy and edge entropy as Human Visual System (HVS) properties to select optimal embedding regions. Blocks with the lowest entropy values are chosen for watermark embedding. Preliminary results demonstrate strong Imperceptibility and resilience against various image processing and geometric attacks. Security is further enhanced through AES-256-bit encryption [16]. The work in [17] combines watermarking and image encryption for secure image transmission. The approach encrypts a secret key using RSA’s private key and subsequently re-encrypts it with the RSA public key before embedding it into the encrypted image. The method is resistant to attacks.

A watermarking technique for colour images based on the Discrete Cosine Transform (DCT) and Lifting Wavelet Transform (LWT). Security and stability are enhanced through encryption (MD5) and encoding (BCH coding) of the watermark and patient records. Experimental results confirm high resistance to attacks and computational efficiency [18]. In [19], it presents a robust copyright protection technique with a high embedding capacity for colour images. The approach employs a Non-Subsampled Contourlet Transform (NSCT) to fuse multiple images, ensuring enhanced information retention. The method demonstrates high security and resilience against image collection attacks.

The work proposed [20] enhances watermarking Imperceptibility and robustness by embedding multiple secret markers with an optimized scale factor. The method integrates spatial and transform domains while leveraging a denoising convolutional neural network (DnCNN) for watermark encryption. The approach improves resilience and security. An introduces a novel image watermarking system based on Visual Cryptography (VC) and block classification. The image is divided into non-overlapping blocks, which are classified using Support Vector Machine (SVM) and edge detection. The VC approach generates two shares: a master share and an owner share containing the watermark. This method improves security and authentication [21].

An SVM classifier in the watermark extraction process enhances resistance against various attacks. The method evaluates Imperceptibility and robustness by analyzing different frequency sub-bands, ensuring an optimal balance [22]. An image watermarking technique using the Shiftable Complex Directional Pyramid Transform (PDTDFB). The method decomposes the host image into frequency sub-bands, and watermarking is performed in the low-pass sub-band. The technique provides high resistance to geometric distortions and maintains visual quality [23]. The study in [24] improves watermark extraction using SVM and Principal Component Analysis (PCA) for feature reduction. The Lifting Wavelet Transform (LWT) is applied to decompose the cover image, and a binary watermark is embedded in the low-pass sub-band. SVM-based classification ensures accurate watermark retrieval.

Authors suggest [25] an enhanced watermarking approach using SVM and Discrete Rajan Transform (DRT). The image is divided into four segments, and DRT is applied to extract relevant coefficients. SVM is used for watermark classification, facilitating accurate extraction. Research in [26] addresses geometric attack resistance using NSCT and Gaussian-Hermite Moments (GHM). The host image is decomposed using NSCT, and watermark embedding is performed in low-pass sub-bands. The method is highly resilient against geometric distortions. The multiwavelet decomposition for watermark embedding using a mean-value modulation technique. SVM-based detection enhances watermark recovery, even under various attacks [27].

Researchers [28] introduce a spread spectrum (SS) and SVM-based watermarking model for medical images. The method involves segmenting images into Regions of Interest (ROI) and Regions of Non-Interest (RONI) before embedding patient data. Work in [29] compares 1-level and 2-level Discrete Wavelet Transform (DWT) watermarking techniques. The results indicate that 2-level DWT provides better watermark imperceptibility and extraction performance. The study [30] applies a hybrid Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD) watermarking approach for authentication. An AES-256 encryption scheme enhances security, making the method highly resistant to common attacks.

Utilizes Weber's Law for watermark embedding and tamper detection. The method divides the image into blocks and selects key pixels for watermark embedding, ensuring robustness [31]. In [32] enhances watermark resistance to rotation attacks by embedding the watermark in square blocks at the center of brightness channels. Zernike moments and a pseudo-random number generator improve resilience against geometric distortions.

The study [33] presents a deep learning-based watermarking approach for medical images. The Lempel-Ziv-Welch (LZW) compression algorithm preserves ROI integrity, while Integer Wavelet Transform (IWT) and SHA-256 ensure secure watermark embedding and extraction. Introduces a blind and robust watermarking method using the YCbCr color space, IWT, and DCT. An artificial neural network enhances computational efficiency, making the approach effective compared to existing techniques [34]. Table 5 provides a detailed overview of conventional watermarking methods.

Table 5. An overview of watermarking using Conventional Approaches

Ref.	Objectives	Techniques Used	Cover/ Water Size	Evaluation metric	Domain	Noticed Weaknesses	Type
[10]	To enable effective self-recovery and image tamper detection	LSB, Smoothing	512×512/12 bit	PSNR, SSIM, Temper detection rate	Spatial Domain	Detection accuracy decreases with increasing block size, such as 8 ×8.	Blind
[11]	to create reliable watermarks for coloured images	DWT, Quantization, Otsu algorithm	512x512/64x64	SSIM, BER, PSNR	Transform	More Processing time	Blind
[12]	Developing a secure colour picture scheme	Encryption, QFT, Geometric algebra	40 × 40/512 × 512	UACI, PSNR, NPCR, NC	Transform	High computation cost	Non-blind
[13]	Content readability, visual ownership identification	HDR-IW method	NA	PSNR, HVS, TF, HEVC	Spatial Domain	Security analysis not performed	Invisible
[14]	Efficient	QHWT,	2^n×2^	PSNR,	Transform		Invisible

	watermarking technique for quantum images	FRQI.	n/ 2^n1× 2^n1	quantum similarity metric		Less robust	
[15]	Evaluating visible watermarking techniques	JND, HVS	512×512 /512×512	PSNR	Transform	The system can be tested for multiple watermarking	Visible
[16]	Maintain Imperceptibility and robustness	SVD, DWT, AES	512×512 / 32×32	PSNR, MSE, BCR	Transform	Less robust against geometrical attacks, false positive issue	Visible
[17]	Watermarking and encryption	DCT, stream Cypher	NA	PSNR	Transform	NA	Invisible
[18]	Fragile watermarking	DCT, LWT, MD5, BCH Codes	512×512 / 64×64	PSNR, NC BER	Transform	Can be be used for other multimedia applications	Invisible
[19]	Robust copyright protection	CT, RSVD, NSCT, pseudo magic squares	512×512/ 128×128	PSNR, NC, BER, SSIM, NPCR, UACI	Spatial and Transform Domain	Less robust against cropping attacks	Invisible
[20]	High Imperceptibility and robustness with improved capacity	LWT, RSVD, DnCNN, pseudo magic Cube	512×512/ 128×128	PSNR, SSIM, NC, BER	Spatial and Transform Domain	Less robust against cropping attacks	Invisible
[21]	Reliable and trustworthy watermarking	SVM and VC	512×512/64×64	PSNR, NC	Spatial and Transform Domain	Other supervised classifiers may be used to implement this technique.	Invisible
[22]	Robust watermarking	LWT, SVM	512×512/16×32	PSNR, NC, BER	Spatial and Transform Domain	It can increase resilience to attacks involving noise and reduce noise.	Invisible
[23]	Watermarking for medical images that is secure	ML, DWT, DCT, SVD and SVM	128×128/256×256	NC, PSNR	Transform Domain	The proposed method can be made less computationally complex.	Invisible
[24]	Medical image watermarking that is robust and secure.	SVM, DWT and SVD	128×128/256×256	SSIM, NC, PSNR,	Spatial and Transform Domain	The proposed scheme's time complexity is too high.	Invisible
[25]	Protecting the medical image	Spread Spectrum, DCT, SVM	256×256/256×256	SR, PSNR	Spatial and Transform Domain	Many classifier types might be used to improve results.	Invisible

[26]	Robust Image Watermarking	SVM and NSCT	256×256/32×32	PSNR, BER	Spatial and Transform Domain	Greater computation time is needed throughout the SVM training phase.	Invisible
[27]	Blind Image watermarking	SVM, DCT and HVS	32×32/ 256×256/	NC, PSNR	Spatial and Transform Domain	NA	Invisible
[28]	Encrypted watermarking method for applications that require security	SVM, DRT	512×512	NC, PSNR,	Spatial and Transform Domain	The proposed idea can be made more durable and aesthetically pleasing by boosting system capacity.	Invisible
[29]	Robust watermarking, visibility Factors	2-Level DWT	512×512/128×128	PSNR, NCC	Transform Domain	Lacking proper robustness analysis with different kinds of attacks	Invisible
[30]	Security and copyright protection	FDT, DCT, SVD, AES	NA	PSNR, MSE, NCC	Transform Domain	After using AES decryption, the approach fails to recover throughout the extraction procedure.	Invisible
[31]	Robust watermarking, Tamper detection	Weber law	255×255/85×85	PSNR	Spatial Domain	Future potential for using Weber Watermarking to recover the compromised watermarked image	Semi-Blind
[32]	Perceived invisibility and resistance to cooperation and rotational attacks	40permutation vector, Pseudo Random Number (PRN) generator, DCT	Video	PSNR, SSIM, MSE	Transform Domain	Through the use of FPGAs, performance can be increased, and the proposed technique can be developed for hardware implementation.	Blind
[33]	Robust medical image watermarking, ROI reversibility	Deep neural network, LZW (Lampel-Ziv-Welch), IWT (integer wavelet transform),	512×512/32×32	MSE,	Transform Domain	performance enhancement, the potential for improved RONI segmentation to more precisely localize tampering	Blind

		SHA-256					
[34]	Blind and robust	YCbCr colourspace, IWT (integer wavelet transform) And DCT, Neural network	512×512/32×32	BER, NC, PSNR, SSIM	Transform Domain	Neural network designs will be used to examine performance enhancement and the extraction process.	Blind

6.2. Computational Intelligence Approaches

The watermarking framework is designed to handle colour images under various attacks using a neural network-based approach [35][38]. When employing the contourlet function in the proposed system, it is acknowledged that some variations may occur. However, selecting the appropriate coefficient groups carefully mitigates these changes. Consequently, the Zenzo edge detector is used to guide the approach, positioning the logo information near the edges of the colour image. The second sub-band edge is identified, and its capacity is subsequently determined. The embedding and extraction processes—applied in the learning algorithm of the aforementioned neural network using a single training dataset—are analyzed in this study. A series of evaluations under different conditions confirm the efficiency of the proposed method.

A novel greyscale image watermarking technique, based on a combination of machine learning algorithms in the wavelet domain, is presented in [36][39]. The selection of non-overlapping and large regions is based on fuzzy entropy information. The low-frequency sub-band is obtained through the Lifting Wavelet Transform (LWT) applied to a selected area, followed by QR factorization. Low-frequency features from each region serve as input for the training phase of the Lagrangian Twin Support Vector Regression (LTSVR). The watermark is then embedded into the output wavelet coefficient dataset generated by the trained LTSVR. To ensure the watermark's security, the Genetic Algorithm (GA) optimizes the watermark scaling factor, while the Arnold Transform enhances invisibility and robustness. Experimental results, along with comparisons against industry standards, demonstrate a significant improvement in resistance to image processing attacks, making this method suitable for copyright protection applications.

The author introduces SMLE, a state-of-the-art and reliable blind watermarking method for colour images. This approach embeds a watermark into a wavelet-domain host colour image in the form of a small-scale image [37]. The study proposes a dependable technique for watermarking digital colour images, particularly for visually impaired individuals. By converting a grayscale image, originally stored using Least Significant Bit (LSB) encoding, to a Most Significant Bit (MSB) representation and employing a quantization strategy in the wavelet domain, a grayscale watermark is fully encoded within a colour host image. Additionally, the 2D Otsu algorithm is utilized to extract the watermark with high accuracy. Experimental results indicate that the proposed system outperforms existing methods in terms of watermark imperceptibility and robustness, except in cases of lossy JPEG compression and rotational distortions.

The symmetrical properties of contourlet coefficients are leveraged to divide them into three quadrants for computation, with the key coefficients being adjusted accordingly [40]. This study presents a discrete contourlet transform-based quantization index modulation method for digital image watermarking. The Lagrange method is used for optimization, leading to a high Peak signal-to-noise ratio (PSNR), indicating minimal perceptual impact on the watermarked image. Additionally, the normalized correlation values are close to one, demonstrating strong computational robustness. The integration of discrete contourlet transforms, discrete cosine transforms, and singular value decomposition, along with careful coefficient selection, results in high simplicity and resistance to attacks.

A novel watermarking framework, integrating a meta-heuristic approach with an embedding technique, is proposed in [41] to enhance performance. A new fitness function ensures optimal convergence for the defined optimization problem. The multiple objectives of the problem are divided into two single-target sub-problems. The proposed approach offers a method to regulate accuracy by adjusting predefined limits. The study finds that the host image, embedding method, and design space constraints significantly influence watermark quality. Experimental results conducted under various attacks and quality thresholds indicate that the proposed method enhances robustness while maintaining quality constraints.

A watermarking technique for colour images, based on the Bessel K function (BKF) distribution and fuzzy least squares support vector machine (FLS-SVM), is introduced in [42]. The study demonstrates that the proposed algorithm achieves excellent watermark invisibility and surpasses traditional methods in robustness. The mathematical distortion limits that enable watermark extraction are initially analyzed using the BKF distribution of Quaternion Wavelet Transform (QWT) coefficients, followed by the incorporation of

FLS-SVM for watermark processing. Despite its effectiveness, the approach has some drawbacks, including the lengthy training process of FLS-SVM. Additionally, certain geometric distortions such as segmentation, line removal, and centre cropping may render the algorithm vulnerable.

A hierarchical model of one-dimensional ergodic chaotic maps incorporating Tsallis-type q-deformation is proposed in [43]. This well-known encryption algorithm addresses issues such as limited key space, encryption speed, and security level. Security analyses are conducted to evaluate the robustness of the proposed scheme. Results suggest that this approach has strong potential for adoption in watermarking applications, demonstrating real-world applicability for image authentication.

A genetic algorithm is employed to optimize watermark embedding strength in the proposed algorithm [44]. This optimization tool effectively determines the best embedding strength to balance PSNR and normalized correlation (NC) values. The proposed digital image watermarking algorithm achieves high PSNR and NC values, even when subjected to attacks such as resizing, filtering, and Gaussian noise. Experimental results confirm the robustness of the approach.

A multi-approach image watermarking scheme is introduced to facilitate adaptive localization, self-recovery, and ownership verification [45]. Greyscale watermarking ensures theoretical and practical consistency in the proposed framework. The host image is transformed into the wavelet domain using Discrete Wavelet Transform (DWT), with specific coefficients modified to embed the watermark. Robustness is further enhanced using Artificial Bee Colony (ABC) optimization, which adjusts the scaling factors to improve watermark strength under various constraints.

A robust and lossless Region of Interest (ROI) watermarking technique for medical images based on M-Ary modulation is presented in [46]. The system is experimentally validated for two distinct brain imaging modalities using quality metrics such as payload capacity, Structural Similarity Index (SSIM), Mean Squared Error (MSE), and PSNR. The M-Ary modulation technique enhances robustness by reducing the number of images needed for encoding binary text messages. Experimental results confirm the effectiveness of this approach in ensuring data security and Imperceptibility in medical image watermarking.

The assessment of the inclining grid's ability to meet strength requirements is conducted using a single evaluation based on watermark data obtained from SVD-based watermarking computations [47]. Genetic algorithms are employed to enhance performance and extend the applicability of PSNR and NC across different watermarking schemes. Initial results indicate that, compared to a single watermarking approach, the diversified watermarking methodology yields more robust outcomes. This enhancement aims to facilitate the implementation of PSNR and normalized correlation (NC). Preliminary findings further suggest that the proposed strategy, leveraging genetic algorithms, demonstrates remarkable complexity and robustness against attacks. However, its performance does not significantly distinguish it from existing approaches.

To enhance the Imperceptibility and robustness of embedded information, this study proposes an improved digital image watermarking technique utilizing a coefficient quantization approach. This method effectively encodes ownership data within each colour channel [48]. To optimally balance robustness and distinctiveness, optimization algorithms such as Ant Colony Optimization (ACO) or Particle Swarm Optimization (PSO) should be employed when selecting robustness factors. However, large-scale computation for big data remains a significant challenge, particularly for multidimensional data like images.

A probabilistic neural network is used to extract the watermark image. The effectiveness of the extracted watermark is evaluated using the Peak Signal-to-Noise Ratio (PSNR) and Normalized Cross-Correlation (NCC) to assess image quality [49]. The proposed algorithm outperforms existing methods in terms of invisibility. The resilience of the watermarked image is verified through various tests, subjecting it to attacks such as JPEG compression, Gaussian noise, rotation, cropping, and median filtering.

A cutting-edge neural network-based digital watermarking method for colour images has been introduced [50]. This approach embeds an invisible watermark within a colour image and utilizes neural networks to analyze the characteristics of the embedded watermark. Due to their learning and adaptive capabilities, trained neural networks can accurately retrieve the watermark from the image, even when subjected to image processing attacks.

To establish identity, the proposed system incorporates three types of watermarks: a medical lump image, a doctor's signature or identification code, and patient diagnostic data in textual form [51]. To enhance resilience and minimize noise interference in the watermarked image, a Back Propagation Neural Network (BPNN) is used for watermark recovery.

A digital watermarking method based on Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) is also proposed [52]. During embedding, the original colour image is decomposed using third-level DWT, where the LL3 low-frequency band undergoes SVD transformation. The SVD algorithm is then applied to the watermarked image. The S component of the host image embeds the watermark data through a modified S vector while preserving the original U and V vectors. The inverse SVD

reconstructs the watermarked image, followed by inverse DWT processing. The extraction algorithm is used to retrieve the watermark.

A neural network-based blind watermarking technique is introduced for use in both discrete and Fourier wavelet transform domains [53]. By adjusting the watermark strength with artificial neural networks, the proposed method achieves optimal trade-offs. The robustness of the watermark is further enhanced by repeatedly embedding a binary image into selected wavelet coefficients. Experimental results confirm that this approach is highly resilient against various attacks, including JPEG compression, Gaussian noise, mean and median filtering, cropping, and salt-and-pepper noise.

A novel technique utilizing coupled neural networks is also explored. The process begins by processing an appropriate grayscale watermark image, which is then embedded as a watermark signal into the discrete cosine transform (DCT) components of image blocks [54]. A cooperative neural network is employed to identify and extract the watermark, where the input represents the suspected watermark signal and the output represents the extracted watermark.

To incorporate image and text watermarks, the host image is first decomposed into third-level DWT, selecting the LL3 low-frequency and LH2 vertical frequency bands for embedding, respectively [55]. Unlike traditional methods that use a single watermark, the proposed approach employs multiple watermarks on the same multimedia content to improve ownership authentication.

The goal of this study is to enhance the creation of watermarked images with high Imperceptibility. Even in the absence of the original image, watermarks can be accurately extracted. To embed a binary watermark image into specific coefficient blocks, the Haar filter-based Discrete Wavelet Transform (DWT) is employed. A probabilistic neural network is then used for watermark extraction. The author presents an image watermarking method incorporating quantization and Back Propagation Neural Networks (BPNN) [56]. The cover image is decomposed into a maximum of three levels using DWT and quantization techniques. A bitmap image is used as the watermark, which is embedded and later extracted using a back-propagation neural network.

A new blind watermarking technique based on Discrete Wavelet Transform (DWT) is also proposed, utilizing Radial Basis Function (RBF) neural networks and the Human Visual System (HVS) model [57]. The RBF network is employed for both embedding and extraction, while the HVS method determines the watermark insertion strength. After training, the neural network can nearly perfectly recover the watermark from the image.

In another method, noise-resistant watermarks are embedded into a 256×256-pixel host image using the Discrete Cosine Transform (DCT), which converts the spatial domain into the frequency domain [58]. Subsequently, 32×32-pixel watermark images are added as watermark identification codes. To ensure Imperceptibility, the Inverse Discrete Cosine Transform (IDCT) is applied, adjusting the frequency domain to restore the spatial domain.

ReD-Mark is an advanced end-to-end watermarking system designed for adaptability across various watermarking algorithms and transformation spaces [59]. The framework consists of two convolutional neural networks with residual structures that function in real-time to embed and extract watermarks. The deep network undergoes end-to-end training for secure blind watermarking. The proposed design includes a dedicated network layer to simulate various attacks, ensuring resilience and robustness. A detailed overview of computational intelligence approaches for watermarking is provided in Table 6.

Table 6. An overview of watermarking using Computational Intelligence Approaches

Ref.	Objectives	Techniques Used	Cover/Water Size	Evaluation metric	Domain	Noticed Weaknesses	Type
[38]	Colour image watermarking	Neural network, Contourlet transform, Zenzo edge detector	512×512/ 128××	MSME, PSNR,	Transform Domain	Lacking Security analysis	Invisible
[39]	Robustness and Imperceptibility	Machine Learning LWT, LTSVR, Genetic algorithm	512×512/ 32×32	PSNR, NC, BCR	Transform Domain	High computation time	Semi-blind
[40]	Higher	CT,	512×512/	PSNR,	Transform	Lacking FPP and	Invisible

	robustness and more effective Imperceptibility	quantization index modulation, DCT, SVD	256×256	MSE	Domain	Security Analysis	
[41]	Intelligent system, optimized performance	ABC, DCT, JND	512×512/ 64×64	PSNR, MSE,	Transform Domain	With high computation time and a lack of security analysis, the algorithm can be validated for dual watermarking	Invisible
[42]	Watermarking in color images that is reliable	Bessel K form distribution, support vector machines, fuzzy least squares, QWT, and QDFT	512×512/ 64×64	BER, PSNR	Transform Domain	The planned FLS-SVM training requires additional time, Less robust against geometrical distortions	Invisible
[43]	Watermarking scheme for image authentication	DWT, Q-deformed chaotic map	512×512/ 32×32	PSNR, MSE, BER, NC	Transform Domain	can be validated for other application	Invisible
[44]	Copyright protection	SVD, GA, DWT	512×512/ 128×128	PSNR, NC	Transform Domain	Lacking proper robustness analysis with different kinds of attacks	Invisible
[45]	Tamper localization, self-recovery and ownership verification	DWT, DCT, SVD, ABC	512×512/ 128×128	PSNR, NCC,	Transform Domain	Less robust against Gamma Correction	Invisible
[46]	ROI medical image for robust and lossless	Fuzzy C-means, DCT, MAry modulation	512×512/ 32×32	PSNR, MSE, SSIM	Transform Domain	Lacking proper robustness analysis with different kinds of attacks	Invisible
[47]	Imperceptibility Robustness	DWT, SVD, GA	512×512/ 48×48	PSNR, MSE, NCC	Transform Domain	Lacking proper robustness & and security analysis	Invisible
[48]	Improve Imperceptibility and robustness	DWT, Coefficient Quantization, Optimal Color Channel, Adaptive Otsu thresholding	512×512/ 32×32	CPSNR, BER,	Transform Domain	Can be validated for high payload capacity	Invisible
[49]	High invisibility	DWT, Probabilistic neural network	512×512/ 64×64	PSNR, NCC	Transform Domain	High computation time	Invisible

[50]	Copyright digital watermarking sa feguarding colour images	ANN	480×512/ 32×32	PSNR, MSE, MAE	Transform Domain	This strategy can be applied to various colour maps.	Invisible
[51]	A Secure Watermarking application for healthcare domain	Arnold Transform, DCT, BPNN SVD	64×64/51 2×512	NC, BER, PSNR	Transform Domain	It is possible to lessen the proposed scheme's time complexity.	Invisible
[52]	Reliable and safe watermarking for social media applications	BPNN, DWT, SVD	64×64/51 2×512	BPN, PSNR	Transform Domain	The proposed scheme's computing complexity has increased.	Invisible
[53]	Robust Watermarking for digital data protection	DWT, FFNN	512×512/ 32×32	PSNR, NC	Transform Domain	The suggested approach can be applied to further neural network models.	Blind
[54]	Digital watermarking that is reliable and secure for use in smart city applications	CNN, DCT,	NA	NC, PSNR	Transform Domain	The suggested scheme can be used with various spatial domain techniques.	Invisible
[55]	Social network protection with hybrid watermarking	BPNN, DCT, DWT, SVD, and ECCs	128×128/ 512×512/ and text of 100 characters	BER, PSNR, NC	Transform Domain	By applying various wavelet transforms, the computational time complexity of this approach can be lowered.	Invisible
[56]	Reliable watermarking for digital content	DW, BPNN	64×64/25 6×256	NC, PSNR	Transform Domain	It doesn't offer a stronger level of JPEG resilience. The idea of fuzzy logic can be used to further increase this scheme's robustness.	Invisible
[57]	To safeguard digital media's copyrights, use a digital watermark.	RBFNN, DWT, HVS	128×128/ 512×512	NC, PSNR	Transform Domain	The suggested approach only defends against a few different kinds of assaults	Blind
[58]	Digital Image Watermarking	BPNN, DCT	32×32/25 6×256	NC, PSNR	Transform Domain	NA	Invisible
[59]	Real-time watermarking approach for applications	Deep Learning algorithm	132×32/5 12×512	SSIM, PSNR	Transform Domain	This method can be used for more real-time applications.	Blind

7. RESEARCH DIRECTION AND POTENTIAL GAPS WITH DIGITAL WATERMARKING

The main conclusions of the experimental work should be presented. The contribution of the work to the scientific community and its economic implications should be emphasized. Research on watermarking

schemes primarily focuses on improving key properties such as resilience, embedding capacity, and invisibility, which can be challenging to balance effectively. Achieving an optimal trade-off among these factors while considering computational complexity and security remains a significant challenge, as these aspects are method dependent.

Some key challenges in watermarking research include:

- Optimizing the trade-off between resilience, capacity, and Imperceptibility when implementing watermarking technology.
- Ensuring both security and computational efficiency in watermarking systems.
- Addressing all potential image-based attacks when developing new watermarking techniques or improving existing ones.
- While combining two or more transform domain approaches enhances performance, it also increases computational complexity.
- The dimensionality of the cover media significantly affects the embedding capacity of the watermarking system. However, some studies suggest that it may not necessarily impact capacity performance.
- The Discrete Wavelet Transform (DWT)-based watermarking system has limitations, such as shift variance and a lack of directional information. Researchers have proposed using Redundant Discrete Wavelet Transform (RDWT) to address shift-variance and down-sampling issues in DWT-based methods.
- Various optimization techniques have been applied to identify the optimal scaling factor and embedding locations to meet watermarking requirements. However, these optimizations often increase the overall computational burden.
- Transform-based watermarking methods provide higher resilience but come with a greater computational cost compared to spatial domain-based techniques.
- To enhance resistance against attacks, watermarking schemes employ fuzzy logic, artificial neural networks, and support vector machine (SVM) classifiers. However, these approaches significantly increase computational complexity.

8. CONCLUSION

This paper presents a comprehensive analysis of various watermarking methods, their characteristics, applications, and the common attacks that target watermarked images. Additionally, it explores different approaches used in watermarking algorithms, categorizing them into two broad groups: conventional and computational-based techniques. A detailed summary of each algorithm is provided, highlighting its objectives, embedding location, evaluation criteria, and limitations. Furthermore, we discuss current challenges in the field and potential solutions. We believe this study offers readers a thorough understanding of watermarking techniques and their advancements.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest in this work.

REFERENCES

[1] P. Aberna and L. Agilandeeswari, "Digital image and video watermarking: methodologies, attacks, applications, and future directions," *Multimed Tools Appl*, vol. 83, no. 2, pp. 5531–5591, Jan. 2024, doi: 10.1007/s11042-023-15806-y.

[2] D. K. Mahto and A. K. Singh, "A survey of color image watermarking: State-of-the-art and research directions," *Computers & Electrical Engineering*, vol. 93, p. 107255, Jul. 2021, doi: 10.1016/j.compeleceng.2021.107255.

[3] A. Anand and A. K. Singh, "Watermarking techniques for medical data authentication: a survey," *Multimed Tools Appl*, vol. 80, no. 20, pp. 30165–30197, Aug. 2021, doi: 10.1007/s11042-020-08801-0.

[4] S. Gull and S. A. Parah, "Advances in medical image watermarking: a state of the art review," *Multimed Tools Appl*, vol. 83, no. 1, pp. 1407–1447, Jan. 2024, doi: 10.1007/s11042-023-15396-9.

[5] S. Kashifa, S. Tangeda, U. K. Sree, and V. M. Manikandan, "Digital Image Watermarking and Its Applications: A Detailed Review," in *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, IEEE, Feb. 2023, pp. 1–7. doi: 10.1109/SCEECS57921.2023.10063033.

[6] H. K. Singh and A. K. Singh, "Comprehensive review of watermarking techniques in deep-learning environments," *J Electron Imaging*, vol. 32, no. 03, Nov. 2022, doi: 10.1117/1.JEI.32.3.031804.

[7] S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, “Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection,” *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 83–91, Jul. 2017, doi: 10.1109/MCE.2017.2684980.

[8] P. Amrit and A. K. Singh, “Survey on watermarking methods in the artificial intelligence domain and beyond,” *Comput Commun*, vol. 188, pp. 52–65, Apr. 2022, doi: 10.1016/j.comcom.2022.02.023.

[9] O. P. Singh, A. K. Singh, G. Srivastava, and N. Kumar, “Image watermarking using soft computing techniques: A comprehensive survey,” *Multimed Tools Appl*, vol. 80, no. 20, pp. 30367–30398, Aug. 2021, doi: 10.1007/s11042-020-09606-x.

[10] R. Sinhal, I. A. Ansari, and C. W. Ahn, “Blind Image Watermarking for Localization and Restoration of Color Images,” *IEEE Access*, vol. 8, pp. 200157–200169, 2020, doi: 10.1109/ACCESS.2020.3035428.

[11] T. Huynh-The *et al.*, “Selective bit embedding scheme for robust blind color image watermarking,” *Inf Sci (N Y)*, vol. 426, pp. 1–18, Feb. 2018, doi: 10.1016/j.ins.2017.10.016.

[12] U. A. Bhatti *et al.*, “Hybrid Watermarking Algorithm Using Clifford Algebra With Arnold Scrambling and Chaotic Encryption,” *IEEE Access*, vol. 8, pp. 76386–76398, 2020, doi: 10.1109/ACCESS.2020.2988298.

[13] K. R. Perez-Daniel, F. Garcia-Ugalde, and V. Sanchez, “Watermarking of HDR Images in the Spatial Domain With HVS-Imperceptibility,” *IEEE Access*, vol. 8, pp. 156801–156817, 2020, doi: 10.1109/ACCESS.2020.3019517.

[14] W.-W. Hu, R.-G. Zhou, A. El-Rafei, and S.-X. Jiang, “Quantum Image Watermarking Algorithm Based on Haar Wavelet Transform,” *IEEE Access*, vol. 7, pp. 121303–121320, 2019, doi: 10.1109/ACCESS.2019.2937390.

[15] E. Fragoso-Navarro, M. Cedillo-Hernandez, M. Nakano-Miyatake, A. Cedillo-Hernandez, and H. M. Perez-Meana, “Visible Watermarking Assessment Metrics Based on Just Noticeable Distortion,” *IEEE Access*, vol. 6, pp. 75767–75788, 2018, doi: 10.1109/ACCESS.2018.2883322.

[16] N. M. Makbol, B. E. Khoo, and T. H. Rassem, “Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics,” *IET Image Process*, vol. 10, no. 1, pp. 34–52, Jan. 2016, doi: 10.1049/iet-ipr.2014.0965.

[17] W. Puech and J. M. Rodrigues, “A New Crypto-Watermarking Method for Medical Images Safe Transfer,” Sep. 2004. https://www.researchgate.net/publication/253934763

[18] A. K. Singh, “Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image,” *Multimed Tools Appl*, vol. 78, no. 21, pp. 30523–30533, Nov. 2019, doi: 10.1007/s11042-018-7115-x.

[19] D. K. Mahto, A. K. Singh, K. N. Singh, O. P. Singh, and A. K. Agrawal, “Robust Copyright Protection Technique with High-embedding Capacity for Color Images,” *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 20, no. 11, pp. 1–12, Nov. 2024, doi: 10.1145/3580502.

[20] D. K. Mahto, A. Anand, and A. K. Singh, "Hybrid optimization-based robust watermarking using denoising convolutional neural network," *Soft comput*, vol. 26, no. 16, pp. 8105–8116, Aug. 2022, doi: 10.1007/s00500-022-07155-z.

[21] A. Fatahbeygi and F. Akhlaghian Tab, “A highly robust and secure image watermarking based on classification and visual cryptography,” *Journal of Information Security and Applications*, vol. 45, pp. 71–78, Apr. 2019, doi: 10.1016/j.jisa.2019.01.005.

[22] M. Islam, A. Roy, and R. H. Laskar, “SVM-based robust image watermarking technique in LWT domain using different sub-bands,” *Neural Comput Appl*, vol. 32, no. 5, pp. 1379–1403, Mar. 2020, doi: 10.1007/s00521-018-3647-2.

[23] H.-Y. Yang, X.-Y. Wang, Y. Zhang, and M. E-nuo, “Robust digital watermarking in PDTDFB domain based on least squares support vector machine,” *Eng Appl Artif Intell*, vol. 26, no. 9, pp. 2058–2072, Oct. 2013, doi: 10.1016/j.engappai.2013.04.014.

[24] V. S. Verma, R. K. Jha, and A. Ojha, “Digital watermark extraction using support vector machine with principal component analysis based feature reduction,” *J Vis Commun Image Represent*, vol. 31, pp. 75–85, Aug. 2015, doi: 10.1016/j.jvcir.2015.06.001.

[25] S. Vairaprakash and A. Shenbagavalli, “A Discrete Rajan Transform-based robustness improvement encrypted watermark scheme backed by Support Vector Machine,” *Computers & Electrical Engineering*, vol. 70, pp. 826–843, Aug. 2018, doi: 10.1016/j.compeleceng.2017.12.029.

[26] X.-Y. Wang, E.-N. Miao, and H.-Y. Yang, “A new SVM-based image watermarking using Gaussian–Hermite moments,” *Appl Soft Comput*, vol. 12, no. 2, pp. 887–903, Feb. 2012, doi: 10.1016/j.asoc.2011.10.003.

[27] H. Peng, J. Wang, and W. Wang, “Image watermarking method in multiwavelet domain based on support vector machines,” *Journal of Systems and Software*, vol. 83, no. 8, pp. 1470–1477, Aug. 2010, doi: 10.1016/j.jss.2010.03.006.

[28] S. Ramly, S. A. Aljunid, and H. Shaker Hussain, “SVM-SS Watermarking Model for Medical Images,” in *Digital Enterprise and Information Systems*, Ezendu Ariwa and Eyas El-Qawasmeh, Eds., Springer Nature, 2011, pp. 372–386. doi: 10.1007/978-3-642-22603-8_34.

[29] R. Choudhary and G. Parmar, “A robust image watermarking technique using 2-level discrete wavelet transform (DWT),” in *2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS)*, IEEE, Nov. 2016, pp. 120–124. doi: 10.1109/CCIntelS.2016.7878213.

[30] S. S. Gonge and A. Ghatol, “Composition of DCT-SVD Image Watermarking and Advanced Encryption Standard Technique for Still Image,” in *Intelligent Systems Technologies and Applications*, 2016, pp. 85–97. doi: 10.1007/978-3-319-47952-1_7.

[31] L. Laouamer, M. AlShaikh, L. Nana, and A. C. Pascu, "Robust watermarking scheme and tamper detection based on threshold versus intensity," *Journal of Innovation in Digital Ecosystems*, vol. 2, no. 1–2, pp. 1–12, Dec. 2015, doi: 10.1016/j.jides.2015.10.001.

[32] A. Karmakar, A. Phadikar, B. S. Phadikar, and G. Kr. Maity, "A blind video watermarking scheme resistant to rotation and collusion attacks," *Journal of King Saud University - Computer and Information Sciences*, vol. 28, no. 2, pp. 199–210, Apr. 2016, doi: 10.1016/j.jksuci.2014.06.019.

[33] R. Sinhal and I. A. Ansari, "Machine learning based multipurpose medical image watermarking," *Neural Comput Appl*, vol. 35, no. 31, pp. 23041–23062, Nov. 2023, doi: 10.1007/s00521-023-08457-5.

[34] R. Sinhal, D. K. Jain, and I. A. Ansari, "Machine learning based blind color image watermarking scheme for copyright protection," *Pattern Recognit Lett*, vol. 145, pp. 171–177, May 2021, doi: 10.1016/j.patrec.2021.02.011.

[35] A. Rai and H. V. Singh, "Machine Learning-Based Robust Watermarking Technique for Medical Image Transmitted Over LTE Network," *Journal of Intelligent Systems*, vol. 27, no. 1, pp. 105–114, Jan. 2018, doi: 10.1515/jisys-2017-0068.

[36] F. Meng, H. Peng, Z. Pei, and J. Wang, "A Novel Blind Image Watermarking Scheme Based on Support Vector Machine in DCT Domain," in *2008 International Conference on Computational Intelligence and Security*, IEEE, Dec. 2008, pp. 16–20. doi: 10.1109/CIS.2008.20.

[37] A. Rai and H. V. Singh, "SVM based robust watermarking for enhanced medical image security," *Multimed Tools Appl*, vol. 76, no. 18, pp. 18605–18618, Sep. 2017, doi: 10.1007/s11042-016-4215-3.

[38] M. F. Kazemi, M. A. Pourmina, and A. H. Mazinan, "Analysis of watermarking framework for color image through a neural network-based approach," *Complex & Intelligent Systems*, vol. 6, no. 1, pp. 213–220, Apr. 2020, doi: 10.1007/s40747-020-00129-4.

[39] R. Mehta, K. Gupta, and A. K. Yadav, "An adaptive framework to image watermarking based on the twin support vector regression and genetic algorithm in lifting wavelet transform domain," *Multimed Tools Appl*, vol. 79, no. 25–26, pp. 18657–18678, Jul. 2020, doi: 10.1007/s11042-020-08634-x.

[40] P. Singh and B. Raman, "A secured robust watermarking scheme based on majority voting concept for rightful ownership assertion," *Multimed Tools Appl*, vol. 76, no. 20, pp. 21497–21517, Oct. 2017, doi: 10.1007/s11042-016-4006-x.

[41] A. M. Abdelhakim, H. I. Saleh, and A. M. Nassar, "A quality guaranteed robust image watermarking optimization with Artificial Bee Colony," *Expert Syst Appl*, vol. 72, pp. 317–326, Apr. 2017, doi: 10.1016/j.eswa.2016.10.056.

[42] C. Wang, X. Wang, C. Zhang, and Z. Xia, "Geometric correction based color image watermarking using fuzzy least squares support vector machine and Bessel K form distribution," *Signal Processing*, vol. 134, pp. 197–208, May 2017, doi: 10.1016/j.sigpro.2016.12.010.

[43] S. Behnia, M. Yahyavi, and R. Habibpourbisafar, "Watermarking based on discrete wavelet transform and q - deformed chaotic map," *Chaos Solitons Fractals*, vol. 104, pp. 6–17, Nov. 2017, doi: 10.1016/j.chaos.2017.07.020.

[44] C. N. Mooers, "Preventing Software Piracy," *Computer (Long Beach Calif)*, vol. 10, no. 3, pp. 29–30, Mar. 1977, doi: 10.1109/C-M.1977.217671.

[45] I. A. Ansari and M. Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC," *Pattern Recognit Lett*, vol. 94, pp. 228–236, Jul. 2017, doi: 10.1016/j.patrec.2016.12.010.

[46] Ritu Agrawal and M. Sharma, "Medical Image Watermarking Technique in the Application of E- diagnosis Using M-Ary Modulation," *Procedia Comput Sci*, vol. 85, pp. 648–655, 2016, doi: 10.1016/j.procs.2016.05.249.

[47] N. Mohananthini and G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms," *Journal of Electrical Systems and Information Technology*, vol. 3, no. 1, pp. 68–80, May 2016, doi: 10.1016/j.jesit.2015.11.009.

[48] T. Huynh-The, O. Banos, S. Lee, Y. Yoon, and T. Le-Tien, "Improving digital image watermarking by means of optimal channel selection," *Expert Syst Appl*, vol. 62, pp. 177–189, Nov. 2016, doi: 10.1016/j.eswa.2016.06.015.

[49] Y. AL-Nabhani, H. A. Jalab, A. Wahid, and R. M. Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network," *Journal of King Saud University - Computer and Information Sciences*, vol. 27, no. 4, pp. 393–401, Oct. 2015, doi: 10.1016/j.jksuci.2015.02.002.

[50] P.-T. Yu, H.-H. Tsai, and J.-S. Lin, "Digital watermarking based on neural networks for colour images," *Signal Processing*, vol. 81, no. 3, pp. 663–671, Mar. 2001, doi: 10.1016/S0165-1684(00)00239-5.

[51] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimed Tools Appl*, vol. 77, no. 4, pp. 4863–4882, Feb. 2018, doi: 10.1007/s11042-016-3862-8.

[52] A. Zear, A. K. Singh, and P. Kumar, "Robust watermarking technique using back propagation neural network: a security protection mechanism for social applications," *International Journal of Information and Computer Security*, vol. 9, no. 1/2, p. 20, 2017, doi: 10.1504/IJICS.2017.10003597.

[53] M. Vafaei, H. Mahdavi-Nasab, and H. Pourghassem, "A new robust blind watermarking method based on neural networks in wavelet transform domain," *World Appl Sci J*, vol. 22, no. 11, pp. 1572–1580, 2013, doi: 10.5829/idosi.wasj.2013.22.11.2828.

[54] D. Li, L. Deng, B. Bhooshan Gupta, H. Wang, and C. Choi, "A novel CNN based security guaranteed image watermarking generation scenario for smart city applications," *Inf Sci (N Y)*, vol. 479, pp. 432–447, Apr. 2019, doi: 10.1016/j.ins.2018.02.060.

[55] A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network," *Future Generation Computer Systems*, vol. 86, pp. 926–939, Sep. 2018, doi: 10.1016/j.future.2016.11.023.
[56] N. Ramamurthy and S. Varadarajan, "Robust Digital Image Watermarking Using Quantization and Back Propagation Neural Network," 2012.
[57] Y. Zhang, "Blind Watermark Algorithm Based on HVS and RBF Neural Network in DWT Domain," 2009.
[58] C.-T. Yen and Y.-J. Huang, "Frequency domain digital watermark recognition using image code sequences with a back-propagation neural network," *Multimed Tools Appl*, vol. 75, no. 16, pp. 9745–9755, Aug. 2016, doi: 10.1007/s11042-015-2718-y.
[59] M. Ahmadi *et al.*, "ReDMark: Framework for Residual Diffusion Watermarking on Deep Networks," Oct. 2018. http://arxiv.org/abs/1810.07248

BIOGRAPHIES OF AUTHORS

Sambhaji Marutirao Shedole is currently a PhD Research Scholar in the School of Computer Science and Engineering at Vellore Institute of Technology, Vellore. He has received his MTech in Computer Science and Engineering from JNTU University, Hyderabad, India. He received his BE in Computer Science and Engineering from Dr Babasaheb Ambedkar Marathwada University, Maharashtra, India. His main research includes digital watermarking, image processing, data hiding, information security, deep learning, machine learning, etc. He can be contacted at email: sambhajis.maruthirao2015@vit.ac.in.

V. Santhi Received her PhD in Computer Science and Engineering from VIT University, Vellore, India. She has pursued her MTech in Computer Science and Engineering from Pondicherry University, Puducherry. She has received her BE in Computer Science and Engineering from Bharathidasan University, Trichy, India. Currently, she is working as a professor at the School of Computing Science and Engineering at VIT University, Vellore, India. She has published many articles in national and international journals. Also, she has published many chapters in different books published by international publishers. She is a senior member of IEEE, and she is a member of many professional bodies like CSI, ISTE, IACSIT, IEEE, and IAENG. Her areas of research include image processing, digital signal processing, digital watermarking, data compression, data mining and computational intelligence. She can be contacted at email: vsanthi@vit.ac.in