ISSN: 2581-3404 (Online) **IF: 5.445 (SJIF)**
IJIRTM, Volume-7, Issue-6, November-2023.

A Detailed Survey on Robust Digital Image Watermarking Techniques

Rakesh Kumar Verma[1], Dr. Daya Shankar Pandey[2], Dr. Varsha Namdeo[3]
rakeshvermabplsrk@gmail.com[1], dayashankar.rkdfist@gmail.com[2], varsha_namdeo@yahoo.com[3]
Computer Science & Engineering, Sarvepalli Radhakrishnan University, Bhopal, Madhya Pradesh, India[1]
Computer Science & Engineering, Sarvepalli Radhakrishnan University, Bhopal, Madhya Pradesh, India[2]
Computer Science & Engineering, Sarvepalli Radhakrishnan University, Bhopal, Madhya Pradesh, India[3]

Abstract: *Digital watermarking has emerged as a powerful and versatile technique for safeguarding digital content through copy protection, copyright enforcement, medical applications, data authentication, fingerprinting, and more. This method involves the embedding of a specific information element, known as a watermark, within the original data, which can encompass various forms, including images, videos, audio, and text. The requirements of a watermarking system vary depending on the nature of the host media and its intended purpose. This research paper presents a comprehensive overview of digital watermarking, highlighting its fundamental characteristics, evaluation metrics, and current real-world applications. Furthermore, it conducts an extensive survey of existing literature on digital image watermarking, delving into optimization techniques. Finally, the paper offers a standardized framework for the design of watermarking methods that meet the essential design criteria for a wide range of applications.*

Keywords:- Digital Watermarking, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Particle Swarm Optimization (PSO), Robustness, attacks.

Introduction

The proliferation of multimedia data and advancements in Internet technology have made it easier for users to store, duplicate, and distribute digital content for various applications [1]. However, safeguarding digital content for security and copyright protection has become increasingly challenging in today's landscape [2]. This challenge is compounded by the rise in cybercrimes, such as identity theft, illegal copying and distribution of data, and privacy breaches [3]. To address these concerns, techniques like steganography and watermarking have emerged as effective methods for securing multimedia content [4].

Steganography, often referred to as the art of data concealment, involves hiding information in a manner that only the intended recipients can decipher the hidden message [5]. This approach offers a significant advantage as it conceals the secret data within the host data, making it difficult for attackers to detect any visible alerts. Nevertheless, steganography faces limitations due to bandwidth constraints [6]. As a result, digital watermarking techniques have been developed by various researchers to provide copyright protection and content authentication for multimedia data. In this method, various types of digital data are embedded within images to enhance their security and privacy while preserving the visual quality of the original data [7]. Digital watermarking offers

additional features such as protection against tampering, access control, ownership authentication, non-repudiation, indexing, and memory and bandwidth efficiency [8].

Digital watermarking technology serves as an effective means to protect the copyrights of digital images, ensure image/content authenticity, monitor broadcasts, and facilitate medical applications. It involves permanently embedding digital data or patterns (watermarks) into other digital multimedia, including audio, video, and images, to safeguard the owner's rights. To prove ownership or establish copyright, the watermark is extracted and verified by the rightful owner.

The process of digital watermarking entails the alteration of multimedia data by adding information to the host media for copyright protection [9]. The system begins by taking the host image and embedding the watermark image into it using an embedding algorithm and a key. Subsequently, the watermarked image is transmitted over a communication channel. Finally, the system retrieves the watermark image by employing a watermark extraction algorithm and the associated key. Figure 1 illustrates this procedure.

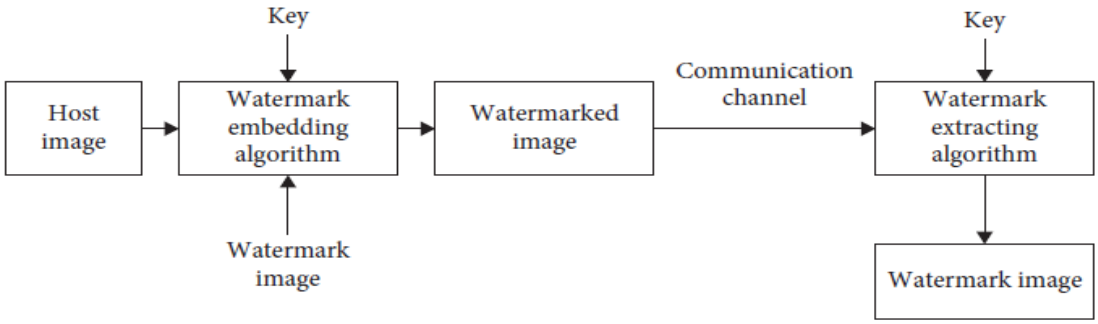

Figure 1: Watermark embedding and extraction Process.

II. Characteristics of Watermarking

The Internet and multimedia technologies have facilitated the duplication, transmission, and distribution of digital images across networks. To counteract unauthorized access and ensure data integrity, digital image watermarking techniques have been developed to embed information within the host media [10]. For such systems to be effective, they need to meet certain criteria. Among these, four fundamental requirements stand out: imperceptibility, robustness, capacity, and security. Figure 2 provides a visual representation of these key requirements.

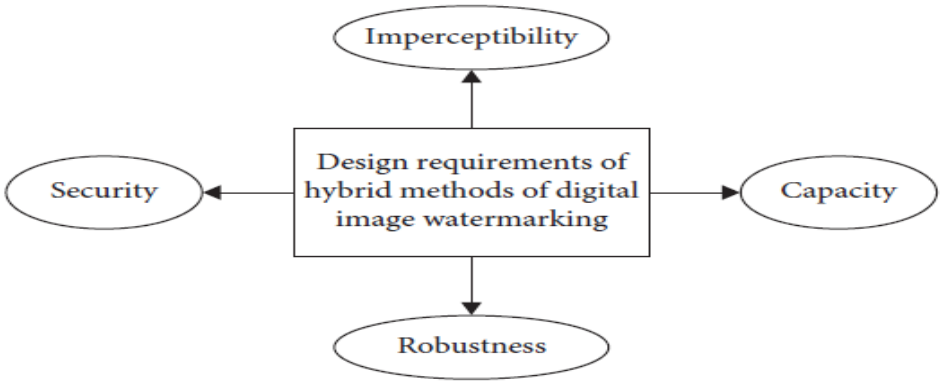

Figure 2: Characteristics of watermarking technique.

The imperceptibility criterion is a vital component of hybrid digital image watermarking methods, serving as a measure of the system's performance. It implies that the watermarked image should appear visually identical to the host image, even after potential degradation in brightness or contrast, making them perceptually indistinguishable to the human eye [11]. Robustness is another crucial requirement, ensuring that the watermark image remains detectable despite the application of common image processing operations. These operations encompass scanning, printing, scaling, translation, spatial filtering, rotation, color mapping, and lossy compression [12]. Robustness can be further categorized into robust, fragile, and semi-fragile, depending on the specific application. Payload capacity assesses the quantity of embedded information in relation to the host image's size. However, inserting additional watermark bits into the host image can be a challenging task contingent upon practical use cases [13]. Security stands as a paramount design requirement for applications like fingerprinting, copyright protection, data authentication, and digital content tracking. It is achieved through the encryption of the watermark image using various encryption techniques. The identified applications, based on their design requirements, are summarized in Table 1.

Table 1: Design requirements and their corresponding applications.

Requirements	Applications
Imperceptibility	Copyright protection and fingerprinting
Robustness	Copyright protection, content authentication, and integrity verification
Security	Copyright protection, content authentication, indexing, medical applications, and telemedicine data exchange.
Capacity	Tamper detection and integrity of medical images
Computational cost	Protection of microscopy images.
False positive	Copy control and ownership
Watermark keys	Copyright protection
Tamper resistance	Authenticity and copyright integrity
Reversibility	Medical applications

III. Domain Techniques of Watermarking

The process of embedding watermark information can be executed through either spatial or transform domains. In the spatial domain, manipulation of pixel values facilitates the direct embedding of data [14]. Spatial domain techniques are known for their simplicity in terms of computational complexity. Notable methods in the spatial domain include the least significant bit (LSB) technique, spread spectrum, and correlation-based approaches [15].
In contrast, watermarking in the transform domain offers heightened resilience against image processing attacks, albeit at the cost of increased computational complexity [16]. Transform-based techniques are more suitable for applications where robustness and imperceptibility are paramount. Prominent techniques in the transform domain

include the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Lifting Wavelet Transform (LWT), Karhunen-Loeve Transform (KLT), and Singular Value Decomposition (SVD).
The primary methods in both the spatial and transform domains are detailed in Table 2.

Table 2: Types of Spatial and Transform domain based watermarking.

Spatial Domain Techniques	
LSB	One of the simplest methods where message bits embedded in LSB of cover media. Not robust against attacks.
Spread Spectrum	Data are hidden in frequency bins in a secure and non-predictable manner
Correlation Based	It is based on correlation properties of additive pseudo random noise pattern.
Patchwork	Pixel position is chosen under pseudo random generated number.
Transform Domain Techniques	
DCT	Data can be easily embedded in lower and middle sub bands
DWT	Multi-resolution, Multi-scaling, good energy compaction, and reducing blocking artifact problem.
KLT	Reversible linear transform which uses linear statistical properties of vector and optimally de-correlates data.
LWT	Takes less memory requirement, good reconstruction, low computational complexity, and low aliasing effect.
SVD	Secure and stable, and high computational cost.

Spatial domain-based methods offer convenience, efficiency, and resilience against basic attacks such as cropping and noise addition. However, these methods exhibit limitations as they are not robust against most signal processing attacks, and incorporating characteristics of the Human Visual System (HVS) is challenging. To address these limitations, various techniques have been developed based on the transform domain, including the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

- **Discrete Cosine Transform (DCT)** - DCT is widely utilized in image and video processing. It is obtained by applying 1D-DCT in both horizontal and vertical directions. Following DCT transformation, a significant portion of the image's energy is concentrated in the top-left corner coefficient, known as the direct current (DC) coefficient, while the values of coefficients gradually decrease from the top-left to the bottom-right [17]. This property makes DCT a fundamental component of image and video compression. Most early DCT-based watermarking methods directly embedded the watermark into DCT coefficients using a fixed embedding strength, like quantization step [18], applied uniformly to all blocks.

- **Discrete Wavelet Transform (DWT)** - DWT offers a more accurate representation of the HVS compared to DCT, thanks to its multi-resolution description of the image. It also demonstrates robustness against various attacks, including additive noise, resizing, and halftoning. DWT decomposes the image into four subbands: LL contains the majority of the image's energy, while LH, HL, and HH represent subbands containing image details [19]. The image can be decomposed into multiple levels by repeatedly decomposing the LL channel. Higher levels contain more detailed information in the corresponding subbands.

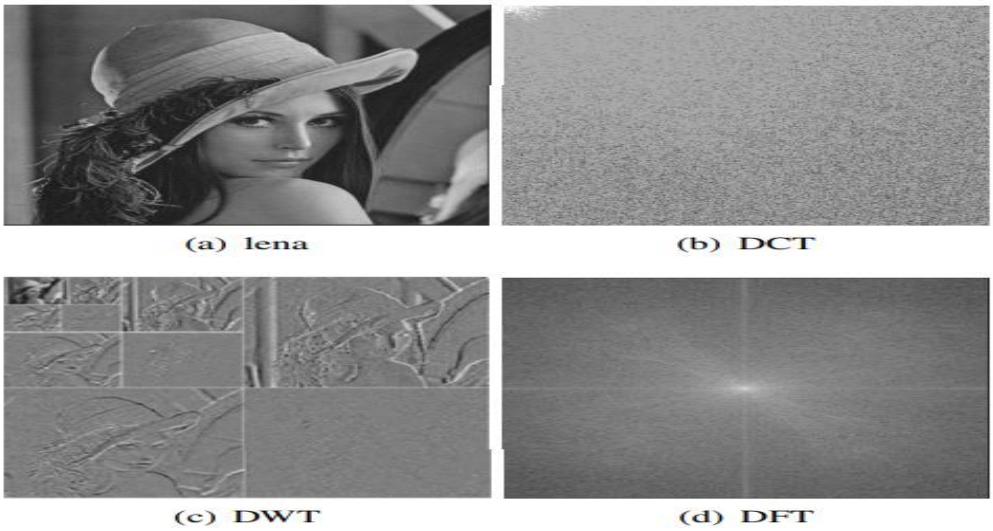

Figure 3: Three spectrum examples of Lena image in DCT, DWT, and DFT domain, respectively.

- **Discrete Fourier Transform (DFT)** - DFT is resistant to many geometric processing operations because it maintains magnitude invariance, making it a suitable host for carrying secret information. In the case of DFT, an image is represented as complex-valued Fourier coefficients, expressed in terms of amplitude and phase. The central component, a low-frequency element, holds particular significance in this regard.

IV. Types of Methodologies Used In The Watermarking Technique

Modern watermarking algorithms increasingly utilize soft computing techniques to strike a balance between robustness, payload capacity, and imperceptibility in watermark systems [20]. These soft computing methods find application not only in the embedding stage but also in other phases such as extraction and pre-processing. In the pre-processing phase, soft computing techniques are employed before the embedding process [21]. This section explores various soft computing applications, including Neural Network (NN), Genetic Algorithm (GA), Support Vector Machine (SVM), Principal Component Analysis (PCA), Meta-Heuristic approaches, Deep Learning (DL), and Fuzzy Logic (FL) in the context of watermarking [22]. The diverse applications of soft computing in watermarking are detailed below.

- **Support Vector Machine (SVM)** - SVM, a well-established supervised learning algorithm, is employed in stages such as watermark embedding, detection, and extraction [23]. SVM exhibits strong learning capabilities and generalization, rendering it a preferred choice in watermarking schemes.
- **Neural Network-** Neural networks play a central role in enhancing watermark robustness during embedding and extraction stages [24]. Various neural network models, including Artificial Neural Network (ANN), Back Propagation Neural Network (BPNN), Feed-Forward Neural Network (FFNN), Convolutional Neural

Network (CNN), Probabilistic Neural Network (PNN), Full Counter-Propagation Neural Network (FCPNN), and Radial Basis Function Neural Network (RBFNN), are commonly applied in watermarking techniques.

- **Genetic Algorithm (GA)** - GA is used to identify the optimal watermark embedding positions and enhance watermark strength and payload capacity [25]. GA serves as a powerful optimization tool, comprising key components such as random number generation, fitness function, selection (reproduction), crossover, and mutation operators.
- **Fuzzy Logic-** Fuzzy Logic finds application in various watermarking stages, including embedding and extraction, to improve watermark scheme performance [26]. Fuzzy Logic deals with linguistic variables and employs rules to convert them into system-understandable knowledge. Fuzzifier and Defuzzifier handle the conversion of variables into fuzzy quantities and vice versa. Fuzzy Inference System (FIS) maps input to output using fuzzy logic concepts.
- **Ant Colony Optimization**- Ant colony optimization is inspired by the behavior of ant colonies searching for food. Ants lay pheromones as they search for food, and the path to the food source is communicated to other ants. Ant colony optimization is a search-based technique where agents (ants) search for the best solution to a problem.
- **Particle Swarm Optimization (PSO)** - PSO is a swarm intelligence strategy that relies on the concept of swarms, inspired by the foraging behavior of birds. It has gained popularity as an effective search and optimization method, not requiring gradient knowledge of the function to be optimized. PSO utilizes simple mathematical operators and is motivated by the social behavior of birds [27]. Numerous scholars have further refined and automated various versions of the PSO algorithm.

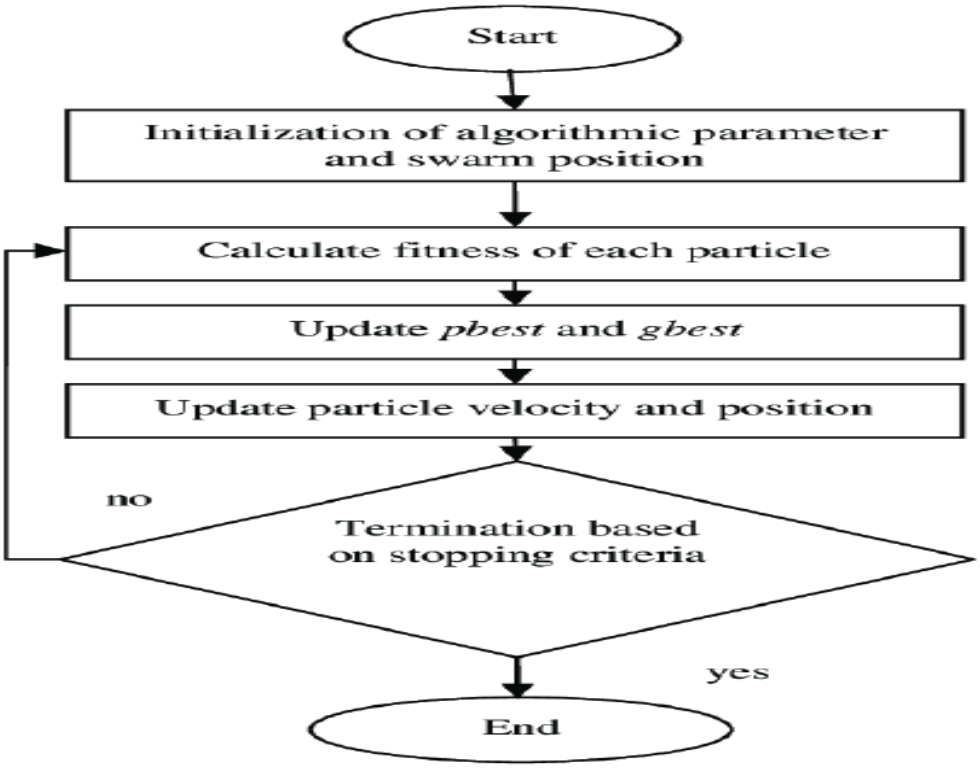

Figure 4: Working Flowchart of PSO Algorithm.

V. Literature Review

In the study conducted by Abdelhakim Assem Mahmoud and colleagues [13], a novel approach to digital image watermarking is introduced, utilizing the Discrete Cosine Transform domain for enhanced resistance against common watermarking attacks. This method involves a training process where a set of images is selected for watermark application, and optimization is achieved through the application of the Artificial Bee Colony algorithm. The study collects perceptual data, including optimal quality values and feature vectors representing the training images. Image features are extracted by evaluating the fitness function at various embedding strength levels.

In the research by Liu Shuai and co-authors [14], a digital watermarking algorithm is developed based on a combination of fractal encoding and the Discrete Cosine Transform (DCT) technique. This approach enhances the traditional DCT method by employing fractal encoding as the primary encryption step, with the encoded parameters used in the DCT method as the secondary encryption. The initial application of the fractal encoding method involves encoding a private image using private scales, and the resulting encoding parameters are used for digital watermarking.

Huang Xiaonan and their team [15] discuss a novel watermarking scheme based on scan chain ordering, designed to offer robust copyright protection for hard IP cores. During the scan chain ordering process for test power optimization, watermark bits influence the choice between different connection styles for specific pairs of scan cells during the minimization process, depending on the output of the IP core under the selected test vector.

In the research by Khazraei Amir and colleagues [16], the study addresses the challenge of replay attacks in a homogeneous multi-agent system. Information exchange among agents follows a network topology, with each agent tasked to meet both local and global objectives. Each agent is equipped with a local estimator and an anomaly detector, which provide stability conditions for the attacked system when replay attacks affect a part of the network.

Deeba Farah and researchers [17] employ the least significant bit (LSB) to embed a watermark in pixel data. However, recognizing that LSB-based methods are not robust in attack-prone environments and lossless compression, they utilize an Artificial Neural Network (ANN) to detect the presence of sensitive information and extract it from the source image. This approach inherently requires ongoing training, retraining, and adaptation for different applications.

Ariatmanto Dhani et al. [18] propose an image segmentation technique where images are divided into non-overlapping 8x8 pixel blocks. The pixel values are transformed using discrete cosine transformations (DCT), and DCT coefficients in the mid-frequency range are selected. Watermark bits are embedded following specific rules based on the average of selected DCT blocks.

Rakhmawati Lusia and her team [19] address data security challenges by introducing a method of sensitive watermarking. This approach leverages the watermark's sensitivity to alterations, making it useful for tamper detection and image recovery when an embedded image is modified by different users.

Huynh-The and colleagues [20] present a novel blind image watermarking system capable of learning and effectively countering attack patterns using a deep convolutional encoder-decoder network. This method conceals a dual watermark image within specific wavelet blocks using optimal encoding rules, minimizing image quality degradation.

Valandar Milad Yousefi and team [21] employ bifurcation diagrams, Lyapunov patterns, spider web plots, and direction graphs to demonstrate the chaotic behavior of the discussed map. Results from DIEHARD, ENT, and NIST test suites indicate that the proposed watermarking algorithm effectively resists image processing attacks.

Cristin Rajan and co-authors [22] introduce a fraud detection scheme based on supervised learning, combining support vector neural networks with the fruit fly optimization algorithm. The process involves surface descriptor

analysis, face detection using the Viola-Jones algorithm, and feature extraction with Gabor filters, wavelets, and texture operators.

In the work by Kora Padmavathi and colleagues [23], the authors discuss the use of Wavelet Coherence (WTC) for ECG signal analysis. WTC measures the similarity between two waveforms in the frequency domain, and the features derived from WTC are optimized using the Firefly algorithm before being fed into a Levenberg Marquardt Neural Network (LM NN) classifier.

Ronan David and team [24] focus on automating noise standardization, equalization, and dynamic range compression to enhance audio mixing quality by reducing inter-channel auditory masking. Their approach extends the MPEG psychoacoustic model's masking threshold algorithm for estimating inter-channel auditory masking, and they propose an intelligent system for masking minimization using mathematical optimization.

In the research by Kumari R. Radha and colleagues [25], a secure digital watermarking framework, abbreviated as S-DWF, is introduced. This framework employs an image fluctuation-based degradation followed by a key-based watermarking process, implemented and assessed through numerical computation.

Abodena Omar and his team [26] utilize a two-level Discrete Wavelet Transform (DWT) followed by Fast Walsh-Hadamard Transform (FWHT) for the analysis of the host image's red channel. The FWHT coefficients are divided into non-overlapping 4x4 blocks, with watermark data embedded using the upper Hessenberg matrix's first row and first column elements. The feasibility and strength of this approach are evaluated using peak signal-to-noise ratio, normalized cross-correlation, and structural similarity index.

Bhowmik Deepayan et al. [27] discuss the relationship between distortion, measured as mean square error (MSE), and watermark embedding modification. The study establishes a direct proportionality between MSE and the total energy of selected wavelet coefficients for watermark embedding alteration, assuming the orthogonality of the discrete wavelet transform."

VI. Attacks on Watermarks

The vast body of literature on various watermarking techniques highlights that extracting or altering concealed watermark data is not an overly challenging task for individuals as information traverses the communication channel. However, a crucial characteristic is the need for watermarking systems to exhibit robustness against potential attacks. Within a watermarking system, any form of processing that has the potential to negatively affect watermark detection or the integrity of the communication conveyed by the watermark is termed an "attack." Consequently, the manipulated watermark data is categorized as "attacked data." These attacks, whether deliberate or accidental, introduce distortions into the watermarked image and encompass a variety of categories such as active attacks, passive attacks, geometric attacks, removal attacks, protocol attacks, cryptographic attacks, blind attacks, informed attacks, tampering attacks, simple attacks, attacks based on key estimation, destruction attacks, and synchronization attacks, among others, as depicted in Figure 5. This sub-section elaborates on some of the prevalent image watermarking attacks.

- **Active Attacks-** Active attacks occur when a malicious actor identifies and exploits vulnerabilities within a watermark detection function, often resulting in the removal or destruction of the watermark. Simply by gaining access to the watermark embedding function, an adversary can easily distort the watermarked image. Common active attacks in image watermarking encompass elimination, collusion, masking, distortion, forgery, copy, ambiguity, and scrambling attacks.
- **Passive Attacks-** Passive attacks involve an attacker attempting to determine the presence or absence of a given watermark without actively seeking to remove or alter it. The attacker's focus is on discerning the watermark's existence and obtaining the associated information. Passive attacks come in various levels and serve different objectives, crucial in the context of covert communication.

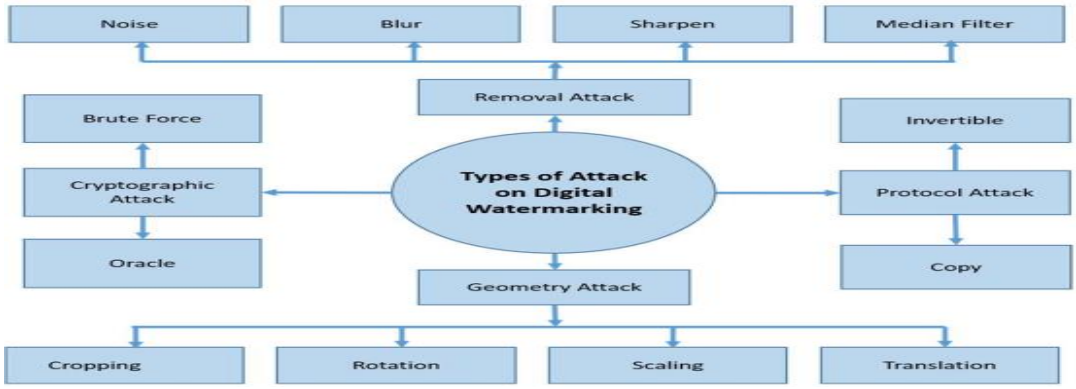

Figure 5: Types of Attacks on Digital Watermarking.

- **Removal Attacks**- Removal attacks aim to eliminate the watermark from the host image without utilizing the key used in the watermark embedding. This category includes blind watermark removal, collusion attacks, remodulation, interference attacks, noise attacks, denoising, quantization, and lossy compression, among other methods. These attacks may not entirely eradicate the watermark but significantly damage the embedded watermark information.
- **Geometric Attacks**- Conventional watermarking algorithms are considered efficient if they exhibit resilience against intentional or unintentional geometric attacks. Geometric attacks do not aim to remove the watermark image itself but rather seek to distort the synchronization of the watermark detector using the inserted information. Unlike removal attacks, these attacks hinder the synchronization process needed to recover the embedded watermark information, resulting in synchronization errors between the original watermark and the extracted watermark during the extraction process.
- **Protocol Attacks**- Protocol attacks directly target the watermarking application and may take the form of invertible attacks, ambiguity attacks, or copy attacks. Invertible watermark attacks occur when the attacker subtracts the watermark from the watermarked data, falsely claiming ownership of the watermarked data and creating ambiguity regarding the original owner.
- **Cryptographic Attacks**- Cryptographic attacks include security attacks and oracle attacks, which aim to breach the security of watermarking schemes by removing the embedded watermark information. Brute-force search techniques mislead the watermark by embedding misleading secret information. Oracle attacks, on the other hand, create non-watermarked signals with a publicly available watermark detector device. Applications must mitigate these cryptographic attacks due to their high computational complexity.

VII. Cost Evaluation of Different Attacks

Cost-effectiveness of Attacks in Digital Image Watermarking: Evaluating the cost-effectiveness of various attacks on digital image watermarking, typically based on computational complexity, involves considering the resources, namely time and memory space, required to successfully execute an attack. These assessments take into account the key and embedding algorithms integral to watermarking, as they are significant parameters for an attack. Different attacks are associated with varying parameters, and the key cost (k), embedding cost (E), cost to remove the watermark (R), geometric distortion cost (G), and new embedding cost generated by an attacker (N) are among the key factors determining cost-effectiveness. The table below provides a comprehensive representation of these cost-effective parameters:

- Cost of Finding the Key (k) - This parameter encompasses the effective key length, serving as a measure of the security level of the watermarking algorithm.
- Embedding Cost (E) - This factor directly impacts the robustness and imperceptibility of the watermarking algorithm, estimating the strength of watermark embedding.
- Cost to Remove the Watermark (R) - This cost represents the resources required for an attacker to successfully remove the watermark from the host image without utilizing the key employed in the watermark embedding algorithm.
- Geometric Distortion Cost (G) - This factor pertains to the cost associated with introducing geometric distortions during an attack.
- New Embedding Cost Generated by an Attacker (N) - This parameter relates to the cost incurred when an attacker generates new embeddings in the watermarked image.

Table 3: Cost of different attacks.

Attacks	**Cost**
Active	K + E + R
Passive	K + E
Removal	R
Geometric	K + E + G
Protocol	K + E + R + N
Cryptographic	K

VIII. Applications of Watermarking

Copyright Protection- In the digital landscape, images are easily shared and widely available on the internet, making them susceptible to commercial use without proper authorization. To safeguard the copyright of digital content, the utilization of Digital Watermarking is indispensable. Digital watermarks can be embedded in the data to serve as a means of identifying the rightful copyright owner.

Fingerprinting- Fingerprinting, within the realm of digital watermarking, serves as a technique for embedding distinct identifiers. These fingerprints should be highly resistant to tampering. The information embedded through fingerprinting is associated with individual customers. It is through this fingerprinting process that it becomes possible to identify authorized customers involved in the unauthorized distribution of copyrighted data, thereby breaching established agreements.

Figure 6: Applications of Digital Watermarking.

Copy Control- Digital watermarking serves as an effective tool for preventing the unauthorized duplication of digital data. Devices designed for replication can detect these watermarks, signalling any copying attempts and thus helping to control and deter illegal duplication.

Broadcast Monitoring- With the exponential growth in the availability and accessibility of media content, much of it being distributed over the internet, it has become increasingly vital for content owners and copyright holders to trace the actual distributors of their content. Digital watermarking plays a pivotal role in enabling this monitoring and identification process.

Medical Application- Visible watermarking can be utilized for embedding a patient's name within medical reports such as MRI scans, CT scans, or X-ray reports. These reports are integral to a patient's treatment, and the application of visible watermarking helps prevent any mix-up of medical reports, ensuring accurate patient care.

Electronic Voting System- With the widespread penetration of the internet from major cities to remote villages, electronic voting systems have emerged as a means to conduct elections while taking security concerns into account. This modern approach allows for secure and efficient election processes.

Remote Education- Small villages often grapple with a shortage of teachers, presenting a significant challenge to education. To address this issue, the adoption of Smart Technology is crucial for facilitating distance learning. Digital watermarking plays a pivotal role in ensuring the secure and authentic transmission of study materials over the internet, contributing to the effectiveness of remote education.

IX. Conclusions

Digital image watermarking, employing a diverse array of techniques, serves as a crucial tool for image authentication, integrity verification, tamper detection, copyright protection, and digital image security. The efficacy of watermarked images is assessed based on robustness, imperceptibility, security, and capacity. This article offers a comprehensive overview of digital image watermarking systems, accompanied by an in-depth classification and characterization. It also addresses significant challenges and potential solutions concerning various attacks to stimulate further research in this field. Furthermore, we present an analysis of various existing watermarking techniques in tabular format. Nonetheless, the realm of digital image watermarking grapples with persistent security challenges, and the integration of IoT and blockchain-based authentication schemes presents a compelling frontier for researchers. Hence, future endeavours could explore amalgamating diverse techniques across different domains to satisfy the three fundamental requirements mentioned above. Additionally, to enhance robustness and security, researchers should direct their efforts towards pioneering advanced methodologies.

REFERENCES

[1] Amrit P, Singh AK, “Survey on watermarking methods in the artifcial intelligence domain and beyond” Computer Communication, 2022 188:52–65

[2] Anand A, Singh AK, Zhou H, “A survey of medical image watermarking: state-of-the-art and research directions” Med Inform Process Secur: Tech Appl, 2023, 14:325–360. https://doi.org/10.1049/PBHE044E_ch14

[3] Anand A, Kumar Singh A, “A comprehensive study of deep learning-based covert communication” ACM Trans Multimedia Comput Commun Appl (TOMM), 2022, 18(2s):1–19

[4] Bagheri M, Mohrekesh M, Karimi N, Samavi S, Shirani S, Khadivi P (2020) Image watermarking with region of interest determination using deep neural networks. In 2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, pp 1067–1072

[5] Chen J, Zhang J, Debattista K, Han J, “Semi-supervised unpaired medical image segmentation through task-afnity consistency”, IEEE Trans Med Imaging, 2023, 42(3):594–605

[6] Ding W, Ming Y, Cao Z, Lin CT, "A generalized deep neural network approach for digital watermarking analysis. IEEE Trans Emerg Top Comput Intell, 2021, 6(3):613–627
[7] Fkirin A, Attiya G, El-Sayed A, Shouman MA, "Copyright protection of deep neural network models using digital watermarking: a comparative study", Multimedia Tools Appl, 2022, 81(11):15961–15975
[8] Ge S, Xia Z, Fei J, Sun X, Weng J, "A robust document image watermarking scheme using deep neural network", arXiv preprint, 2022, arXiv:2202.13067
[9] Liu Y, Zhang D, Zhang Q, Han J, "Part-object relational visual saliency", IEEE Trans Pattern Anal Mach Intell, 2022, 44(7):3688–3704
[10] Mahapatra D, Amrit P, Singh OP, Singh AK, Agrawal AK, "Autoencoder convolutional neural network-based embedding and extraction model for image watermarking" J Electron Imaging, 2022, 32(2):021604
[11] Singh HK, Singh AK, "Comprehensive review of watermarking techniques in deep-learning environments", J Electron Imaging, 2023, 32(3):1–23
[12] Wang X, Ma D, Hu K, Hu J, Du L, "Mapping based residual convolution neural network for nonembedding and blind image watermarking. J Inform Secur Appl 2021, 59:102820
[13] Abdelhakim, Assem Mahmoud, and Mai Abdelhakim. "A time-efficient optimization for robust image watermarking using machine learning." Expert Systems with Applications 100 (2018): 197-210.
[14] Liu, Shuai, Zheng Pan, and Houbing Song. "Digital image watermarking method based on DCT and fractal encoding." IET image processing 11, no. 10 (2017): 815-821.
[15] Huang, Xiaonan, Aijiao Cui, and Chip-Hong Chang. "A new watermarking scheme on scan chain ordering for hard IP protection." In 2017 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-4. IEEE, 2017.
[16] Khazraei, Amir, Hamed Kebriaei, and Farzad Rajaei Salmasi. "Replay attack detection in a multi agent system using stability analysis and loss effective watermarking." In 2017 American Control Conference (ACC), pp. 4778-4783. IEEE, 2017.
[17] Deeba, Farah, She Kun, Fayaz Ali Dharejo, and Hira Memon. "Digital image watermarking based on ANN and least significant bit." Information Security Journal: A Global Perspective 29, no. 1 (2020): 30- 39.
[18] Ariatmanto, Dhani, and Ferda Ernawan. "An improved robust image watermarking by using different embedding strengths." Multimedia Tools and Applications: 1-27.
[19] Rakhmawati, Lusia, Wirawan Wirawan, and Suwadi Suwadi. "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability." EURASIP Journal on Image and Video Processing 2019, no. 1 (2019): 61.
[20] Huynh-The, Thien, Cam-Hao Hua, Nguyen Anh Tu, and Dong-Seong Kim. "Robust Image Watermarking Framework Powered by Convolutional Encoder-Decoder Network." In 2019 Digital Image Computing: Techniques and Applications (DICTA), pp. 1-7. IEEE, 2019.
[21] Valandar, Milad Yousefi, Milad Jafari Barani, and Peyman Ayubi. "A blind and robust color images watermarking method based on block transform and secured by modified 3-dimensional Hénon map." Soft Computing (2019): 1-24.
[22] Cristin, Rajan, John Patrick Ananth, and Velankanni Cyril Raj. "Illumination-based texture descriptor and fruitfly support vector neural network for image forgery detection in face images." IET Image Processing 12, no. 8 (2018): 1439-1449.
[23] Kora, Padmavathi, Ch Usha Kumari, and K. Meenakshi. "Heart Arhythmia Detection Using Wavelet Coherence and Firefly Algorithm." Int. J. Comput. Appl 975 (2018): 8887.
[24] Ronan, David, Zheng Ma, Paul Mc Namara, Hatice Gunes, and Joshua D. Reiss. "Automatic minimisation of masking in multitrack audio using subgroups." arXiv preprint arXiv:1803.09960 (2018).

[25] Kumari, R. Radha, V. Vijaya Kumar, and K. Rama Naidu. "S-DWF: An Integrated Schema for Secure Digital Image Watermarking." In Computer Science On-line Conference, pp. 25-34. Springer, Cham, 2019.
[26] Abodena, Omar, and Mary Agoyi. "Colour Image Blind Watermarking Scheme Based on Fast Walsh Hadamard Transform and Hessenberg Decomposition." Studies in Informatics and Control 27, no. 3 (2018): 339-348.
[27] Bhowmik, Deepayan, and Charith Abhayaratne. "Embedding distortion analysis in wavelet-domain watermarking." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 15, no. 4 (2019): 1-24.