iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72460

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

Securing Digital Media via Watermarking: Applications in Healthcare, Surveillance, Communication

Vinayak Raj Gupta[1], Tushar Basak[2], Angshuman Ghosh[3], Koushik Pal[4], Anurima Majumdar[5], Anirban Ghosal[6]
[1, 2, 3, 4, 5]*Department of Electronics and Communication Engineering, Guru Nanak Institute of Technology, Kolkata, India*
[6]*Department of Electronics and Communication Engineering, JIS College of Engineering, Kalyani, West Bengal, India*

Abstract: ***When digital media is pervaded in all of modern life including such critical areas as healthcare, surveillance and secure communication, the demand for strong, scalable and intelligent way for protecting the information embedded in digital media can never be more greatly felt. Digital watermarking has become a significant tool to embed invisible security features into multimedia data, providing authentication, tracing, and tamper resistance. This survey focuses on the applications to watermarking, considering its use in a comprehensive review of three important fields of interest, namely, medical imaging, surveillance systems and secure communications. The paper also emphasizes the specific needs and limitations of the scenarios, e.g., reversibility in the health care, real-time decision making in surveillance, and robustness in the communication network. An extensive review of the current state of the art, weighing advantages against drawbacks, is then introduced, paving the way for the proposition of a unified, domain-adaptive watermarking methodology, deployable across multiple sectors. The paper concludes with the open issues in the field, such as AI based watermarking, blockchain-based verification, 3D media protection and quantum watermarking. By refocusing from comparative techniques to applications, the goal of this review is to bring the innovative academic research toward security-driven applications. The learned insights provided play a role of a compass for investigators and practitioners targeting the next generation of secure, interoperable, and intelligent watermarking solutions.***

Keywords*: Digital Watermarking, Media Security, Healthcare Imaging, Surveillance, Secure Communication, Unified Framework, Blockchain, AI, Data Authentication*

I. INTRODUCTION

Multimedia data is now used more than ever before as a result of the quick digitization of information in fields including communication, healthcare, and surveillance. These days, digital photos and videos are essential to everyday tasks, from keeping track of medical information to keeping an eye on public areas and facilitating instantaneous communication. But this increasing reliance raises important questions about digital media's integrity, security, ownership, and authenticity.

Even though they work well to limit access to data, traditional encryption methods frequently fall short once the material is decoded or made available to the public. Digital watermarking, on the other hand, provides a supplementary solution that permanently protects data throughout its lifecycle by embedding invisible, secure information into the content. While preserving the host media's perceptual quality, this embedded data, often referred to as a watermark, might include timestamps, ownership credentials, tamper proof, and other verification information.

Digital watermarking's main advantage is its adaptability. It can be made to be fragile (for tamper detection), reversible (for sensitive applications like medical imaging), or strong (resistant to compression and attacks). This review's main focus is on how these characteristics have made it possible for it to be adopted in a range of application-specific scenarios.

We examine the function of watermarking as a security measure in three crucial areas in this paper:

Healthcare, where maintaining the integrity and confidentiality of medical images is essential; Surveillance, in which forensic and judicial procedures are supported by image authenticity; Communication systems use watermarking to make sure that data is sent safely and that copyright is enforced.

Instead of looking at algorithms or techniques in isolation, this review takes a descriptive, application-focused approach. It summarizes how watermarking has been used in real life, what problems still need to be solved, and how current research is working to solve them. This structure helps researchers and developers who want to use watermarking in mission-critical areas understand how to do it.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

II. FUNDAMENTAL OF DIGITAL WATERMARKING

Digital watermarking refers to the act of hiding information - digital information - (which is referred to as a watermark) within digital multimedia objects (images, video, audio, etc.), either visibly or invisibly, using one of several techniques. The primary purpose of a watermark in this context is to protect digital content by embedding what can be thought of as an invisible layer of additional metadata that can be extracted or verified later, thus revealing claims of ownership or authenticity, etc. The integrity of the content could even be verified using a digital watermark.

A. Basic Principles

A digital watermark could be thought of a binary or signal-based representation embedded directly into the media. There are two major domain approaches to the process of embedding a watermark into digital content:

- *Spatial Domain:* These techniques are characterized by directly changing the pixel values of an image. They are simple to implement, and quick to compute, but tend to lack a wider robustness. The simplest example is the Least Significant Bit (LSB) modification.
- *Transform Domain:* These watermarking techniques embed the watermark into the transformed coefficients of the media's content. Some examples of transform methods include Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD). These methods tend to be more resilient methods to compression noise and other normal signal processing operations.

B. Types of Watermarking

Digital watermarking based on application requirements can be classified into one of the types as follows:

- *Robust Watermarking:* It is designed to withstand attacks or manipulations like compression, filtering or cropping. Commonly used for copyright protection and forensic tracking.
- *Fragile Watermarking:* Sensitive to even the slightest alterations in the host media, making it the perfect choice for tamper detection.
- *Semi-fragile Watermarking:* Can be used to detect and reveal any tampering while preserving the integrity under certain conditions such as format conversion or mild compression.
- *Reversible Watermarking:* Accommodates an exact restoration of the original content, after removing the watermark. This is particularly relevant in the medical and legal fields, where the original data needs to be intact.

C. Watermarking System Model

- *Embedding Process:* The process of inserting the watermark into the host media, usually involves the use of an algorithm. A secret key may also be used to capture security.

Input: Original Image + Watermark + Secret Key → Output: Watermarked Image

- *Extraction or Detection Process:* The watermark is extracted (with odd without the original image) for input, to verify the authenticity, ownership or tamper of the digital media.

Input: Watermarked image (+ Key) → Output: Extracted Watermark

D. Performance Metrics

Different metrics can be used to measure and quantify watermarking effectiveness:

- *Imperceptibility:* There should be little to no noticeable difference in the visual quality of the image after embedding. Common measures include Peak Signal-to-Noise Ratio or Structural Similarity Index.
- *Robustness:* The watermark should survive common processes, for example, compression, resizing, or filtering.
- *Security:* The watermark should not be easily removable or easily forgeable.
- *Capacity:* Amount of information that can be embedded with no loss of quality.
- *Computation Complexity:* Particularly crucial for real-time processes, and also for embedded devices.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

III.DESCRIPTIVE REVIEW OF APPLICATION DOMAINS

A. Application of Watermarking in Healthcare Imaging

Healthcare is probably one of the most regulated and sensitive domains regarding the protection of digital information. The transference and protection of medical images such as MRI, CT scans, and X-ray images has become commonplace and involves the routine electronic capture, storage, sharing, and analysis of images. Even the slightest unauthorized alteration of a medical image, or unauthorized breach of confidentiality can lead to misdiagnosis, liability, or even violation of legislation aimed at safeguarding patients, as in the case of HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation).

Digital watermarking is a powerful method of securing digital integrity, confidentiality, and proofs of image authenticity in digital medical images without disrupting the clinical workflow or degrading image quality.

1) Use Cases and Real-world Applications:

- *Embedding Patient Identification:* Hospitals embed patient information (such as name, ID number, date and time, and clinical diagnosis) in diagnostic imaging. This guarantees that peer information is neither lost nor altered when conveyed from department-to-department or onto the cloud servers.
- *Tamper Detection of DICOM Images:* Fragile watermarks are a type of passive watermark used to detect image tampering in Digital Imaging and Communications in Medicine (DICOM) images. Any type of tamper to the compressed pixel-level data will break the fragile watermark.
- *Telemedicine and Teleradiology Security:* When medical images are shared for remote consultations and/or second opinions, the images are transmitted across a networking infrastructure. Watermarking of the medical images ensures that the transmitted image is able to be validated as the original image with identified peer tracking of potential manipulation.
- *Reversible Watermarking to Maintain Lossless Quality of Image Recoverability:* In diagnostic imaging, any distortion in imaging capture technique (even if very small) can have implications in clinical decision making. Thus, reversible watermarking is utilized, allowing the image to be returned to its original form post-identity verification.

2) Techniques Commonly Used in Healthcare:

TABLE I
TECHNIQUES COMMONLY USED IN HEALTHCARE

Technique	Purpose	Domain
LSB + Encryption	Lightweight patient data embedding	Spatial
DWT + SVD	Robust and invisible watermarking	Transform
Histogram Shifting	Reversible watermarking	Spatial
Difference Expansion	Reversible & high capacity	Hybrid

Transform domain techniques (e.g., Discrete Wavelet Transform with Singular Value Decomposition (DWT-SVD)) are often used for digital watermarking because of the introduced ability to maintain both invisibility and robustness. Specifically, by embedding watermark in the transformed coefficients instead of spatial domain leads to making the watermark resilient to common attacks (e.g. compression, noise, and filtering) and increases the visual quality to the original image.

Region-based watermarking is useful in sensitive fields, such as medical imaging, where qualitatively the ROI must remain untouched. In region-based watermarking, the image is segmented, then we can determine what parts of the imaged regions are of interest (ROI) and what parts are of no interest (NROI). Watermarking can be applied to NROI, but not to ROI to avoid altering valuable clinical features. For example, if the NROI were a tumor region on an MRI scan, watermarking would have no effect on the clinical value and/or diagnostic of the image whilst still ensuring the necessary accountability and authentication.

3) Challenges in Healthcare Watermarking:

- *Reversibility Requirement:* In medical imaging the watermark is required to be lossless and therefore is very complicated to create compared to irreversible watermarking in other fields.

©IJRASET: All Rights are Reserved

- *Regulatory Compliance:* Watermarking systems must meet the privacy (autonomy) and auditability requirements in the given health laws.
- *Computational Constraints:* Watermarking must be completed in real-time or not delay the time sensitive nature of diagnostic imaging systems such as PACS (Picture Archiving and Communication Systems).
- *Standardization:* There is no universally accepted protocol or standardized benchmarking for the field of medical watermarking.

4) Novel Trends in Medical Image Watermarking:

- *Watermark embedding via AI:* Neural networks are being developed to embed and extract watermarks while maintaining diagnostic quality.
- *Blockchain + Watermarking:* Some systems are storing watermark hashes on blockchain for decentralized integrity checking.
- *3D Medical Imaging:* Early studies are investigating watermarking volumetric data like 3D MRI or CT scans.

B. Application of Watermarking in Surveillance and Forensics

Digital images and videos are commonly considered evidence in legal and investigative processes when it comes to surveillance and forensics. The lack of integrity and authenticity of visual media is a critical factor in many legal processes, particularly in light of the sophistication of manipulated media (i.e., deep fakes and further tampered video). While encryption can help assure the authenticity of digital visual media, once data is decrypted, the ability to trace, or even know if it is tampered data, is considerably hampered. In these circumstances digital watermarking provides an additional embedded authenticity barrier that is persistent. Essentially digital watermarking, is assurance that a particular digital image or video is protected in a way that can be customized to ensure discovered media digital provenance and being able to understand when or how media has been forensically accountable.

1) Key Use Cases:

- *Chain-of-Custody Validation:* Surveillance footage receives a watermark with the date and time, along with the location where the footage was captured. This allows verification later, in court, that the footage has not been altered through storage and/or transfer, when provided
- *Tamper-Evident Footage in Public Settings:* Crime and traffic camera systems embed weak or semi-weak watermarks with video streams and analyze the watermarks with additional cryptographic measures to make the changes, such as cropping or removing frames, from the original video stream evident.
- *Police Body-Worn Cameras and Aerial Drone Systems:* Police body-worn cameras and aerial drone systems embed GPS location, functioning device ID and date and time as real-time watermark features. This protects the visual evidence obtained on behalf of the public sectors during public events, by lawful inspection or arrest.
- *Forensic Data Authenticity:* Forensic investigators identify crime scene images and biometrics (finger, iris) with watermarks to demonstrate ownership, guarantee originality, and authenticate, when submitted as digital evidence.

2) Techniques and Domain-Specific Needs:

TABLE II
TECHNIQUES AND DOMAIN-SPECIFIC NEEDS

Technique	**Application**	**Characteristics**
Semi-Fragile Watermarking	Scene authentication	Detects selective tampering
Compressed Domain Watermarking	CCTV video feeds	Real-time embedding during compression
SVD-DCT Combination	High-fidelity surveillance	Maintains quality and robustness
Region-based Fragile Watermarking	Biometric evidence	Avoids embedding in key forensic areas

Watermarking in the compressed domain is most useful to real-time surveillance systems, as it also prioritizes speed and efficiency. Surveillance systems often store and transmit video data in a limited (compressed) format, such as MPEG or H.264.

Compressing video minimizes the amount of bandwidth and storage needed; therefore, watermarking in the compressed domain means that it can embed a watermark into the compressed (bitstream), and thus eliminate the need to decompress, embed the watermark, and then recompress the data, all of which prolongs processing time for a video and increases computing power. Watermarking in the compressed domain provides further assurance that the watermark is preserved through standard compression procedures—ideal for real-time monitoring applications often encountered in live CCTV, body-worn cameras, and automated monitoring systems.

Likewise, region-selective watermarking is universally opted in sensitive contexts, such as forensic imaging, as it helps maintain the authenticity and evidential weight of visual content. Generally, this process requires that images are analyzed in order to identify critical regions (identifiable features, forensics marks, injury pattern, etc.) that should not be changed regardless of watermarking. Watermarks then only embedded in non-critical areas, again minimizing infringement on content admissibility/value in legal/investigative matters. Region-selective watermarking attempts to meet the boundary between immense data protection, and evidential reliability.

3) Challenges in Surveillance-Based Watermarking:

- *Real-time Constraints:* Most types of surveillance utilize live watermarking with very little latency, which are computationally intensive to carry out on high fidelity video streams.
- *Multiple Sources:* When video is captured from multiple types of sources (CCTV, drone, phone) watermarking needs to maintain consistency and interoperability.
- *Legal Admissibility:* Courts also require standards of verifiable traceability and verification. Any watermarked content must be accompanied by verifiable logs and cryptographic proof.
- *Environmental Conditions:* Dia/Low-light, occlusion, noise, motion blur may hinder the robustness of the watermarking.

4) Emerging Trends and Innovations:

- *Edge-Based Watermarking:* By embedding watermarks where the camera edge is using smart IoT surveillance, the processing requirement for central servers is reduced while tracking video for evidence.
- *Multi-Layer Watermarking:* Embeds both robust and fragile watermarks to trace ownership and alert to tampering and evident changs.
- *AI-Driven Tamper Detection:* Deep learning is being merged with watermark extraction for analysis against identifying and flagging inconsistencies, or reasonably potential manipulations.
- *Watermarking in Bodycam AI Systems:* Modern bodycams now identify a person and simultaneously watermark the visual data thereby increasing situational transparency.

C. Application of Watermarking in Secure Communication Systems

Secure communication is essential for modern digital infrastructure. It includes personal texting, corporate file transport, satellite photo across-the-format data and even communications regarding multimedia transmission processes across formats. While encryption cannot guarantee any recipient confidentiality; it does not automatically convey proof of ownership, authentication or trustworthiness of the message internally, or after decryption; watermarking provides this second, continuous layer of security through implied and applied knowledge—for example, even after decrypting or forwarding the encrypted content of a message.

Watermarking does ensure that the content, if transmitted or published, still contains invisible proof of credentials or verifications tokens, to verify the identity of the sender, maintain originality, and block unauthorized redistribution.

1) Use Cases in Communication Systems

- Copyright Protection in Multimedia Transmissions: Video and audio content are often transmitted via a streaming platform or through the use of a satellite link. Most video and audio streams will also supply watermarks or information that specifies whether the content was created by the company or authorized by that entity. This provides a deterrent against pirated content and may also be useful for copyright claims.
- Secure Messaging within Defense and Government Systems: Explicitly sensitive messages or documents of government or military organizations may also embed metadata in the form of watermarking (e.g., identity, date/timestamp, clearance),

allowing both the sender and receiver to prove authorship of messages, even if those messages have been shared/circulated unlawfully.

- Broadcast Authentication: When a live signal is being transmitted, such as in a TV or radio broadcast system, watermarking can also be used to authenticate the source of the signal transmission. Broadcasters can embed an authentication watermark to provide proof against signal hijacking or piracy.
- Digital Rights Management (DRM): The mechanism of identification and tracking of digital content is one of the most important roles of watermarking in DRM. Watermarking of content is always user-specific content, and helps identify leaks of digital content or can provide the basis for usage policies to be enforced, such as Netflix, Spotify, or in e-learning systems.

2) Common Techniques and Protocols:

TABLE III

Technique	Use Case	Notes
Spread Spectrum Watermarking	Secure messaging	High robustness and low detectability
Quantization Index Modulation (QIM)	Audio watermarking	Efficient for real-time applications
DWT-DCT-SVD Hybrid	Video streaming	Good trade-off between imperceptibility and robustness
User-specific Keyed Watermarking	DRM	Ensures leak tracing to individual user

Spread spectrum watermarking is extremely robust against a wide range of attacks, such as noise, compression and format change, by using a watermark signal spread over a wide bandwidth, similar to the process used in wireless. This low power, wide-band process allows the watermark to stay imperceptible, while being able to survive different types of attacks like JPEG/MPEG compression and transmission noise, ultimately facilitating watermark recovery. This is particularly advantageous when either a low bandwidth or noise environment exists, as an example, in multimedia streaming, mobile content delivery, and satellite transmission.

In contrast to the spread spectrum watermarking approach, in a user-specific (e.g. digital fingerprinting) watermarking procedure, each user has a distinct watermark and allows tracing the unlawful redistribution that occurred. In this case, if pirated content does arise, it is possible to conduct forensic analysis on the pirated data to identify the user responsible. This does not prevent the misuse, but it does allow for accountability and enforcement of copyright in digital libraries, subscription service environments, and any situations where files are confidential.

3) Key Challenges in Communication-Based Watermarking:

- Bandwidth Limitations: Adding excessive watermark data may affect transmission efficiency or exceed bandwidth limits, particularly in mobile communications or satellite.
- Synchronization challenges: In real-time transmissions, achieving synchronization between the watermark encoder and the watermark decoder can be a challenge, especially in the event of packet loss.
- Dynamic Content: Watermarking needs to be dynamic to accommodate changing bitrate, resolution and codecs while streaming or conferencing.
- Detection without the original: In many architectures, watermark extraction must occur without access to the original content - requiring blind watermarking methods.

4) Novel Trends in Secure Communication Watermarking:

- AI-Adaptive Watermarking: Models based on artificial intelligence will be trained to dynamically select watermark location and embedding strength based on the network noise.
- Quantum watermarking ideas: Initial research has shown work embedding watermarking data into quantum states for ultra-secure communications of the future.
- Blockchain: Watermarked data is stored as timestamped hashes on the blockchain that provide immutable proof of originality and transmission history.

- Watermarking in IoT and 5G: In such a world of billions of interconnected devices, there will be lightweight, low-energy watermarking systems to secure the data being transferred from edges to cloud.

IV. ANALYSIS & DISCUSSION

A. Key Benefits of Digital Watermarking Across Domains

Digital watermarking provides cross-functional security and authentication, tailored to the unique requirements of each application domain. Here are the distinct advantages in each area:

Table IV
Benefits Of Digital Watermarking

Domain	Benefits
Healthcare	- Secures patient data within medical images- Supports tamper detection and reversibility- Ensures data integrity in telemedicine
Surveillance & Forensics	- Provides verifiable chain-of-custody- Detects manipulation in evidential footage- Adds traceability to visual records
Secure Communication	- Enables post-decryption authentication- Supports content ownership and copyright- Allows user-specific fingerprinting and leak tracing

While cryptography protects data in transit, watermarking protects data at rest and after decryption — filling a crucial gap in modern security systems.

B. Technical Requirements and Implementation Aspects

The effectiveness of digital watermarking depends on its technical integration with the host system's constraints — whether in medical scanners, surveillance cameras, or streaming platforms.

1) *Imperceptibility:* The watermark must not reasonably impair the original media's quality, including invisible and audible forms of decay. Additionally, this requirement is particularly important in sensitive domains such as medical imaging, where diagnostic quality could be severely compromised.
2) *Robustness:* The watermark should withstand a number of common processing methods. Some common processing methods would include compression, noise addition, size distortions, and file format changes. These would be critically important for applications such as surveillance video, where the footage is likely to undergo even a few of these processes.
3) *Security:* As mentioned before, only legitimate users should be allowed to embed, extract, or change the watermark. The watermark must offer a method of embedding to only authorized parties using key-based means for security to protect and reduce the chance of tampering.
4) *Real-Time Processing:* If counseling or some connected form of communication occurs in real-time (like surveillance) level of watermarking should be performed in milliseconds and not require lengthy processing time or any human or hardware delay.
5) *Reversibility:* There may be times in some domains like healthcare or other sensitive applications where it may be critical to fully reverse the watermarked form of the original image, as residual medical information could be lost.
6) *Compatibility:* Watermarking solutions must be compliment and adhere to current standards, practices, and protocols for various forms of media, such as DICOM (to standardize medical images), MPEG (compressed video), or any DMR systems (for streaming digital media).

Thus, Hybrid approaches (e.g., DWT-SVD or DCT-SVD) are often used to balance imperceptibility, robustness, and capacity.

C. Limitations and Open Issues

Despite its advantages, digital watermarking faces several technical and practical limitations that need attention for broader adoption and standardization.

1) *Limitations*

- Capacity vs. imperceptibility trade-offs: While embedding more information is generally conceivable, there may be a decay in the quality of the content.

- Fragility of formats: Some image and video formats compress and may damage watermark information in the process.
- Hardware limitations: Embedding real-time watermarking into battery-operated IoT or surveillance hardware is still a challenge.
- Blind extraction limitations: In many real-world use cases, watermark detection needs to occur in a "blind" capacity (without anything to compare the media to), so providing robustness can be difficult.

2) Open Research Issues:

- Universal watermarking standards: This still means that in many industries there is not yet an agreement on watermarking (e.g. common protocols for DICOM + MPEG + DRM).
- AI attacks, counter-attacks: Adversarial AI models are currently able to remove or spoof watermarks; AI resilient watermarking is an emerging necessity now.
- 3D and multimodal watermarking: As 3D imaging and holography are being pushed into medical domains and defense applications, there is a need to develop watermarking techniques and applications for volumetric watermarking.
- Ethical & Legal considerations: Watermarking protects data, but watermarking also needs to remain compliant with privacy legislation. Including patient information directly into images means privacy protection would not exist, and patient ID without encryption may create a legal breach.

Toward the future: Recent interest in using blockchain and AI for verification and to enable adaptive watermarking is a very promising trend that may help relieve many of the issues put forward in the project feasibility study.

V. PROPOSED UNIFIED FRAMEWORK FOR CROSS-DOMAIN WATERMARKING APPLICATIONS

A. Motivation for a Common Architecture

Watermarking systems have historically been developed in their own environments for specific areas such as healthcare, surveillance, and multimedia. However, these areas converging means that there is a need for a single, flexible and scalable watermarking framework for use across the areas to respond to a growing need (for example, telemedicine uses surveillance while video conferencing by law enforcement is secured).

This new framework can:

1) Enable interoperability.
2) Minimize duplication of development.
3) Allow a standard reference point for comparative review.
4) Allow for use by domains with specific customization but share a common architecture.

B. Design of the Framework

The proposed universal framework is a modular framework comprised of the following components:

1) Input Handler: Accepts input in multiple formats - image, video, audio, text - and accepts combinations of formats including DICOM (medical), formats such as MP4 (video) which require specialized data, and encrypted documents which require access credentials/ key, etc.

2) Preprocessing Unit: Performs normalization, format conversions, color/grayscale conversion and may extract Region of Interest for selected watermarking.

3) Watermark Creator: Creates watermark credentials based on: i. ownership credentials, ii. metadata (timestamp, device ID, location), iii. biometric identity (forensics), iv. patient data (health); and user session Id or U id (communication).

4) Domain Adaptive Embedding Engine: Selects watermarking method and technique based on domain

i. Reversible Watermarking for healthcare domain
ii. Real-time Fragile Watermarking.
iii. Robust Spread-Spectrum or Hybrid (fragile) in communication; and appropriate transform domain (DWT/DCT/SVD).

5) *Encryption and Access Control Layer:* May optionally encrypt watermark (symmetric or asymmetric) with user-level access management (e.g. doctor vs radiologist, etc.).

6) Quality & Robustness Evaluator: Evaluates imperceptibility (in PSNR, SSIM), and f. robustness (in Bit Error Rate, NC), and maintains a log of tampering detection (in fragile mode).

7) Watermark Extraction Module: Performs blind or semi-blind extraction and may verify a watermark and detection and may indicate if tampering was detected (and log) or mismatched (alert/log).

C. Domain-Specific Configurations

TABLE V
DOMAIN SPECIFIC SONFIGURATIONS

Domain	Customization	Embedding Strategy	Priority
Healthcare	DICOM format support, reversible watermarking	ROI-based LSB + encrypted payload	Accuracy & reversibility
Surveillance	Real-time processing, timestamp & device ID	Semi-fragile in compressed domain	Speed & tamper detection
Communication	User-specific fingerprinting, DRM tag	Spread Spectrum + QIM	Robustness & ownership tracking

Advanced watermarking systems can operate dynamically in either fragile, semi-fragile, or robust modes in any domain (spatial, transform, or compressed mode), depending on application needs. The systems are also able to continuously adjust embedding parameters including strength, location, and redundancy at run-time, to optimize performance and compliance. This adjustment will usually depend on the following factors:

1) *Network Conditions:* On unstable or low-bandwidth networks, a robust watermarking mode with higher redundancy may be better to provide protection through compression/transmission errors. Whereas high-bandwidth, stable conditions may allow for lighter-weight watermarking that require less redundancy to preserve media quality.
2) *Hardware Capability:* Lower-end devices (e.g., IoT cameras or mobile devices) will often not have the computational capacity to perform steeply-complex watermarking algorithms. In addition to just simpler, spatial domain embedding, devices may be limited depending on their performance in the transform domain, due to using stronger, more secure embedding strategies.
3) *Privacy and Regulatory Compliance (e.g., HIPAA, GDPR):* In sensitive domains such as health or legal forensics, watermarking must comply with privacy considerations. This means that information embedded does not violate any personal data and, in cases, should provide some reversibility, enforce access control to the embedded information, however, should always provide traceability in even the most extreme cases of leakage or unauthorized access.

D. Benefits of a Unified Approach

1) *Cross-Domain Scalability:* A productive watermarking framework should be flexible enough to be deployed in a number of sectors such as healthcare, defense, media, forensics, etc. The framework should be able to use the same watermarking tool in a wide range of environments with only slight adjustments for their respective sectors. This feature adds to the functionality and fluidity of watermarking solutions and minimizes the management of independent architectures. It also enhances interoperability and provides the user's experience most common use cases.
2) *Benchmarking Platform:* A more productive framework will provide benchmarking platform to compare and validate new approaches in a fair way. The benchmarking platform allows researchers and designers to use a standardized environment to assess watermarking algorithms and measure the imperceptibility, robustness, computation cost, etc., in the same controlled environment, which has standard reproducible constraints. A standardized benchmark lowers barriers to entry and encourages innovation at a faster more productive pace and when more solutions are available, the overall value goes through the roof!
3) *Cost & Time Savings:* The availability of a reusable and extendable framework minimizes the duplicating of labor in both academic research and product development. Developers will be able to devote their time, resources, and effort to improving only one area, rather than needing to build an entire system. This will allow for faster deployment, cheaper development, and a more efficient use of time and resources.
4) *Modular Innovation:* The architecture should be modular with the flexibility of adding new embedding and detection designs as plug-ins. This allows the system to be upgraded, customized, and tinker without requiring a complete overhaul. This level of modularity enables continuous improvement and adaptation, considering ongoing advances in technical and regulatory issues and the demands to deploy systems, risk-free at an organizational level.
5) *Regulatory Flexibility:* A variety of configurable modules can be used to comply with different regulatory standards (e.g., HIPAA for Medical Data, GDPR for privacy, DRM policies for media, etc.). The modules can be pre-configured to support enforcement of specific rules about data handling, access controls, and audit requirements in order for the system to remain legally compliant, whilst offering strong watermarking capabilities.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

E. Feasibility & Implementation Considerations

1) Challenges

- Performance tuning is particularly difficult because one must balance robustness and imperceptibility, plus there are multiple media types and use cases.
- Hardware limitations in IoT and embedded surveillance systems means fewer options for performing complicated implementations of watermarking.
- The legal issue of data protection can come into conflict with the ethical responsibilities of the researcher (tension between security versus privacy obligations). In cases where researchers are embedding medical data, there can be serious issues with privacy law.
- Systems working together easily despite differing software platforms, file formats, and codecs. This is a technical concern and difficult if not impossible to ensure.

2) Solutions:

- Container-based deployment and image classification - The use of containers such as Docker allows for modular, scalable deployments across heterogeneous systems.
- AI-based optimization, when implemented as either types of technology, allows for real-time adjustment of the robustness and location of the embedding, which will allow for better performance and adaptability.
- Blockchain verification logs, where the information is made available through blockchain which allows verification logs to be secure and tamper-proof allows data to be traceable and accountable.
- Federal repositories, when a standardized dataset is made domain specific, jurisdictions can be evaluated performance-wise yet still be compliant.

VI. FUTURE RESEARCH DIRECTIONS & EMERGING TRENDS

As watermarking evolves beyond conventional applications, several emerging trends and future research directions are shaping the next generation of secure digital media systems. These innovations aim to overcome current limitations and expand the utility of watermarking across more complex, dynamic, and intelligent ecosystems.

A. AI-Driven Adaptive Watermarking

1) What's Emerging: Machine Learning (ML) and Deep Learning (DL) models are being integrated together, capable of adaptively selecting:
   i. Embedding strength
   ii. Optimal region of interest (ROI)
   iii. Robust transform domains

2) Why it Matters: The ability to enable content-aware watermarking, application agnosticism, and auto-optimizing watermark strength for the situation (compression/noise issues).

3) Use Cases:
   i. Real-time adaptive watermarking on video calls.
   ii. Quality assurance in telemedicine, automatically scaling watermark robustness based on available bandwidth.

B. Blockchain-based Watermark Verification

1) What's Emerging: Blockchain is being used for logging actions that take place during watermark creation/embedding, and extraction to create a log of events that cannot be tampered with.

2) Why it Matters: Creates a time-stamped record of ownership status and an immutable audit trail which is important for forensic, legal and admissibility processes.

3) Use Cases:
   i. Timestamped surveillance footage with provenance tracking.
   ii. Healthcare records, access trails in telemedicine systems.

C. 3D and Multimodal Watermarking

1) *What's Emerging:* Developing watermarking for:
   i. 3D medical scans (CT/MRI)
   ii. Holographic images
   iii. Multimodal dataset, images + audio + metadata
2) *Why it Matters:* Represents a huge leap forward for data integrity with the advent of high information content and discretionary imaging systems for many applications within healthcare, defense, and industrial inspection.
3) *Problems:*
   i. Establishing a formal measure of perceptual transparency in 3D.
   ii. Getting watermarking in 3D and across its modalities to work in sync.

D. Quantum Watermarking (Theoretical Frontier)

1) *What's emerging:* It is an experimental notion known as quantum watermarking to mark, with quantum states, a verifiable ownership or authenticity tags.
2) *Why it matters:* May result in a non-cloneable watermarking scheme based on quantum no-cloning and uncertainty.
3) *Limitations:*
   i. Still theoretical
   ii. Subject to advances in quantum computing and quantum communication

E. Juridical, Ethical and Privacy Friendly Watermarking

1) *What's emerging:* Privacy-aware watermarking is indispensable in the context of legal frameworks such as GDPR, HIPAA, and DPDP in India:
   i. Embedding also should not threaten user or patient privacy.
   ii. Should be reversible or encrypted (as per 3 above).
2) *Why it matters:* Especially for the applications in health and secure communication.
3) *Open Research Topics:*
   i. How to anonymize yet retrieve data?
   ii. How to embed without exposure of sensitive data?

F. Interoperability, and Standardization

1) *What's emerging:* The demand for the standardization in the watermark embedding, detection and evaluation across industry is increasing.
2) *Why it matters:*
   i. Allows easy to embed watermarking in DICOM, MPEG and streaming applications.
   ii. Facilitates inter-vendor inter-operation.
3) *Current Gaps:*
   i. No thorough API framework for watermarking.
   ii. No well-established global benchmarks across all domains.

G. Watermarking for Deepfake Detection and Synthetic Media Verification

1) *What's emerging:* With the rise of AI-generated media, watermarking is being used to investigate :
   i. Embed authenticity signatures in original content.
   ii. Track where on the platform the media was manipulated.
2) *Future Application Areas:*
   i. Social media moderation.
   ii. Admissibility of digital evidence in court.
   iii. Authentication of news media.

VII. CONCLUSIONS

Digital watermarking becomes an important technology for protecting multimedia data in various applications which require confidentiality, authenticity, and integrity. This article investigated its application in three high-impact domains — Health Care Services, Surveillance, and Secure Communication—, each with specific technical and ethical consideration.

Watermarking is used in health care to securely transmit sensitive diagnostic images without compromising the privacy of the patient. It confers an evidence integrity in surveillance and forensics and enables the chain-of-custody verification and tampering detection. To guarantee secure communication, watermarking strengthens the authentication feature together with user traceability and content protection when they are inevitably exposed to cyber-attacks.

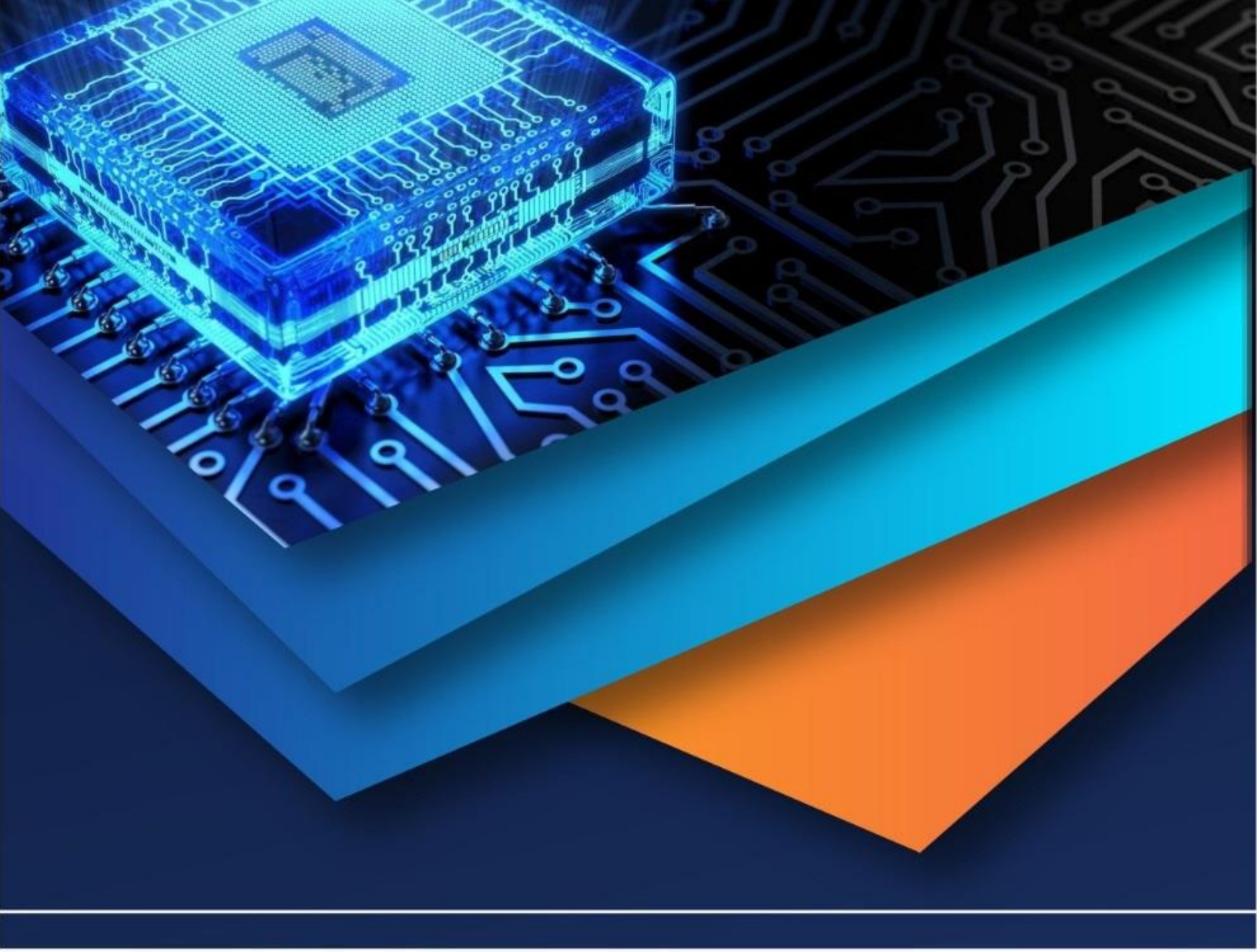
In addition to providing various practical applications, this article also introduced a unifying extensible framework that can be used as a model for the cross-domain instantiation of watermarking systems. This architecture facilitates flexibility, scalability, regulatory-friendly' development and promotes interoperability and cost-efficient development.

The review also outlined some future directions including AI-powered watermark optimization, Blockchain-based verification and the possibility of quantum watermarking. These technologies potentially allow watermarking systems to accomplish even more than the watermarking literature would have anticipated – e.g., in the age of synthetic media, telemedicine, and intelligent surveillance.

In summary, digital watermarking is not just one of the many specialized cryptographic tools anymore, but has become a core basis for trust in digital world. As multimedia technologies become increasingly converged and the potential for misuse of information is a major concern, watermarking is expected to be one of the key building blocks of a secure digital infrastructure. Further investigation, standardization and interdisciplinary innovative adaptation will be important to realize these full potentials.

REFERENCES

[1] R. Liu and T. Tan, “An SVD-based watermarking scheme for protecting rightful ownership,” IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, Mar. 2002.
[2] M. Barni, F. Bartolini, and A. Piva, “Improved wavelet-based watermarking through pixel-wise masking,” IEEE Trans. Image Process., vol. 10, no. 5, pp. 783–791, May 2001.
[3] A. Swaminathan, Y. Mao, and M. Wu, “Robust and secure image hashing,” IEEE Trans. Inf. Forensics Secur., vol. 1, no. 2, pp. 215–230, Jun. 2006.
[4] A. A. Paul and A. H. Reza, “A survey of reversible watermarking techniques in medical images,” J. Biomed. Inform., vol. 93, pp. 103–127, Apr. 2019.
[5] M. A. Qureshi, A. H. Altalbe, and M. Y. Javed, “Securing telemedicine through blockchain-based watermarking for medical images,” IEEE Access, vol. 9, pp. 45713–45726, 2021.
[6] K. Ma, W. Zhang, and N. Yu, “Reversible watermarking with optimal value transfer,” IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 3, pp. 406–414, Mar. 2009.
[7] J. Fridrich, “Applications of data hiding in digital images,” Proc. SPIE, vol. 5020, pp. 29–36, Dec. 2003.
[8] A. T. S. Ho, X. Zhu, and P. Marziliano, “Tamper detection in compressed medical images using watermarking,” IEEE Trans. Biomed. Eng., vol. 53, no. 3, pp. 469–480, Mar. 2006.
[9] H. Farid, “Digital image ballistics from JPEG quantization,” ACM Trans. Appl. Percept., vol. 2, no. 1, pp. 22–25, Jan. 2005.
[10] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized-LSB data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.
[11] A. H. Allaf and M. Ait Kbir, “A review of digital watermarking applications for medical image exchange security,” in Proc. Int. Conf. Security and Cryptography, Tangier, Morocco, Mar. 2019. [Online]. Available: https://www.researchgate.net/publication/330905652
[12] N. I. R. Yassin, “Digital watermarking for telemedicine applications: A review,” Int. J. Comput. Appl., vol. 129, no. 17, pp. 30–37, Nov. 2015. [Online]. Available: https://ijcaonline.org/archives/volume129/number17/23168-2015907183.pdf
[13] S. Gull and S. A. Parah, “Advances in medical image watermarking: A state of the art review,” Multimedia Tools Appl., vol. 82, pp. 1407–1447, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11042-023-15396-9
[14] H. Chaudhary and V. P. Vishwakarma, “Analysis of healthcare data security with DWT-HD-SVD based algorithm in invisible watermarking against multi-size watermarks,” Sci. Rep., vol. 14, Apr. 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-61479-4
[15] “Digital watermarking,” Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Digital_watermarking



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)