Partners Universal Multidisciplinary Research Journal (PUMRJ)
Volume: 02 Issue: 06 | October-November 2025 | ISSN: 3107-5789 | www.pumrj.com

Digital Watermarking in Cloud Environments for Copyright Protection: A Comprehensive Review

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract – **Background:** The emergence of cloud platforms at a very fast rate has altered the way we develop, store, distribute, and consume digital content. The scale, easy access, and reduced cost of cloud computing are unparalleled, yet cloud computing poses serious challenges on the intellectual property protection and enforcement of copyrights. Digital watermarking, which entails installing tiny symbols of ownership within media, has become a necessity when it comes to copyright safeguarding, authentication of content and tracking of these same elements in clouds environments. As cyber-attacks are becoming more advanced and quantum computers pose a threat to the conventional cryptography, it is time to discuss current watermarking technologies and their development in the direction of more adaptive, more secure, and quantum resistant solutions.

Objectives: This is a review that systematically examines digital watermarking technologies that are intended to work in cloud environments and protection of copyright. The goals are:

1. To examine the fundamentals and types of watermarking techniques.
2. To assess the way new technologies including AI, machine learning and blockchain are being incorporated into watermarking systems.
3. To evaluate security risks, types of attacks and security defenses in cloud based watermarking architectures.
4. To discuss adaptive algorithms, which can be applied to the multi-user cloud context.
5. To explore quantum -resistant watermarking strategies in post-quantum cryptography.
6. To determine the research gaps and propose the way forward to generate strong, scalable, and secure watermarking systems in the distributed computing ecosystem.

Methodology: The article uses systematic literature review with critical synthesis of the recent technological advances. We used Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and Google Scholar to find peer-reviewed articles, conference proceedings, and technical reports published in 2015-2025. The search keywords were the following digital watermarking, cloud computing, copyright protection, blockchain, artificial intelligence, machine learning, quantum cryptography, content authentication, and others. We have also applied citation tracking backward and forward to locate more sources. The review provides a balance between the new and old materials that establish the present paradigms and contains both theoretical viewpoints and empirical research.

Key Findings: The review points at some crucial tendencies in digital watermarking on clouds.
1. The traditional approaches have a disadvantage of difficulties in operating within a dynamic cloud environment, including the inability to resist sophisticated attacks, scalability of the system spread across the entire network, and adaptability to a variety of content types.
2. AI and machine learning have revolutionized the concept of watermarking by providing adaptive embedding, automatic attack detection, and automated parameter adjustments depending on both content attributes and the emerging threats.
3. Blockchain has the potential to transform further by providing decentralized and irreversible records of

watermark registration, verification, and ownership verification thereby eliminating the problem of trust in centralized systems.
4. Multi-domain techniques which blend several transform domains (i.e. DCT, DWT, and SVD) offer superior tradeoffs between imperceptibility and robustness than single-domain techniques.
5. Existing cryptographic foundations of watermarking are also under attack by quantum computing, making the development of quantum-resistant algorithms in lattice-, hash-, and code-based cryptography an urgent task.
6. Real time watermarking with low latency is enabled by edge computing integration, and comes with real time workloads that demand instant processing including IoT systems and streaming media.
7. There are still legal and technical issues across jurisdictions, particularly on cloud service provider liability and safe-harbor provisions.

Conclusion: Digital watermarking has become a crucial part of extensive copyright protection in cloud setting. The rapid development of cloud frameworks, more complex attacks, and the emergence of quantum computing require new watermarking technology to be developed constantly. The intersection of AI, blockchain, and quantum-resistant cryptography leads to the future of adaptable, decentralized, and future-proof system. Such findings have implications to content creators, cloud providers, policymakers, and security researchers. Scholars obtain practical results on implementing effective watermarking at multi-tenant clouds. Policymakers see loopholes in the existing legal systems and international regulations and harmonization. To innovate watermarking technologies, researchers find ways in which interdisciplinary efforts can be used, including signal processing, cryptography, distributed systems, and machine learning. Finally, to ensure the protection of intellectual property in the cloud, it is necessary not only to develop technologies but also legal, technical, and organizational activities to create reliable, scalable, and enforceable protection systems of the digital era.

Keywords: Digital Watermarking, Cloud Computing, Copyright Protection, Blockchain Technology, Artificial Intelligence, Machine Learning, Quantum Cryptography, Content Authentication.

1. INTRODUCTION

The digital revolution has completely changed the way humanity generates, disseminates, and consumes information. Cloud computing is the core of this change, and this paradigm has democratized access to computational resources, storage infrastructure, and software applications at an unprecedented level. Market projections have it that the international cloud computing sector will surpass more than 678 billion dollars by the year 2027, because of its ubiquitous use in virtually every sector of the contemporary economy. This explosive development has been fueled by the compelling value proposal of cloud computing virtually unlimited scalability, pay-as-you-go cost frameworks, ubiquitous availability, and the freedom of operating complicated physical infrastructure. Companies of all sizes, including multinational corporations, and individual content creators, are now making regular use of cloud-based services to store digital content, to distribute multimedia performance, to work on creative projects, and to provide services to worldwide consumers.

But this digital ecosystem that is cloud-based emerges with deep issues in the protection of intellectual property and enforcement of copyright. The very attributes that make cloud computing enticing such as simple copying, frictionless sharing, distributed storage in different jurisdictions, and physical control abstraction also allow malicious parties to exploit them to engage in unauthorized duplication of content, piracy, and theft of intellectual information. In contrast to the traditional models of content delivery, where the physically enforced barriers to infringement by having physical media and central control points,

cloud environments have radically different architectures, with data fragmentation across distributed nodes, multi-tenancy with many users sharing the infrastructure, high replication of content to optimize performance, and long chains of intermediaries between creators and consumers of content. These architectural facts make the traditional means of copyright protection more inefficient.

Digital watermarking has become an important technology to deal with such issues, through entrenching invisible yet strong identification marks directly into the digital object. By contrast with the external metadata, which is easily removed, or the digital rights management (DRM) systems, which prevent usage with the help of encryption, watermarking alters the content itself in such manner that it can withstand the typical transformations and can remain undetected by humans. This embedded signature can store several different types of information, such as the ownership of copyright and identification of creators, distribution dates, licensing, and user identifiers that can be used in forensics. Properly utilized, watermarks have survived compression, format conversion, cropping, and other digital content manipulations typically applied to digital content, on clouds. Moreover, watermarking also supports a variety of complementary applications beyond copyright control, such as content verification to detect infringement, forensic tracing to find sources of leakage, broadcasting to verify legitimate use, and automatic rights management in complex licensing situations.

Digital watermarking convergence with cloud computing, though, provides a set of technical issues unprecedented in the history of cloud implementations, which is why cloud-based implementations differ with offline watermarking. Cloud infrastructures require watermarking systems capable of running a system of millions of pieces of content every day on a distributed architecture. They need real time or close to real time performance, so that the interactive applications do not cause poor performance. They must support a high level of heterogeneity in the content types, formats, the quality and usage patterns. Their adversarial threats are advanced such as collusion attacks whereby multiple users join together to remove the watermark of an image with partial information, insider threats where there is a cloud administrator that is able to access the image and thus remove the watermark without losing the perceptual quality of the image and advanced machine learning based threats that are intended to remove the watermarks on the image without adversely affecting the perceptual quality of the image. Also, cloud watermarking systems are required to traverse multi-tenant scenarios, which include more than two users with different security needs, privacy limitations, and performance expectations, but who are sharing a common back-end infrastructure.

The last few years have been characterized by impressive innovations that strive to resolve such challenges by incorporating the latest technologies. Machine learning and artificial intelligence have transformed watermarking by making adaptive systems that teach good embedding patterns on the data, detect and mitigate attacks, and change parameters dynamically depending on content properties and attacker environments. The blockchain technology has the transformational opportunities of decentralizing the watermark registration and verification, establishing abiding audit trails of content provenance, and removing single-point failures characteristic of centralized systems. Watermarking architectures are getting quantum-resistant cryptographic primitives to provide enduring security in the face of attacks by quantum computers on traditional encryption schemes. Integration of edge computing also allows preprocessing at network edges, which minimizes the latency and bandwidth usage in real-time usage. Transform domain approaches Hybrid transform domain methods that intermix discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD) have been shown to be much stronger in terms of robustness imperceptibility trade-offs than single-domain methods.

Although these developments have been made, there are still vast gaps in the technical performance and theoretical knowledge of the cloud-based watermarking systems. A large portion of the current methods have been optimized to work in offline scenarios, and when applied to dynamic cloud environments with unstable network conditions, various attack vectors and with high latency requirements, they will perform suboptimal. Security evaluation of the watermarking systems is not always rigorous, and little thought is given to advanced adversarial models such as quantum attackers, machine learning-based watermark removals and colluding with others. The legal and regulatory provisions of copyright in cloud computing are still not unified across jurisdictions and are thus confusing the issue of liability, and enforcement schemes as well as safe harbor provisions of cloud service providers. There are privacy issues because a user-specific identifier may be embedded in watermarking systems to perform unauthorized tracking or profiling. The process of standardization has failed to match the pace with technology change thus causing incompatible standards of implementation, which impedes the process of interoperability.

2. RESEARCH GAP AND PROBLEM STATEMENT

Although a considerable amount of literature has been done on digital watermarking methods and individually on cloud computing security, it has a significant gap in thorough analysis that treats the special bracket involving the watermarking technology when it comes to copyright protection on clouds. Most of the current reviews are either shallow in the context of the discussions of watermarking algorithms without considering a cloud deployment situation or are broad based on the concept of cloud security without addressing watermarking-specific issues in-depth. Also, transformative technologies, such as AI-driven adaptive watermarking, blockchain-based verification services, and quantum-resistant cryptographic solutions, are emerging very fast, and a new synthesis, reflecting these new changes and their impacts on copyright protection in the cloud, is required. This review seeks to address such gaps to give an in-depth, critical analysis of digital watermarking technologies, specifically in cloud environments with specific reference to new and emerging innovations and trends.

3. OBJECTIVES AND SCOPE

The article has several objectives which are interconnected. It begins initially by systematically analyzing the basic concepts, types and performance attributes of digital watermarking methods that apply to copyright protection on clouds. Second, it critically examines how the new technologies, especially artificial intelligence, machine learning, blockchain, and quantum-resistant cryptography, are changing watermarking functionality and overcome restrictions of the old methods. Third, it analyzes security issues such as taxonomies of attacks, vulnerability analysis, and defensive mechanisms of cloud deployment. Fourth, it explores adaptive watermarking algorithms that would be applicable in multi-user cloud settings with different security need and usage characteristics. Fifth, it presents the real-time watermarking applications in cloud-edge computing systems and discusses the methods of latency optimization and performance trade-offs. Sixth, it evaluates the incorporation of blockchain that manages watermarks in a decentralized way and authenticates the content. Seventh, it discusses quantum-resistant watermarking strategies in anticipation of the post-quantum cryptography age. Lastly, it establishes the research gaps which are crucial and gives practical directions to be taken in future research.

The literature included in the review is peer-reviewed scholarly articles, industry reports, and technical documents that were published after 2015 and with some selectivity published earlier when needed to provide historical context. The paper narrows its scope down to watermarking schemes that can be applied to the cloud computing systems to protect copyright and authenticate contents, both in theory and in practice. Although the discussion is related to other relevant fields such as steganography, digital rights management, and cloud security in general, the consideration is majorly on watermarking technologies and their cloud-oriented solutions. It covers the world, yet it focuses on specific legal and regulatory trends in large markets such as the United States, European Union, and Asia-Pacific markets where cloud usage is the least developed.

4. METHODOLOGY

The systematic literature review methodology used in this article aims at facilitating the total coverage, critical synthesis, and reproducibility. There were several organized stages in the review process. To begin with, we have designed our extensive search strategy using the following keywords or keyword combinations digital watermarking, cloud computing, copyright protection, blockchain watermarking, AI watermarking, quantum-resistant watermarking, content authentication, adaptive watermarking, cloud security, and other technical terminology, and have searched the major academic databases Scopus, Web of Science, IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar. Second, we applied inclusion criteria where sources should be topical to digital watermarking methods and have a clear focus on cloud computing, copyright protection, or integration of new technologies must be published in peer-reviewed journals or authoritative technical publication and must make significant technical or empirical contributions and not just describe concepts in an abstract way. Third, we conducted a primary screening on titles and abstracts to determine potentially useful sources and subsequently were subjected to full-text screening to make final inclusion decisions. Fourth, to enhance database searches, we have used backward and forward citation tracking to consider other relevant sources. Fifth, we carefully arranged the data obtained as thematic categories that were consistent with the aims of the review. Lastly, a critical synthesis determines patterns, trends, debates, and gaps in literature, which is the basis of the subsequent discussion sections.

5. DISCUSSION

5.1 Fundamental Watermarking Techniques and Cloud Environment Challenges

Digital watermark consists of numerous methods which may be classified by various factors the strength of the watermark, where watermark is inserted, what watermark is watermarked and how it is observed. Strong watermarks is designed to withstand both willful and unintentional watermark assaults that include compression, filtering, geometries, and even intentional deletion. It is therefore applied in copyright protection where the watermark is supposed to continue functioning regardless of the changes made. Weak watermarking, in its turn, is supposed to identify even minor alterations. It is utilized to authenticate, as well as detect tampering detection ought to occur whenever any alteration has been made. Semi-fragile watermarking is in the middle between these extremes. It can withstand weak and harmless changes such as compression and yet warning of malicious changes, balancing security and sensitivity on applications which require copyright protection and integrity checks.

A second significant distinction is the distinction of blind (oblivious) and non-blind watermarking this depends upon what is required to detect the watermark. Non-blind techniques need the original

waterless material when extracting the content. This restricts their practical application in most cloud applications, in which the original might not be accessible by verifiers. Blind watermarking defeats this by enabling extraction of the watermarked data in addition to a secret key. It allows checking in distributed environments whereby content is checked at numerous locations with no central coordination. The semi-blind methods require partial knowledge of the watermark, but not the full original content, which offers a compromise between the detection accuracy and the practical limitations.

Embedding domain is also a category of watermarking method. Spatial-domain techniques perform direct manipulation of pixel values. They are not difficult to implement but are typically not resistant to signal-processing attacks. Transform-domain techniques alter coefficients in frequency representations of Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), or a combination of any of these. Under JPEG compression, DCT -based watermarking is more famous, where the watermark is added as a frequency coefficient, where there is good compression resistance but is not noticeable due to perceptual masking. Multi-resolution analysis is applied to DWT-based methods to insert watermarks into sub-bands so that the watermarks can adjust to the local image properties to tune the trade-off between robustness and invisibility. Hybrid methods combine several transforms, such as DCT-DWT-SVD and have demonstrated better performance through the benefit of using different representations.

As offline watermarking is transferred to cloud implementations, a number of basic challenges appear. Scalability is high since cloud solutions must support massive content at a distributed infrastructure. Single image tuned algorithms are not typically capable of performing as well in the cloud environment. Thus, it requires parallelization, distributed processing architecture, and optimizations to the computations. The heterogeneity of content in terms of types, forms, quality, and patterns of use demands watermarking systems to be flexible and change their embedding strategies rather than use a one- size-fits-all strategy. The quality of a strong watermark on high-resolution professional photographs can be too much in the case of casual mobile photographs, and video watermarking can also add a time component that is lacking in still photographs.

The nature of security threats in cloud environment is not the same as that, in traditional situations. Multi-tenancy increases the risk of cross-tenant based attacks, during which malicious users may attempt to identify watermarks in the content of other tenants, or use the shared resources to perform side-channel attacks. The presence of insider threats by cloud administrators with privileged access is a major vulnerability which cannot be fully addressed through pure cryptography. Collusion attacks are easier to execute when a group of users having diverse watermarked copies join forces to find out and delete watermarks. The machine-learning attacks The machine-learning attacks can run on large sets of watermarked content to identify methods of detection and removal based on statistical trends that appear when the same machine-learning algorithm is used multiple times.

The issue of privacy arises due to the conflict between forensic tracking and rights to privacy of the user. The presence of unique identifiers of both users and transactions allows tracking the content leak on the network with high accuracy but also leads to unauthorized surveillance or profiling in case watermark information is abused. Environmental laws like the General Data Protection Regulation (GDPR) by the EU can create severe restrictions on the gathering, processing, and storage of personal data, which may restrict watermark solutions that add user identifying data. To achieve the need to balance effective copyright protection and protection of privacy, system design, use of privacy-preserving watermarking, use of encrypted watermark domains, and limited disclosure verification protocols that authenticate watermarks without exposing user-specific information must be employed.

The cloud requires near-real-time or real-time embedding and extraction of performance to prevent negative user experience. Video streaming services cannot withstand high latencies that would affect the quality of playback. Online teamwork systems require flawless watermarking of papers and files without any observable lag time. To meet these constraints, it is necessary to implement algorithms more efficiently, use a hardware accelerator such as a graphics card or special processors, and make architectural tradeoffs, such as pre-computed watermark templates and incremental processing schemes.

The problems of interoperability are due to the variety of cloud platforms, watermarking, and content formats. Proprietary schemes bind users to vendors and do not allow content protected in one place to be checked anywhere. Standardization is missing such that solutions regarding the management of rights and authentication in an ecosystem can be provided on a global level. Breathing in new life Bodes like ISO and MPEG are in the early stages of standardization and are yet to gain universal acceptance.

Empirical researches of the performance of watermarking in the cloud setting display great trade-offs. Imperceptibility is usually minimized by increasing robustness since changes become more pronounced. More capacity to embed information increases the fragility of the watermark. The performance is likely to be degraded by the increased computational load due to the use of advanced cryptographic watermarking to create more difficult watermarks. These trade-offs require application-specific optimization watermark parameters are optimized according to content properties, security requirements, and performance limits.

Recent studies discuss context-sensitive watermarking dynamically adjusting embedding strategies, such as content analysis, threat models, and contexts of use. The system could use more intense watermarks on high-value copyrighted material and less intense watermarks in user-generated material with low piracy risk, etc. Watermarks may also be enhanced when they are sent to unreliable environments though reduced when sent internally. Machine-learning can be used to recognize context and optimize the parameters, to learn the best strategies based on historical data on content characteristics, attack modes and performance results.

The shift to cloud-based watermarking casts doubt on threat assumptions and trust model. Classical watermarking presupposes a secure place of embedding keys and algorithms. This assumption is made more difficult by the cloud environments, where processing using a shared infrastructural system under developer control is the norm. The cryptographic methods involved in ensuring the key confidentiality even in the face of untrusted servers include homomorphic encryption, secure multi-party computation, or trusted execution environment. These enhanced techniques introduce considerable computing requirements, posing further performance compromise that must be traded against security requirements.

5.2 Artificial Intelligence and Machine Learning in Adaptive Watermarking

Combining both artificial intelligence and machine learning has transformed digital watermarking out of rule-based approaches to watermarking systems, which are now data-driven. Such adaptive models can predict attacks, self-tune, and be more effective in a wide variety of settings. Conventional methods use manually developed algorithms that have fixed parameters and thus must be tuned by experts and have very limited adaptability to new content or attack strategies. In comparison, AI-based methods automatically discover useful embedding and detection rules, learn, and adapt to new threats.

Watermarking has been made particularly effective using deep learning. Deep neural networks are trained to understand complicated correlations among original material, watermarks, and the resulting watermarked indications. Convolutional neural networks (CNNs) encode image pixels with watermark bits and place watermarks in a manner that compromises between strength and invisibility. Trained in large image-watermark datasets, the network can optimize its embedding policy to minimize loss functions based on perceptual quality (e.g. PSNR, SSIM), robustness (extraction quality following attacks) and capacity (carried information).

The watermarking is typified with encoder-decoder architectures. The watermark is woven by the encoder on the host signal, and the decoder can obtain the watermark even following the occurrence of possible attacks. Conditional adversarial training on training against simulated adversarial conditions produces embeddings that are resistant to the expected forms of attacks. Generative adversarial networks (GANs) are an extension of the concept a generator imprints the watermark, and a discriminator attempts to guess it back. The generator is trained to produce watermarks that are invisible to the discriminator and are representational of real-life situations, where attackers are interested in identifying watermarks and eliminating them.

Reinforcement learning models of watermark embedding as a serial decision-making. An agent will monitor content properties, choose embedding behaviors (e.g. alteration of selected coefficients) and is rewarded depending on the watermarks quality, strength, and invisibility. By trial and error, the agent acquires advanced tactics that can have been difficult to discover by hand, particularly in cases where there are conflicting and multiple objectives.

Transfer learning enables learning in one task to be helpful in another one. An image watermarking trained network may be fined to do video or document watermarking with fewer samples, reducing development and data needs. Pre-trained vision models learn rich features that can be used in embedding and detection even when the specific data (domain-wise) are few.

The intelligent attack prediction is also driven by machine learning. Models predict probable attacks in the future by analyzing the trends of past attacks and proactively fortify areas of vulnerabilities in watermarks. The anomaly detectors identify anomalous extraction outcomes, which is a signal to apply adaptive countermeasures (e.g., increase the frequency at which it is verified or use more robust watermark payloads). Classification models evaluate the quality of extracted watermarks, and they give confidence scores, which are used to make fined ownership decisions instead of an over-the-counter decision of present/absent.

ML is used to adaptively parameterize embedding strength in Adaptive parameter optimization. The model does not learn a fixed level but rather learns to change the strength depending on texture, density of edges, colour distribution and semantics. As an example, it can use stronger watermarks in very textural regions where the alterations lie concealed and weaker watermarks in smooth regions to prevent artifacts. Content features can be mapped to optimum parameters using regression, decision trees or neural nets.

Content -based watermarking combines natural language processing and computer vision to protect semantic significance. Face, logo, text detection, and segmentation identify areas of interest that must not be tampered with, and the background enables watermark insertion to take place. Video watermarking applies scene analysis to select either temporal embedding of scenes that are not moving or different approaches to rapid motion sequence. Document watermarking identifies boilerplate and sensitive text in documents and only places strong watermarks where necessary.

Application of AI in the cloud creates new problems and possibilities. Distributed learning allocates learning to many servers, using massive compute and a variety of data. Federated learning trains models in a joint manner, wherein parties do not share raw data, thus preserving privacy. Cloud AI services enable small content providers to access advanced watermarking by accessing APIs, making entry barriers low, and without requiring deep knowledge of ML.

There is a significant threat of adversarial machine learning. In AI-based detectors, attackers can create inputs that deceive the detector or delete the learned patterns of watermarks. These threats can be alleviated by strong training, powerful defensive methods, and ensemble approaches to mix different models, although the arms race is also expected to persist.

The obstacle of interpretability still exists. Deep networks tend to act as a black box, and it is difficult to trace how a particular embedding choice was arrived at, or to formally verify security properties. The visualization of attention, saliency mapping techniques and simple model designs partially solve this, although generally, simplifying the model decreases the performance.

The amount of training data and bias are also issues that question the reliability of the model. ML algorithms require massive representative data to represent deployed real situations. If the data is biased towards frequent types of data, the model can break on rare or adversarial inputs. When diverse content is involved, thorough curation, data enhancement, and thorough testing are keys to good results.

Regardless of these challenges, AI and ML are driving watermarking to fully adaptive, intelligent, and automated systems. Few-shot learning, meta-learning, and neural architecture search are developed to minimize data requirements and design automatically. Constant learning enables the systems to evolve to new attacks and media without forgetting the old knowledge. With the maturity of these technologies, AI-based adaptive watermarking is destined to become the baseline of the copyright protection offered in clouds, where maximum strength, invisibility, and effectiveness have never been seen before.

5.3 Blockchain-Enhanced Watermarking and Decentralized Content Authentication

The digital watermarking is now revolutionized by blockchain technology. It removes the fundamental issues of centralized watermark systems by deploying decentralized tamper-evident ledgers. These ledgers result in credible documentation of ownership, the time created and as well as the distribution of content.

Majority of traditional watermark systems have central databases or certificate authorities. They enroll in the watermarks, verify identity, and maintain audit records. This key argument may break down, be ruined, or be spoilt. It also involves faith in one person in power which makes it vulnerable to abuse, corruption, or controversy over originality.

There are several important elements of combining blockchain and watermarking. To begin with, watermark registration can be achieved by creators creating a watermark and sharing the metadata with the blockchain. This metadata has the cryptographic value of the original data, the watermark identifier, the digital signature of the creator, timestamps, the licensing conditions, and ownership statements. The blockchain records create unalterable evidence that the content exists at a specific point in time and creates precedence in ownership claims.

Self-executable blockchain programs known as smart contracts automate the registration process and implement business rules. They are allowed to charge a fee, authenticate creator identity, and emit events upon access and transfer of the content.

Decentralized verification allows anyone to verify watermarked content by retrieving the watermark,

computing the hash of the content, and making a query to the blockchain. There is no need to have central authority. The ownership claims can be verified independently by the court, arbitrators, or other parties via comparing extracted data with the blockchain record.

With the immutability of blockchain, provenance tracking can be used to create end-to-end audit trails. Every single action which includes uploading, embedding, distributing, illegitimate copying, or transferring is logged as a transaction. The resulting chain provides an uncovered history which can be utilized by forensic teams to locate leakage points.

Smart contracts allow application of rights management automation. The usage rights can be in the form of a watermark, which the contract enforces. An example is that the contract can permit use on payment or only in particular regions or time or may require the payment of royalty every time the content is used. Embedded watermarks can identify these contracts without the use of trusted intermediaries.

Some of the blockchain structures would be appropriate for watermarking. Maximum censorship resistance and decentralization Public blockchains, such as Bitcoin and Ethereum, are the most decentralized. Any node may become a member, and information is duplicated in thousands of nodes. They are, however, accompanied by transaction fees, low throughput, and full transparency-problem when watermark data are required to remain confidential. Permission or private blockchains are restricted to only authorized nodes, which enhances speed, privacy, and control. Nonetheless, they lose certain decentralization and continue to depend on trust between the consortium. Hybrid designs place high-value registrations on a public chain and the operations that are of frequent and privacy-sensitive nature on a private chain.

Timestamp anchoring provides a tradeoff. Off-chain systems record watermarking events into a local database, and periodically merge cryptographic evidence, e.g. Merkle tree roots, into a publicly available blockchain. This approach ensures that operations remain effective and confidential, although it ensures that the off-chain records were present at a given point, even in the event of a database attack.

The watermarking improved with blockchain provides cloud-based environments with several advantages. It avoids the use of potentially compromised cloud providers ownership is verified on the blockchain, and not on provider databases. The next thing that can be derived is cross-platform interoperability since ownership record can be available to any Internet-connected system. There is also increased ease in regulatory compliance blockchain audit trails cannot be altered, and this means that copyright and privacy laws have a clear indication of how the data is handled, owned, and how it is licensed.

Challenges remain. Blockchain systems presently can process thousands of transactions per second, which is significantly less than the millions of watermark computations that large cloud systems may require. New consensus mechanisms, layer-2 solutions, and sharding work on a better scaling, although they are in development. Public blockchain transparency may publish sensitive data on the content, ownership, or business relationships. The methods such as zero-knowledge proofs, encryption or privacy-preserving architectures may assist, but they introduce complexity and computing cost.

The other obstacle is legal uncertainty. The question of how blockchain records can be used as evidence in an ownership dispute or copyright case remains to be established by courts and regulators. The issues of jurisdiction, cross-border enforcement, the legal role of smart contracts and liability of automated decisions are still to be addressed. The adoption of a secure blockchain is also a complex and highly skilled process in terms of distributed systems, cryptography, and blockchain platforms, which not every

content provider would be adept at.

More recent studies examine high level integration models. The fusion of AI-blockchain merges watermark embedding based on machine learning and reliable blockchain registration and verification, which will create responsive and responsible systems. Quantum-resistant watermarking anticipates future threats of cryptography by adopting digital signatures and hash functions that are quantum-safe. Cross-chain protocols enable watermark records to cut across blockchains, which makes them resilient and prevents vendor lock-in.

Empirical research demonstrates that blockchain-based watermarking is viable to moderate-scale applications, yet performance limits are observed on high-volume operations. The blockchain provenance tracking has proven more trustworthy and accountable in the industries of journalism, photography, medical imaging, and legal documentation than the traditional centralized systems. However, the barrier of technology, ambiguous regulatory instructions, and issues about cost as compared to the traditional methods inhibit its broad use.

In the future, the watermarking with blockchain additions will possibly gain progressive adoption in high-value, sensitive-to-trust, and requirements where the decentralization, immutability, and transparency will be worth the added cost and complexity. With maturity of the technology, in terms of enhancements to scalability, privacy, and usability, wider use of the cloud-based approach to content protection should be anticipated. Combining blockchain with AI-controlled adaptive watermarking and quantum-resistant cryptography would ultimately provide end-to-end, future-proof intellectual property protection to distribute digital ecosystems.

5.4 Security Analysis Attack Vectors, Vulnerabilities, and Countermeasures

To come up with effective protection systems against unauthorized access to their watermarking systems, it is paramount to understand what security threats these systems face and be able to develop both opportunistic and advanced adversarial attacks. Attacker goals (removal, detection, forgery, or protocol attacks), technical methods (signal processing, geometric, cryptanalytic, or machine learning-based), and resources requirements (computational complexity, access to original content, or knowledge of watermarking algorithms) can be used to classify watermarking attacks.

Removal attacks focus on removing watermarks to be able to redistribute content without detection. Simple removal attacks involve the application of the most popular signal processing techniques like lossy compression (JPEG, MPEG), filtering (smoothing, sharpening, denoising), addition of noise, or requantization. The techniques usually perform well with fragile watermarks but not with strong designs that can withstand such alterations. Advanced removal In more advanced attacks, wavelet denoising is used to mask watermark signals at a fixed quality collusion attacks are used to combine multiple copies together to remove watermarks, or neural networks are trained to remove watermarks in large dataset adversarial machine learning.

Geometric attacks modify content by geometric warping, either spatially or temporally, to use watermark-synchronization vulnerabilities, such as rotation, scaling, cropping, aspect-ratio changes, or shifting video frames. Most of the algorithms expected extraction to be done on geometrically similar content and hence any deviation would lead to failure in detection. Some countermeasures comprise embedding in geometry-invariant spaces, an autocorrelation property or synchronization pattern which is invariant under transformations, or exhaustive search over the space of possible transformations at the extraction point, albeit with a very high computational cost.

The protocol attacks are aimed at the system process, but not at the watermark. The copy attacks strips a watermark of one piece of work and places it in another, which might allow invalid claims of ownership. Forgery attacks generate counterfeit watermarks that verifiers are deceived by. Oracle attacks query detectors repeatedly to get to know algorithmic information and locate the slightest changes that eliminate watermarks without being detected. Cryptographic authentication in the defense, detector design resistant to oracle attacks by rate limiting or randomness, and legal or technical constraints preventing access to the detector by attackers are required.

Cryptanalytic attacks target the cryptographic elements of the watermarking systems, making attempts to determine the secret keys, crack encryption schemes used to protect watermark data, or create digital signatures. Brute-force attacks use up key spaces and only work with systems having inadequate key lengths. Side-channel attacks take advantage of physical leakage, e.g. timing, power, or electromagnetic emanations, which are correlated with secret keys. Mitigations involve the use of secure key lengths (e.g. 256-bit symmetric keys or 3072-bit RSA keys), constant-time algorithms and the use of hardware security modules to store and execute keys and operations without tampering.

A type of attack that is currently becoming an emerging threat is machine-learning based attacks, which involves the adversaries identifying, identifying, or erasing watermarks through the use of AI. The process can be used to classify watermarked as unwatermarked content where the statistical artifacts added by watermarking can be learnt even when the watermark is imperceptible to the human eye. Generative models which are trained on watermarked- original data can be trained to learn transformations which remove watermarks without affecting the perceptual quality. The adversarial examples that are specific to the AI detectors elude detection. The defenses are adversarial training to introduce watermarking systems to synthetic ML attacks, ensemble-based, which is a combination of different detection algorithms, and randomization, which makes learned models less predictable.

The cloud-related vulnerabilities introduce new attack surfaces into distributed environments. Multi-tenant attacks take advantage of the shared infrastructure to analyse side-channels, cross-tenant data leakage, or resource-exhaustion denial-of-service to watermarking services. Weaknesses of cryptography One can bypass cryptographic protection by privileged administrators who have access to watermarked content, keys, or algorithms. Supply-chain attacks can introduce backdoors into the software, libraries, or hardware that can be used to remove the watermarks or extract keys. Migration attacks can impact on content transfers between cloud providers or storage levels, and content might replace watermarked content with unmarked content on transit.

The proposed countermeasures to cloud-specific threats are secure computation in untrusted environments with homomorphic encryption to watermark encrypted data, trusted execution environments which isolate sensitive computations and secure multi-party computation where the processing is distributed so no one party learns sensitive information. Digital signatures and message authentication codes with cryptographic authentication and integrity protection keep the content and watermarks intact in the process of storage or transmission. Reducing the insider threats is achieved through access control, minimizing privileges, separation of duty, and constant observation of unusual access patterns, reducing access of administrators to keys and algorithms.

Watermark strength testing should be done under organized attacks with extensive benchmarks. The suites of attacks, coded as compression, filtering, geometric transformations and combinations, are offered by standardized toolkits like Stir Mark, Checkmark and their descendants to compare various watermarking algorithms against each other. Nevertheless, the current benchmarks usually do not keep

with state-of-the-art attacks, especially those involving machine-learning and cloud-specific attacks. Continuing to come up with revised benchmarks that depict modern attacks capabilities is a significant research agenda.

The analysis of watermarking system in formal security frameworks is not well-developed. Finally, most of the assessments are based on empirical testing to known attacks, but not formal proofs to well-defined threat models. Establishing strong theory, such as clear definitions of security properties (unforgeability, undetectability, removability), and formal proofs that we have a certain scheme meeting these properties under very clear assumptions, would go a long way toward making watermark security credible.

Dynamically responding adaptive defense mechanisms that are responsive to observed attacks have potential to improve resilience. The intrusion detection systems can request patterns of anomalies in the extraction of watermarks, content manipulations or access logs that can point to continued attacks, and respond by hardening subsequent watermarks, credential revocation, or triggering alarms. Adaptive watermarking algorithms have the capability to enhance the embedding power when the environment is known to be under high threat as per threat intelligence but decrease overhead when the environment is known to be of lower risk. That is because honeypot watermarks on decoy materials can identify and research the attacker capabilities without exposing precious properties.

The presence of the arms race between the defenders and the attackers guarantees that the issue of security analysis continues to be a matter of constant priority. Attackers also innovate in watermarking removal as the watermarking schemes become more effective, so more innovations in embedding and detection are made. Such a dynamic requires ongoing security research, frequent updates to implementations, and active threat hunting to identify new attack vectors before they become a mass exploit.

5.5 Quantum-Resistant Watermarking and Preparing for Post-Quantum Cryptography

Real quantum computers have a risk to the cryptographic basis of currently used digital security systems, such as those used to protect digital watermarks.

Quantum algorithms like the Shor or algorithm can factor and calculate discrete logarithms, breaking popular public-key primaries like RSA, DSA, and ECC. Such schemes now defend keys to watermarks, watermark verification, and watermarking system traffic security. Protecting copyright may take decades even though large-scale quantum machines capable of attacking current standards are yet to be developed. Hence, we should be ready to face a post-quantum world now.

Post-quantum cryptography bases cryptography on mathematical problems that are difficult even to quantum computers. Some of the leading families are lattice-based schemes (e.g. LWE, SIS), code-based schemes, hash-based signatures, multivariate polynomial schemes, and isogeny-based cryptosystems. NIST has also conducted multi-year assessments and suggests certain algorithms in key encapsulation, digital signatures, and other primitives, which gives a transition roadmap.

To make post-quantum cryptography part of the watermarking process, the key generation and distribution process should be prepared with quantum-resistant algorithms to preserve the watermark keys against the quantum attack. Lattice based schemes, including CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Di lithium (signatures), are both highly secure and have efficient implementations that are scalable to performance sensitive watermarking applications. Digital signatures can be used to prevent forgery and ensure non-repudiation hence we need to substitute weak RSA or ECDSA signatures by

quantum-resistant signatures such as SPHINCS+ and lattice-based signatures. Embedding server to Distribution network and verification endpoint communication is advised to upgrade TLS based on public-key primitives to protocols based on quantum-resistant key exchange and authentication.

Hybrid strategies merge classical and post quantum algorithms to combat present and future threats. E.g a key encapsulation might employ a combination of ECDH, and a lattice based scheme an attacker would have to break both to violate confidentiality. This defense in depth system is safe if a post quantum algorithm is later proved to be flawed, but resistant to quantum attacks. Hybrid designs, in turn, introduce computational overhead and complexity in implementation, that need to be handled with care.

The watermark embedding domains might need to change since not all the techniques are based on number-theoretic structures and can be exploited by quantum algorithms. Quantum attacks directly target watermarking schemes using discrete logs on some finite field or elliptic curve. Switching to quantum-resistant designs, e.g. lattice-based designs, hash-based commitments or coding-theory designs, is such that embedding and extraction are both secure against quantum adversaries.

Quantum key distribution employs quantum mechanics as a tool to generate provably secure keys invulnerable to both classical and quantum attacks. QKD protocols transmit qubits (commonly photons) via optical media and observe eavesdropping as the artifacts of measurement. Although QKD offers security, which is theoretically ideal, practical implementations have problems range is limited, the equipment is specialized, and there are side-channel attacks on physical devices. QKD can be cost-effective in high-value watermarking, where the security of keys is paramount otherwise post-quantum cryptography can be more feasible.

The size of key, length of signature and cost of computation of post-quantum algorithms are usually larger than, e.g., classical schemes. The attraction of lattice-based schemes is that they utilize keys of kilobyte size and are rapidly implemented with number-theoretic transforms. The most secure signatures are the hash-based signatures which require minimum assumptions but generate large signatures which are not ideal in size limited applications. Code-based cryptography is also relatively fast for encrypting and decrypting but uses very large public keys which might not be able to fit in embedded devices. The choice of the appropriate algorithm thus relies on the factor of trade-off between security, performance and resource constraints when using a particular watermarking application.

A transition to quantum-resistant watermarking should maintain the capability to authenticate previously encrypted classical cryptography work. A gradual transition may be performed by continuing to support old verification and watermarking new content under quantum-resistant watermarking schemes, a process that progressively changes the installed base. Cryptographic agility, i.e. the ability to easily change the algorithm used without a significant architectural modification, is the ability to design systems that can be adapted to changes in post-quantum standards.

Although NIST and other standards organizations have progressed with post-quantum primitives, there is little guidance on watermarking. Industry associations, academics, and standards bodies should work jointly to create best practices, reference implementations and conformance tests of quantum-resistant watermarking, interoperability, and security in the transition.

Conservative estimates say that the emergence of large-scale quantum machines as a way to break the cryptography we know of today will take 10-20 years, although many technical challenges still exist. The so-called harvest now, decrypt later model, in which attackers store encrypted information now and will decrypt it later, recommends urgent implementation of transition to quantum-resistant cryptography, particularly of content that will be required to be verified decades in the future. Therefore, preemptive

deployment is acceptable even with unpredictable schedules.

Future directions include designing watermarking schemes that are based on post-quantum primitives, finding quantum information theory solutions that apply superposition and entanglement to achieve greater security, and establishing post-quantum secure multiparty computation schemes to implement distributed watermarking in the cloud. Watermarking systems should also keep up with the advancement of quantum technology to ensure that vital copyrights are preserved.

6. CONCLUSION

Summary of Findings

This review analyzes watermarking technologies that are used to secure copyright on clouds in digital computing. The use of traditional types of watermarking has been grounded on a strong foundation, yet the dynamic and distributed, as well as adversarial characteristics of cloud ecosystems entail some core innovations in methodologies, architecture, and security controls.

To begin with, cloud-based security has issues that are not like the traditional offline watermarking. These are the necessity to scale to a massive degree over distributed infrastructure, the necessity to support heterogeneous content, content quality, multi-tenancy, and insider access attack vectors, and the necessity to trade-off forensic tracking with user privacy. Real time processing is also required by performance constraints. Common watermarking algorithms are designed to be single image offline, and in complex cloud applications are not robust, adaptive, or efficient.

Secondly, machine learning and artificial intelligence cause a revolutionary change. Adaptive watermarking systems can discover optimum embedding techniques using data, dynamically predict and mitigate attacks and learn over time using experience. Deep learning models, reinforcement learning agents and content-aware computer-vision processes are superior to non-dynamic and manual methods. Nevertheless, AI-powered systems also come with novel vulnerabilities through adversarial attacks and pose interpretability issues to security-critical applications.

Third, blockchain technology solves fundamental issues of trust. Immutable records of ownership, provenance and licensing are formed by decentralized ledgers that cannot be tampered with. Blockchain allows cross-border trustless verification and automated rights management through smart contracts by removing single points of failure. Its implementation, though, is mostly in high-value, trust-based situations because of the scale constraints, privacy conflicts, legal ambiguities, and technical complexity.

Fourth, the analysis of security shows that there is an arms race. There are more advanced attackers of signal processing, geometric, cryptanalytic, protocol, and machine-learning attacks to which defenders must deal. Multi-tenant vulnerabilities, insider threat, and supply-chain compromise represent cloud specific threats that require defense in depth approaches based on strong embedding, cryptographic authentication, secure computation, access control and continuous monitoring. A major gap in research is that formal security analysis frameworks are not well developed relative to modern cryptography.

Fifth, quantum computing will pose a menace to the cryptography principles behind the existing watermarking regimes. Quantum algorithms can break existing public-key schemes. Long-term security requires a proactive switch to post-quantum encryption, namely lattice-based, hash-based, code-based or other quantum-resistant primitives, particularly with decades-long copyright protection durations. Although these algorithms are over heading, a compromise between security, efficiency, and backward compatibility can be achieved through hybrid solutions and the judicious choice.

7. CONTRIBUTION AND SIGNIFICANCE

The review provides a synthesis of the integration of watermarking technologies with the cloud computing needs. It is an intersection of signal processing, cryptography, distributed systems, machine learning, and legal norms, providing both backward-looking information on the evolution of technology and direction on how it is going to evolve. Cloud-specific challenges, attack vectors, and countermeasures taxonomy offers researchers, system designers, and security practitioners an organizational framework on how to balance robustness, imperceptibility, capacity, performance, and security. The review educates decision-making in particular application situations by critically evaluating traditional, AI-based, blockchain-based, and quantum-resistant methods and strategies.

To academic researchers, it highlights open problems that include the construction of formal security models, efficient quantum resistant implementations, and blockchain architectures that are privacy preserving. To the industry practitioners, it shows the state-of-art possibilities, implementation factors, and the migration of the next generation watermarking solutions. As to policymakers and legal scholars, it can explicate the technical basis in order to design informed copyright laws, liability frameworks, and coordination mechanisms across borders in clouds.

8. IMPLICATIONS

The implications of the findings are very profound in various fields. To creators and people who own copyright, the discussion demonstrates that the best cloud security features include not only leaving DRM of the past and adopting advanced watermarking technology but also incorporating AI adjustment, blockchain authentication, and quantum-resistant security. Knowledge of these abilities and constraints allows superior content protection strategies, platform choice, and risk control.

To cloud service providers, the review is an indication that there are increased demands on embedded watermarking capabilities as an integral part of a platform and not a feature-on-demand. The providers must negotiate between security, performance, privacy, and usability and operate within the realms of liability in matters involving copyright infringement. Placing investment in quantum-resistant and AI-adaptive infrastructure makes the provider competitive as security becomes the focus of the customer needs.

To technology vendors and system integrators, AI, blockchain, and post-quantum cryptography convergence can present both opportunities and challenges. Technological combinations that can suit market needs can be developed by new solutions, yet technical complexity, interoperability, and the changing threats must be managed. Standardization is essential to common interfaces, protocols, and metrics of evaluation.

The technology environment highlights policymakers and regulators the pressing nature of having to revise legal frameworks that govern copyright in distributed digital environments. Current regulations presuppose centralized control and territorial relocation which do not align with multi-jurisdictional clouds. The priority areas are international coordination of the enforcement of cross-border compliance, provider liability in safe harbor statutes, and alignment of privacy regulations with forensic watermarking provisions.

To society, there should be a balance between incentives towards creative production, access to information to the people, privacy, and innovation when protecting copyright in the cloud. Watermarking technologies must navigate these tensions carefully providing the kind of protection of legitimate rights without being oppressive surveillance or suppressive of the transformative uses. Watermarking

implementations can be aligned with democratic principles and human rights through transparent governance, algorithmic accountability, and participatory design.

9. LIMITATIONS

This review observes that there are several limitations that must influence the interpretation of the findings and reflect the future working areas.

First, watermarking and cloud architecture technological change is fast new technologies have the potential to make some of the aspects of this analysis obsolete. The review deals with the underlying principles and some challenges that still exist irrespective of certain changes in technical aspects, though the readers must add to it continuous tracking of new studies and industry developments.

Second, although the coverage of literature is quite comprehensive, it cannot be called absolute due to the enormous number of research works in numerous fields that are growing rapidly. The given systematic search strategy was intended to reveal the key themes, representative works, and significant innovations, but each individual reader with specific interests can find some additional sources that add to the specific part of the analysis.

Third, the review is broader in covering a wide range of watermarking methods, areas of application, and integration with technology compared to depth in a single subject. More expert reviews which concentrate on narrow subtopics, like lattice-based watermarking or blockchain-based content authentication, may be able to provide more information than a general overview can.

Fourth, comparison of empirical performance of various watermarking methods is low due to missing a set of standardized evaluation systems, diverse experimental environments and proprietary watermarking systems that make them not repeatable. The challenges of quantitative meta-analysis that combine performance metrics between studies is that the methodologies used are heterogeneous such that comparisons are hard to make. The review is an attempt to synthesize qualitative trends and relative performance characteristics and recognize these empirical limitations.

Fifth, cloud-based watermarking has interdisciplinary coverage in terms of technical, legal, economic, and social. Although the review is based mostly on a technical computer-science viewpoint, different things may be highlighted or different conclusions made by legal scholars, economists, or other social scientists depending on the disciplinary paradigms they operate under. The interdisciplinary discussion that includes these interpretations would enhance the knowledge that is not provided by a review that is single-disciplinary.

10. FUTURE RESEARCH DIRECTIONS

The discussion shows that there are a lot of open prospects in future research to overcome limitations, new opportunities and promote knowledge in cloud-based digital watermarking to protect copyright.

1. Federated and privacy preserving watermarking.

Study can come up with methods of enabling joint watermark training and verification across organizational lines without revealing sensitive data, trade secrets, or personal details of users. A technical basis through leverage of federated learning, secure multiparty computation, differential privacy, and homomorphic encryption is necessary, but specific applications on watermarking require studies.

2. Propositional security structures and witnessed security.
Formulating accurate definitions of watermark security, like semantic security in cryptography, and reducing them to well-known computational hardness conjectures can help people have more confidence in protection systems. The creation of watermarking schemes with reasoning security guarantees is a significant theoretical design, with key real-life consequences.

3. Cross-domain watermarking
An international structure that works across pictures, video, audio, files and 3D designs- and amongst cloud environments- would enhance interoperability and decrease implementation intricacy. Studies are needed on transfer learning, interfaces that are standardized, and domain-independent algorithms.

4. Watermarking of edge devices that is eco-friendly in terms of energy usage.
Resource-constrained IoT endpoints require lightweight algorithms that can compromise security with little computation, memory, and energy overhead. Approximate computing, hardware acceleration and algorithm-hardware co-design Studies have prospects.

5. Adversarial robustness
Watermarking systems should be trained to be resistant to learned strategies of removing watermarks, generative adversarial techniques and adaptive attacks that leverage defensive information. Adversarial training, certified defenses with provable guarantees and randomization are ways to increase resilience.

6. Quantum watermarking
The use of quantum information theory based watermarking - superposition, entanglement, and the no-cloning theorem - has presented a source of novel security opportunities. Even though the technical difficulties of quantum watermarking are still a challenge at present, theoretical work can map the way forward in the implementation as quantum technologies reach maturity.

7. Standardization and interoperability.
The industry, academia, and standards bodies ought to work together and develop standard protocols, interfaces, and evaluation systems that can verify a watermarked content across systems, algorithms, and organizations. Conformance testing and reference implementations and certification programs will spur the growth of the ecosystem.

8. Human factors and usability
Researching user interaction with watermarked content, perceptions of copyright protection, and response to watermark notification can be used to design better systems. To balance security with user experience, transparency and automated enforcement whilst taking into consideration privacy one needs to understand the social and cognitive aspects.

9. Legal and ethical systems.
The cooperation of different fields can result in the recommendations of the responsible deployment, such as the forensic tracking limits, accountability tools and the dispute resolution system. These models will facilitate ethical application of watermarking technologies.

10. Economic analysis
Research into the cost, benefits and incentive schemes of watermarking can guide business models, pricing policies and policy interventions. The effect on the content creation incentive, the efficiency of distribution, the platform competition, and the social welfare will serve as the proof of assessing policy options.

Taken together, these study directions constitute a deep roadmap of future development of cloud-based

digital watermarking. The advancement needs long-term cooperation between the researchers, practitioners, policymakers, and users combined with technical innovation and social awareness to develop solutions that secure copyright without violating privacy, encourage innovations, and in the best interest of the population.

AUTHOR'S NOTE

This review presents the summary of existing information on the topic of digital watermarking in clouds to safeguard copyrights, discusses the basic principles, new technologies, including AI and blockchain, security issues, quantum-resistant solutions, and prospective research approaches. It attempts to make researchers, practitioners, policymakers, and informed general readers appreciate the essential cross-section of the protection of copyright, cloud computing, and advanced security technologies. Since the field is dynamically developing, it is recommended that the readers add to this review by performing ongoing evaluations of the newest scholarly literature, developments in the industry, and legal frameworks.

REFERENCES

[1] Chippagiri, S. (2026). Cloud-Based Content Distribution and Copyright Vulnerabilities. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 1-36). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch001

[2] Agrawal, A., Verma, S., Sharma, A. K., Kumar, A., Mann, M., & Baniya, P. (2026). Security Challenges in Cloud-Based Watermarking. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 37-64). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch002

[3] Lokireddy, C. R., Princi, Sinha, P., Sharma, A. K., Mishra, R., & Sharma, A. K. (2026). Blockchain in Digital Watermarking. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 65-84). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch003

[4] Dr.A.Shaji George, & Dr.T.Baskar. (2025). Domestic Service Transformation in India: Digital Integration, Economic Mobility, and Social Dynamics in the Informal Maid Service Sector. Partners Universal International Research Journal (PUIRJ), 04(02), 89–111. https://doi.org/10.5281/zenodo.15710098

[5] Vats, S., Sharma, V., Singh, P., Thakur, S., & Rawat, D. (2026). How Do LLMs Work?: A Deep Dive Into Transformer Models. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 85-106). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch004

[6] Yadav, N., Singh, M., & Tyagi, V. (2026). AI and ML Approaches in Adaptive Watermarking. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 107-140). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch005

[7] Yadav, N., Singh, M., & Tyagi, V. (2026). Security Analysis: Attacks and Countermeasures in Watermarking Systems. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 141-174). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch006

[8] Dr.A.Shaji George. (2025). The Digital Carbon Footprint: Examining Email Proliferation and its Socio-Environmental Impact. Partners Universal Multidisciplinary Research Journal (PUMRJ), 02(03), 160–182. https://doi.org/10.5281/zenodo.15477192

[9] Saraswat, B. K., Joshi, P., Ritika, Yadav, S. P., & Munjal, H. (2026). Adaptive Watermarking Algorithms for Multi-User Cloud Environments. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 175-194). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch007

[10] Kapoor, E., Mahendru, A., Goswami, K., & Yadav, R. K. (2026). Hybrid DCT-DWT-SVD Watermarking: A Comparative Performance Analysis. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 245-260). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch011

[11] Tyagi, R., Singh, S., Takuli, A. K., & Bhardwaj, A. (2026). Dynamic Watermarking for Multi-Tenant SaaS Applications. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 313-326). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch014

[12] Dr.A.Shaji George. (2024). Digital Transformation in Business: Opportunities, Challenges, and Implications. Partners Universal Innovative Research Publication (PUIRP), 02(06), 46–54. https://doi.org/10.5281/zenodo.14599717

[13] Banerjee, P., Faraz, A., Kumar, M., & Mitra, D. (2026). An Analytical Study of Cloud Computing Fundamentals and Applications. In A. Kumar, A. de Alexandria, S. Yadav, & A. Galletta (Eds.), Digital Watermarking in Cloud Environments For Copyright Protection (pp. 327-354). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3785-2.ch015

[14] Sanivarapu PV, Rajesh KNVPS, Hosny KM, Fouda MM. Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques. Applied Sciences. 2022; 12(17):8724. https://doi.org/10.3390/app12178724

[15] Naem , S. A. S. ., & Hameed , S. M. . (2025). Digital watermarking techniques, challenges, and applications: A review. Mesopotamian Journal of CyberSecurity, 5(2), 453-476. https://doi.org/10.58496/MJCS/2025/028

[16] Fkirin, A., Attiya, G., El-Sayed, A. et al. Copyright protection of deep neural network models using digital watermarking: a comparative study. Multimed Tools Appl 81, 15961–15975 (2022). https://doi.org/10.1007/s11042-022-12566-z

[17] Kumar, A.; Kumar, M.; Verma, S.; Kavita; Jhanjhi, N.Z.; Ghoniem, R.M. Vbswp-CeaH: Vigorous Buyer-Seller Watermarking Protocol without Trusted Certificate Authority for Copyright Protection in Cloud Environment through Additive Homomorphism. Symmetry 2022, 14, 2441. https://doi.org/10.3390/sym14112441

[18] Boland, F.M., O'Ruanaidh, J.J., & Dautzenberg, C. (1995). Watermarking digital images for copyright protection.

[19] Boujerfaoui S, Riad R, Douzi H, Ros F, Harba R. Image Watermarking between Conventional and Learning-Based Techniques: A Literature Review. Electronics. 2023; 12(1):74. https://doi.org/10.3390/electronics12010074

[20] Veginadu P, Calache H, Gussy M, Pandian A, Masood M. An overview of methodological approaches in systematic reviews. J Evid Based Med. 2022 Mar;15(1):39-54. doi: 10.1111/jebm.12468. PMID: 35416433; PMCID: PMC9322259.

[21] Gusenbauer M. Beyond Google Scholar, Scopus, and Web of Science: An evaluation of the backward and forward citation coverage of 59 databases' citation indices. Res Synth Methods. 2024 Sep;15(5):802-817. doi: 10.1002/jrsm.1729. Epub 2024 Jun 14. PMID: 38877607.

[22] Dr.A.Shaji George. (2025). DIGIPIN: India's Revolutionary Geo-Coded Addressing System and Its Impact on Digital Public Infrastructure. Partners Universal Innovative Research Publication (PUIRP), 03(03), 20–34. https://doi.org/10.5281/zenodo.15606630

[23] Ahmed, S. (2025). Enhancing data security and transparency: The role of blockchain in decentralized systems. International Journal of Advanced Engineering Management and Science, 11(1), 167–176. https://doi.org/10.22161/ijaems.111.12

[24] AMan's AI Journal • Primers • Generative Adversarial Networks (GANs). (n.d.). https://aman.ai/primers/ai/gan/

[25] Author. (2019, December 11). What is blind and non-blind watermarking? – Heimduo. https://heimduo.org/what-is-blind-and-non-blind-watermarking/

[26] George, D. (2024). Bridging the digital Divide: Understanding the human impacts of digital transformation. Zenodo. https://doi.org/10.5281/zenodo.11287684

[27] Awasthi, D., Tiwari, A., Khare, P., & Srivastava, V. K. (2023). A comprehensive review on optimization-based image watermarking techniques for copyright protection. Expert Systems With Applications, 242, 122830. https://doi.org/10.1016/j.eswa.2023.122830

[28] George, D., & Dr.T.Baskar. (2025). Artificial intelligence transformation of digital interaction platforms and economic opportunity structures. Zenodo. https://doi.org/10.5281/zenodo.17147924

[29] Hoshi, A. R., Zainal, N., & Fadhil, M. (2024). Digital watermarking: Innovations and challenges in copyright protection. AIP Conference Proceedings, 3232, 020023. https://doi.org/10.1063/5.0236361

[30] George, D., & George, A. (2025). How artificial intelligence systems function as digital migrants creating more profound societal disruption than human immigration. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.16112307

[31] IEEE Xplore Full-Text PDF: (n.d.). https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11017625

[32] Li, W., & Peng, X. (2020). Evaluation of cloud computing Copyright Protection based on AHP.

Mathematical Problems in Engineering, 2020, 1–11. https://doi.org/10.1155/2020/6671331

[33] Mekhfioui, M., Bazi, N. E., Laayati, O., Satif, A., Bouchouirbat, M., Kissi, C., Boujiha, T., & Chebak, A. (2025). Optimized digital watermarking for robust information security in embedded systems. Information, 16(4), 322. https://doi.org/10.3390/info16040322

[34] Nna Halima, A., Danlami Abdulmalik, M., Aminu, E. F., & Adepoju, S. A. (2022). A survey of digital watermarking Techniques for data Protection in cloud computing. 2022 5th Information Technology for Education and Development (ITED). https://doi.org/10.1109/ITED56637.2022.10051180

[35] Protecting Intellectual Property in the Cloud. (n.d.). https://www.wipo.int/en/web/wipo-magazine/articles/protecting-intellectual-property-in-the-cloud-39196

[36] Reddio. (2025, February 16). Chapter 1: Understanding Blockchain Scalability Challenges. Reddio Technology Blog. https://blog.reddio.com/chapter-1-understanding-blockchain-scalability-challenges/

[37] Singh, B., & Kasana, G. (2024). A review of digital watermarking techniques: Current trends, challenges and opportunities. Web Intelligence, 22(4), 523–553. https://doi.org/10.3233/web-230280

[38] Sundhararaj, V., Meenakshipriya, B., Devi, P. N., & Vignesh, K. E. (2025). DWT-DCT-SVD: A Hybrid Image Watermarking Algorithm with FPP Resistant Enhancement. Circuits Systems and Signal Processing, 44(9), 6650–6675. https://doi.org/10.1007/s00034-025-03097-7

[39] Team, C. (2024, March 19). Ensuring Intellectual Property Protection in the Era of Cloud Computing - Claimistry. My Blog. https://claimistry.com/cloud-computing-and-ip-protection/

[40] Top 20: Digital content creation companies in the world. (n.d.). https://www.globalgrowthinsights.com/blog/digital-content-creation-companies-475

[41] Uddin, M. S., Ohidujjaman, Hasan, M., & Shimamura, T. (2024). Audio Watermarking: A Comprehensive review. International Journal of Advanced Computer Science and Applications, 15(5). https://doi.org/10.14569/ijacsa.2024.01505141

[42] Wang, B. (2025, January 17). Why trustless infrastructure is the key to blockchain's future | NextBigFuture.com. NextBigFuture.com. https://www.nextbigfuture.com/2025/01/why-trustless-infrastructure-is-the-key-to-blockchains-future.html

[43] Watermarking Process | adobe/trustmark | DeepWiki. (n.d.). DeepWiki. https://deepwiki.com/adobe/trustmark/2.2-watermarking-process

[44] Ye, P., Li, Z., Yang, Z., Chen, P., Zhang, Z., Li, N., & Zheng, J. (2025). Periodic watermarking for copyright protection of large language models in cloud computing security. Computer Standards & Interfaces, 94, 103983. https://doi.org/10.1016/j.csi.2025.103983