Office of the Controller General of Patents, Designs & Trade Marks
Department for Promotion of Industry and Internal Trade
Ministry of Commerce & Industry,
Government of India

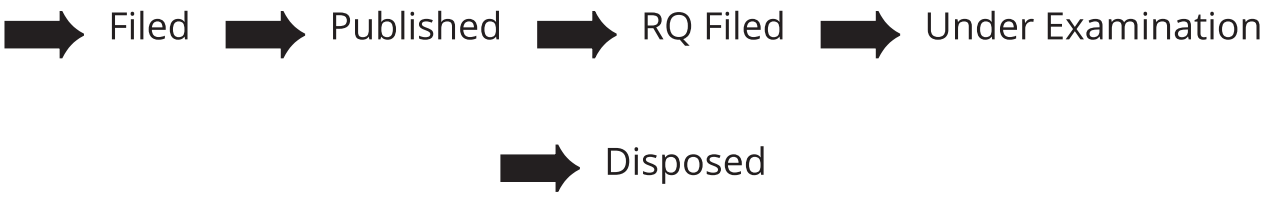
(http://ipindia.nic.in/index.htm)

(http://ipindia.nic.in/index.htm)

Application Details	
APPLICATION NUMBER	202511036219
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	15/04/2025
APPLICANT NAME	**1 . Mr. Merdul Sharma** **2 . Ms. Aastha** **3 . Mr. Divyanshu Ranjan Singh** **4 . Mr. Aman** **5 . Dr. Ashish Dixit**
TITLE OF INVENTION	TAMPER-PROOF MEDIA PROTECTION SYSTEM USING SECURE MACHINE LEARNING-BASED DIGITAL WATERMARKING
FIELD OF INVENTION	COMPUTER SCIENCE
E-MAIL (As Per Record)	rajudixit1984@gmail.com
ADDITIONAL-EMAIL (As Per Record)	
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	--
PUBLICATION DATE (U/S 11A)	02/05/2025

Application Status	
APPLICATION STATUS	**Awaiting Request for Examination**

View Documents



In case of any discrepancy in status, kindly contact ipo-helpdesk@nic.in

पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 18/2025	शुक्रवार	दिनांक: 02/05/2025
ISSUE NO. 18/2025	FRIDAY	DATE: 02/05/2025

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :15/04/2025

(21) Application No.202511036219 A
(43) Publication Date : 02/05/2025

(54) Title of the invention : TAMPER-PROOF MEDIA PROTECTION SYSTEM USING SECURE MACHINE LEARNING-BASED DIGITAL WATERMARKING

(51) International classification	:G06T0001000000, G06N0020000000, H04L0009320000, G06F0021100000, G06F0021640000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Mr. Merdul Sharma
Address of Applicant :B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh ---------- ----------
2)Ms. Aastha
3)Mr. Divyanshu Ranjan Singh
4)Mr. Aman
5)Dr. Ashish Dixit
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Mr. Merdul Sharma
Address of Applicant :B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh ---------- ----------
2)Ms. Aastha
Address of Applicant :B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh ---------- ----------
3)Mr. Divyanshu Ranjan Singh
Address of Applicant :B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh ---------- ----------
4)Mr. Aman
Address of Applicant :B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh ---------- ----------
5)Dr. Ashish Dixit
Address of Applicant :Associate Professor, Computer Science & Engineering Department, Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh, India ---------- ----------

(57) Abstract :
The present invention relates to a secure, machine learning-based digital watermarking system and method designed to ensure tamper-proof protection of digital media content. The invention integrates intelligent watermark embedding, extraction, and tamper detection using adaptive machine learning algorithms, allowing imperceptible yet robust watermarking that resists a wide range of modifications, including compression, cropping, and malicious alterations. By leveraging feature-based learning models, the system dynamically identifies optimal embedding zones within the media and ensures accurate verification and authentication of ownership and integrity. This solution is applicable across various digital formats such as images, videos, and audio, offering a scalable, real-time, and highly secure mechanism for digital rights management, forensic tracking, and media authenticity verification. Accompanied Drawing [FIGS. 1-2]

No. of Pages : 24 No. of Claims : 10

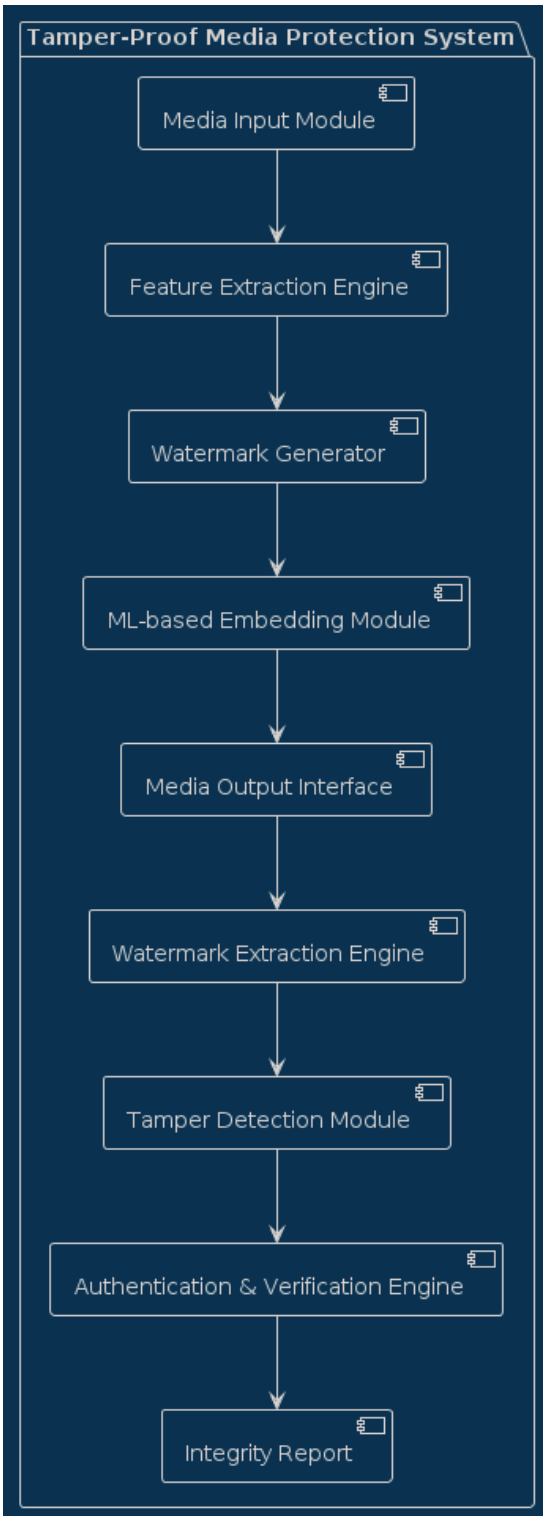


Fig. 1

Signature: Merdul Sharma

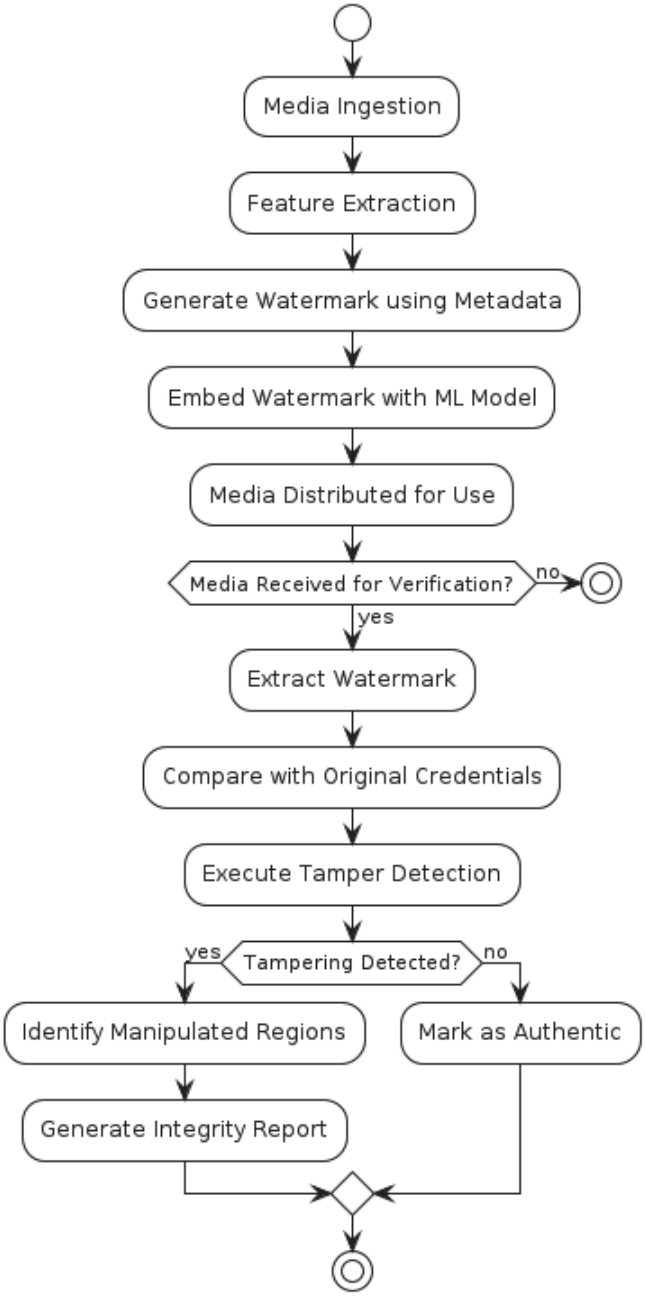


Fig. 2

Dated this 14th day of April 2025

Signature: Merdul Sharma

Applicant(s) Name: Mr. Merdul Sharma et. al.

FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

The Patent Rules, 2003

COMPLETE SPECIFICATION

(See section 10 and rule 13)

TITLE OF THE INVENTION

"TAMPER-PROOF MEDIA PROTECTION SYSTEM USING SECURE MACHINE LEARNING-BASED DIGITAL WATERMARKING"

Applicant(s)

NAME	NATIONALITY	ADDRESS
1. Mr. Merdul Sharma	Indian	B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh
2. Ms. Aastha	Indian	B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh
3. Mr. Divyanshu Ranjan Singh	Indian	B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh
4. Mr. Aman	Indian	B. Tech Scholar, Department of Computer Science &Engineering (Artificial Intelligence & Machine

		Learning), Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh
5. Dr. Ashish Dixit	Indian	Associate Professor, Computer Science & Engineering Department, Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh, India

The following specification particularly describes the nature of the invention and the manner in which it is performed:

FIELD OF THE INVENTION

[001] The present invention relates to the field of digital media security and authentication. More particularly, it pertains to a system and method for embedding, securing, and verifying digital watermarks within multimedia content such as images, audio, and video using machine learning techniques. The invention is designed to provide robust protection against unauthorized manipulation, duplication, or tampering by enabling intelligent, adaptive, and tamper-proof watermarking that enhances the traceability, authenticity, and integrity of digital assets in various domains including media distribution, digital forensics, copyright protection, and secure content sharing.

BACKGROUND OF THE INVENTION

[002] In the modern digital era, the proliferation of multimedia content across the internet and communication platforms has made it increasingly easy to access, share, and modify digital media. While this democratization of content has revolutionized information exchange, it has also introduced substantial challenges in terms of intellectual property protection, unauthorized replication, and media tampering. Images, videos, and audio files can now be copied, edited, and redistributed with minimal effort, often without any attribution to the original creator or owner.

[003] Digital watermarking has long been a widely adopted solution to counter such misuse. It involves embedding an invisible or imperceptible signal (the watermark) into digital content, which can later be extracted or detected for purposes such as ownership verification, copyright enforcement, or tamper

detection. Traditional watermarking techniques primarily rely on fixed algorithms based on spatial or frequency domain manipulations. Although effective to some degree, these conventional methods are often static, vulnerable to deliberate attacks, and lack the adaptability to withstand sophisticated modifications such as deepfakes, compression artifacts, and machine-generated forgeries.

[004] In recent years, attackers have developed advanced tools that can identify and strip or distort watermarks without degrading the overall quality of the media. Such tools exploit the predictability of traditional watermarking algorithms, making it easier to remove or forge watermark signals. Moreover, with the emergence of generative AI and deep learning techniques, malicious entities can now recreate content that mimics original media while eliminating embedded ownership markers. These evolving threats have rendered many traditional watermarking techniques inadequate for secure, high-stakes applications like digital rights management, forensics, or legal evidence validation.

[005] Simultaneously, the diversity of digital content formats and resolutions poses another challenge. A watermarking method that is effective for static images may not perform well on high-definition videos or audio streams due to differing compression standards and signal characteristics. Additionally, content shared across social media platforms is often automatically resized, cropped, or compressed, further complicating the watermark’s durability. There is a critical need for a universal, intelligent watermarking system capable of

adapting to a wide range of media formats and resistant to automated tampering mechanisms.

[006] Machine learning (ML) has shown significant promise in addressing complex pattern recognition and signal processing tasks. By leveraging its ability to learn from vast datasets, ML-based systems can be trained to understand optimal embedding points in media files, maintain perceptual invisibility, and resist adversarial alterations. Furthermore, deep learning architectures, such as convolutional neural networks (CNNs), generative adversarial networks (GANs), and autoencoders, can be used to embed, extract, and validate watermarks with far greater precision and resilience than traditional methods.

[007] However, despite the potential of ML in this domain, few watermarking solutions fully exploit the capabilities of modern AI techniques. Existing ML implementations often focus on only one aspect of the watermarking process—typically embedding or extraction—while ignoring holistic integration that includes tamper detection, adversarial resilience, and real-time verification. There remains a significant gap in the development of a complete, secure ML-based watermarking system that can dynamically adapt to new types of media and tampering strategies.

[008] In addition to robustness and adaptability, the need for automation is becoming increasingly important. Manual watermark embedding processes are inefficient and prone to human error. In fast-paced industries such as news media, entertainment, or online education, creators require automated tools that can embed, authenticate, and monitor watermarks at scale. Machine

learning enables such automation by dynamically learning watermarking strategies for different media types and adapting to changing content conditions in real time.

[009] Furthermore, a truly secure watermarking system must not only embed identifiers but also serve as a forensic tool capable of verifying content authenticity and detecting any signs of tampering or forgery. By integrating anomaly detection techniques and adversarial training methods, such a system could act as an intelligent watchdog—flagging modified content, isolating altered regions, and preserving the chain of custody for digital evidence. This is especially relevant in legal, journalistic, and governmental contexts where the integrity of digital media is critical.

[010] Accordingly, there is a compelling need for an intelligent, tamper-proof, and highly adaptive digital watermarking system that uses secure machine learning algorithms to protect multimedia content. The present invention addresses this need by offering a comprehensive, end-to-end watermarking solution capable of intelligent embedding, real-time extraction, tamper detection, and ownership verification across various types of media.

SUMMARY OF THE INVENTION

[011] The present invention introduces a novel system and method for tamper-proof protection of digital media through the application of secure machine learning-based digital watermarking. It leverages advanced machine learning algorithms to embed, extract, and validate watermarks in various types of multimedia content such as images, audio files, and videos. The system is

designed to address the shortcomings of traditional watermarking methods by offering an intelligent, adaptive, and resilient solution that maintains watermark integrity even under intentional or unintentional modifications of the media.

[012] At the core of the invention is a machine learning model trained to identify optimal embedding regions in digital content, ensuring that the watermark is imperceptibly hidden while maintaining its robustness against common alterations such as compression, resizing, cropping, and noise injection. The watermark is dynamically generated based on both the content features and ownership metadata, including user identity, timestamp, and cryptographic hashes, thereby providing traceability and secure authentication.

[013] The invention also incorporates a secure embedding module that uses frequency domain techniques—such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Singular Value Decomposition (SVD)—guided by the ML model to embed the watermark into perceptually insignificant regions. This ensures that the watermark remains invisible to human senses but recoverable by the system's decoding engine, even after various media transformations.

[014] A corresponding watermark extraction and verification module is responsible for detecting and validating the embedded watermark. This module utilizes an inverse ML model trained to decode watermarks from modified media files. The system compares the extracted watermark data against the original metadata to assess authenticity and identify any tampering attempts. In cases where tampering is detected, the system can pinpoint altered regions and generate a tamper map that visually highlights the inconsistencies.

[015] Additionally, the invention features a tamper detection engine that is trained using adversarial learning techniques. This component enhances the system's ability to detect advanced forms of media forgery, including AI-generated manipulations and deepfakes. The engine is capable of learning and evolving alongside emerging tampering strategies, ensuring that the system remains effective against future threats.

[016] The system is designed to be scalable, media-type agnostic, and capable of functioning in real-time applications. It can be deployed in a wide range of industries including digital media production, online content distribution, legal documentation, digital forensics, and copyright protection. The invention not only secures ownership rights but also ensures the integrity of digital content, making it an essential tool in today's increasingly digitized and manipulated media landscape.

[017] In summary, the invention offers a comprehensive, intelligent, and secure watermarking framework that outperforms traditional methods by integrating machine learning for dynamic watermark generation, robust embedding, and precise tamper detection. This results in a highly reliable solution for protecting and authenticating digital media assets across diverse platforms and applications.

BRIEF DESCRIPTION OF THE DRAWINGS

[018] The accompanying figures included herein, and which form parts of the present invention, illustrate embodiments of the present invention, and work

together with the present invention to illustrate the principles of the invention Figures:

[019] Figure 1, illustrates the system architecture of the tamper-proof media protection system using secure machine learning-based digital watermarking.

[020] Figure 2, illustrates the overall operational workflow of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[021] The present invention relates to a robust and secure system and method for protecting digital media content through a machine learning-based digital watermarking approach. This invention addresses the limitations of traditional watermarking systems, offering an intelligent solution capable of adapting to various types of media, preventing tampering, and ensuring content integrity through a machine learning-driven embedding and extraction process.

[022] System Architecture and Key Components

The system is composed of several key modules that work synergistically to provide secure watermark embedding, extraction, and tamper detection. These modules include the **Media Input Module**, **Feature Extraction Engine**, **Watermark Generation Unit**, **Machine Learning-Based Watermark Embedding Module**, **Watermark Extraction Engine**, **Tamper Detection Module**, and the **Authentication & Verification Unit**.

1. **Media Input Module**: The media input module is responsible for receiving and processing various types of multimedia content such as images, audio, and video files. The module ensures that the input

content is prepared for feature extraction by handling pre-processing tasks like resizing, normalization, or format conversion as required.

2. **Feature Extraction Engine**: The feature extraction engine analyzes the input media to extract relevant characteristics or features. These features may include color histograms, edge details, texture patterns, frequency-domain coefficients, or even higher-order representations such as deep learning embeddings. The extracted features serve as the foundation for embedding the watermark in the most perceptually invisible and robust regions of the media.
3. **Watermark Generation Unit**: This unit is responsible for generating the watermark itself. The watermark is typically created using a combination of user-specific metadata (such as ownership information, timestamps, or cryptographic hashes) and the extracted media features. The metadata is encoded into a unique watermark pattern, ensuring that the watermark is not only difficult to detect or remove but also personalized to each piece of media.
4. **Machine Learning-Based Watermark Embedding Module**: The heart of the invention lies in its machine learning-based watermark embedding module. This module uses advanced machine learning models—such as convolutional neural networks (CNNs), deep autoencoders, or generative adversarial networks (GANs)—to learn optimal embedding strategies for different media types. The model is trained to embed the watermark into perceptually insignificant regions of the media, ensuring that the watermark is invisible to human viewers but still recoverable through the system’s extraction engine. By considering the media's

content features, the model adjusts the watermark embedding process for each media instance, making it highly adaptive and resistant to common forms of media manipulation.

5. **Watermark Extraction Engine**: Once the watermark is embedded into the media, the watermark extraction engine is responsible for recovering the watermark during the verification process. The extraction engine uses the inverse of the embedding model, typically a machine learning-based decoder, to extract the watermark from the media. The system is designed to handle various types of alterations, such as compression, cropping, or noise, which may have been applied to the media after watermark embedding.
6. **Tamper Detection Module**: The tamper detection module is a crucial feature of the system. It uses advanced anomaly detection and adversarial learning techniques to detect any alterations or tampering in the media. By analyzing the difference between the extracted watermark and the original metadata, the system can flag any inconsistencies. If any tampering or forgery is detected, the system is capable of isolating the specific regions where alterations occurred, generating a tamper map that highlights these regions for forensic investigation.
7. **Authentication & Verification Unit**: This unit ensures that the extracted watermark is authentic and matches the original user metadata. It performs a comparison of the extracted watermark with the stored reference data to verify the ownership and integrity of the content. In case of discrepancies, such as the absence of a valid watermark or the detection of tampered media, the system flags the content as potentially

compromised. This is essential in applications like digital forensics, legal validation, and media content protection.

[023] Watermark Embedding Process

The watermark embedding process begins with the ingestion of digital content into the media input module. The content is then passed through the feature extraction engine, where key features are identified and extracted. These features may include color histograms, texture patterns, and edge information, which are then analyzed by the machine learning model to identify suitable regions for watermark embedding.

The watermark generation unit creates a digital watermark based on the content's features and embedded user-specific metadata, such as ownership details, timestamps, and cryptographic hashes. The machine learning-based watermark embedding module intelligently embeds the watermark into the media using the optimal points identified during training. This embedding is done in such a way that the watermark is imperceptible to human observers, maintaining the visual or auditory quality of the media while ensuring robustness against common modification techniques.

[024] Watermark Extraction and Verification Process

The watermark extraction process begins when the media content, potentially altered or modified, is input for verification. The watermark extraction engine applies the inverse of the embedding model to recover the watermark from the modified media. The extracted watermark is then compared to the stored reference metadata to verify its authenticity and detect any discrepancies.

The system also includes a tamper detection engine that performs a detailed analysis of the content. If the extracted watermark does not match the reference data, or if tampering is detected, the system flags the media as compromised. The tamper detection module can also highlight specific altered regions in the media, helping investigators identify the extent and nature of the tampering. This feature is particularly useful in digital forensics, where the integrity of media must be maintained for legal or investigative purposes.

[025] Tamper Detection and Adversarial Training

The tamper detection module is trained using adversarial machine learning techniques to identify new forms of media manipulation, including AI-based attacks like deepfakes or generative content. The system learns to differentiate between genuine media and altered versions by analyzing subtle changes in the watermark, its position, and the surrounding content. This adversarial approach allows the system to evolve with emerging threats, ensuring that it remains effective in protecting against sophisticated tampering methods.

[026] Applications of the Invention

The tamper-proof media protection system has broad applications across various industries, including digital media production, online content distribution, digital forensics, and intellectual property protection. In the media industry, it can be used to safeguard copyrighted content, ensuring that media files cannot be easily copied or modified without detection. In legal and forensic contexts, the system can validate the authenticity of digital evidence, ensuring that media submitted as evidence has not been altered. Additionally, it can be

employed in sectors such as healthcare, education, and government, where the integrity of digital documents and media is critical.

[027] Scalability and Real-Time Performance

The system is designed to be scalable and adaptable to different media formats, resolutions, and compression types. The machine learning models used in the system are trained on large datasets and can generalize to handle a wide variety of media content. Additionally, the system is optimized for real-time performance, allowing for fast embedding, extraction, and verification processes suitable for large-scale media distribution platforms or content management systems.

[028] In conclusion, the invention presents a groundbreaking solution for securing digital media through machine learning-based watermarking techniques that ensure robust protection against tampering and unauthorized use. By embedding imperceptible watermarks and incorporating advanced tamper detection and verification methods, this system offers a scalable, adaptive, and secure way to safeguard multimedia content across various industries. The integration of machine learning ensures that the system can intelligently adapt to different types of media and evolving tampering methods, providing a high level of protection for digital content. This technology is poised to transform the way digital media is managed, validated, and secured, offering valuable benefits in fields such as copyright protection, digital forensics, and media authenticity.

[029] Looking ahead, the future scope of this invention lies in its potential for further enhancement and adaptation to emerging technologies. With the continuous growth of artificial intelligence and deep learning techniques, the watermark embedding and extraction models can be refined to handle more complex media manipulations, including more advanced deepfakes and AI-generated content. The system could also be integrated with blockchain technology to create immutable records of digital media ownership and verification, adding another layer of security and transparency. Additionally, as virtual and augmented reality technologies advance, the invention could be adapted to protect immersive media content, ensuring that virtual environments, 3D models, and augmented visuals remain secure and traceable.

[030] The invention also holds promise for widespread adoption in various industries beyond media and entertainment, including healthcare, education, government, and law enforcement. Its ability to verify the authenticity and integrity of sensitive digital documents or multimedia evidence can be crucial in areas such as medical records, academic publications, legal proceedings, and government communications.

[031] In summary, this invention represents a significant leap forward in digital media protection, combining machine learning with traditional watermarking methods to create a dynamic, intelligent, and tamper-proof solution. With further advancements in AI and emerging technologies, the system's capabilities will continue to expand, offering even greater levels of security and authenticity for digital media in an increasingly interconnected world.

We Claim:

1. A system for protecting digital media content, comprising a media input module for receiving digital content, a feature extraction engine for extracting content features, and a watermark generation unit for generating a watermark using the extracted content features and user-specific metadata, wherein the watermark is embedded into the content using a machine learning-based watermark embedding module.
2. The system of claim 1, wherein the watermark embedding module utilizes a trained machine learning model to determine optimal regions within the media content for embedding the watermark, ensuring that the watermark remains imperceptible to human perception while maintaining robustness against alterations.
3. A method for embedding a tamper-proof watermark in digital media, comprising the steps of extracting features from the digital content, generating a watermark using the extracted features and metadata, and embedding the watermark into the media content using a machine learning-based model that adapts the embedding process to different types of media and modifications.
4. The method of claim 3, wherein the watermark embedding process involves using frequency domain techniques, including Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Singular Value Decomposition (SVD), to embed the watermark in perceptually insignificant regions of the media content.
5. A system for verifying the authenticity of digital media, comprising a watermark extraction engine that recovers the embedded watermark from the media, a tamper detection module that identifies any alterations in the media, and an

authentication unit that compares the extracted watermark with stored metadata to verify the integrity and ownership of the content.

6. The system of claim 5, wherein the tamper detection module uses adversarial machine learning techniques to detect advanced forms of tampering, including deepfakes and AI-generated content, by analyzing discrepancies in the watermark or media content.
7. A method for detecting tampering in digital media, comprising the steps of extracting the watermark from the media, comparing the extracted watermark with the original watermark metadata, and identifying regions of the media that have been modified by analyzing differences between the original and extracted watermark data.
8. The method of claim 7, wherein the tamper detection process includes generating a tamper map that visually highlights the altered regions of the media to aid forensic analysis and investigation.
9. A computer-readable medium storing machine-readable instructions that, when executed by a processor, cause the processor to implement the steps of extracting content features from a media file, generating a watermark based on the features and metadata, embedding the watermark using a machine learning model, extracting the watermark for verification, and detecting any tampering in the media.
10. The system of claim 1, wherein the watermark embedding, extraction, and tamper detection processes are optimized for real-time performance, allowing for rapid verification and validation of media content in large-scale content distribution platforms.

Dated this 14th day of April 2025

Signature: 

Applicant(s)

Mr. Merdul Sharma et. al.

ABSTRACT

TAMPER-PROOF MEDIA PROTECTION SYSTEM USING SECURE MACHINE LEARNING-BASED DIGITAL WATERMARKING

[032] The present invention relates to a secure, machine learning-based digital watermarking system and method designed to ensure tamper-proof protection of digital media content. The invention integrates intelligent watermark embedding, extraction, and tamper detection using adaptive machine learning algorithms, allowing imperceptible yet robust watermarking that resists a wide range of modifications, including compression, cropping, and malicious alterations. By leveraging feature-based learning models, the system dynamically identifies optimal embedding zones within the media and ensures accurate verification and authentication of ownership and integrity. This solution is applicable across various digital formats such as images, videos, and audio, offering a scalable, real-time, and highly secure mechanism for digital rights management, forensic tracking, and media authenticity verification.

Accompanied Drawing **[FIGS. 1-2]**

Dated this 14th day of April 2025

Signature: 

Applicant(s)

Mr. Merdul Sharma et. al.