Adaptive Methods for Embedding Digital Watermarks to Protect Audio and Video Images in Information and Communication Systems*

Pavlo Skladannyi[1,2,*,†], Yuliia Kostiuk[1,†], Svitlana Rzaieva[1,†], Bohdan Bebeshko[1,†] and Nataliia Korshun[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudryavska str., 04053 Kyiv, Ukraine*
[2] *Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, 42 Ac. Glushkov ave., 03680 Kyiv, Ukraine*

Abstract

This paper introduces an adaptive approach for embedding digital watermarks into image, audio, and video files to protect multimedia content within modern information and communication systems. The proposed method leverages the host signal's spectral, statistical, and perceptual properties to ensure high perceptual fidelity and robustness against various attacks, including compression, filtering, and geometric distortions. A mathematical model for the watermarking process, based on a secret key, has been developed; this model formalizes the procedures for watermark embedding and extraction while ensuring minimal perceptual distortion. The system architecture is implemented as a multi-agent framework incorporating cryptographic protection, open Application Programming Interfaces (APIs), and automated integrity verification modules. Comprehensive testing conducted on real-world multimedia data has confirmed the effectiveness of this approach. The proposed solution is suitable for application in various domains, including digital forensics, copyright protection systems, streaming platforms, and digital archiving.

Keywords

adaptive embedding, digital watermarks, multimedia content protection, perceptual transparency, data integrity, steganography, digital identification, digital forensics, information and communication systems

1. Introduction

The rapid proliferation of digital multimedia content within information and communication systems has intensified the need for robust methods to protect such data from counterfeiting, unauthorized distribution, and loss of authenticity. This challenge is particularly acute for video and audio content transmitted over open communication channels or stored in cloud environments. To address these issues, digital watermarking (DWM) technologies have become a key solution, providing mechanisms for digital identification, authorship verification, data integrity control, and the tracking of content distribution sources.

Digital watermarks are imperceptible or minimally perceptible data structures embedded within a media object that convey auxiliary information—identifiers, hash values, or digital certificates—without degrading the user's perceptual experience. In contrast to conventional watermarking schemes, which rely on static rules and predetermined parameters, adaptive methods dynamically configure the embedding algorithm based on a local analysis of a specific segment's properties within the media file. This approach enables the dynamic adjustment of watermark parameters, such as embedding depth, spectral characteristics, spatial position, and intensity, in response to the signal's energy spectrum, local image contrast, and models of human perception.

* *CQPC 2025: Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine*
* Corresponding author.
† These authors contributed equally.
p.skladannyi@kubg.edu.ua (P. Skladannyi); y.kostiuk@kubg.edu.ua (Y. Kostiuk); s.rzaieva@kubg.edu.ua (S. Rzaieva); b.bebeshko@kubg.edu.ua (B. Bebeshko); n.korshun@kubg.edu.ua (N. Korshun)
0000-0002-7775-6039 (P. Skladannyi); 0000-0001-5423-0985 (Y. Kostiuk); 0000-0002-7589-2045 (S. Rzaieva); 0000-0001-6599-0808 (B. Bebeshko); 0000-0003-2908-970X (N. Korshun)

Therefore, adaptive digital watermarking algorithms provide high imperceptibility (imperceptible to human sight or hearing) and robustness to a wide range of attacks and transformations, including JPEG and MP3 compression, filtering, cropping, scaling, and re-encoding, while ensuring minimal degradation of the original signal quality. Furthermore, there is a pressing need to counteract emerging forms of content manipulation, particularly deepfake technologies, neural reconstruction, and other generative models to create synthetic audio and video materials. Such fabricated content can be deployed for phishing, cyber blackmail, disinformation campaigns, or evidence tampering in digital forensics.

This study aims to develop and implement an adaptive method for embedding digital watermarks designed to protect audio and video content within information and communication systems. The proposed approach leverages spectral and perceptual analysis, in addition to statistical and neural network models, to optimize embedding parameters according to the specific characteristics of each media object (e.g., image, sound, video) [1]. This methodology results in an increased resilience of the watermark to attacks, improved accuracy of its detection and identification, and the preservation of the visual and acoustic quality of the digital content [2, 3].

This study also formalizes the architecture of an adaptive software framework that comprises modules for preprocessing, watermark embedding, detection, quality assessment, and integration with information and communication protocols. The architecture is founded upon the principles of modularity, scalability, and compatibility with common multimedia standards (e.g., H.264, AAC, JPEG2000), enabling the implementation of the proposed algorithms in on-premises environments and in cloud infrastructure or real-time streaming systems.

Consequently, the developed adaptive digital watermarking methods provide an effective solution for protecting multimedia content from unauthorized use, distortion, and loss of authenticity, while preserving high perceptual quality and ensuring suitability for integrating modern information and communication technologies.

2. Literature review

Modern research in digital watermarking increasingly incorporates adaptive and neural network-based methods to enhance robustness against attacks while preserving the quality of multimedia content. For instance, Taha, Ngadiran, and Ehkan [4] proposed an adaptive image watermarking algorithm that utilizes an efficient perceptual map to model the human visual system's sensitivity to luminance changes. This algorithm exhibits high resistance to JPEG compression and geometric transformations, making it an effective solution for protecting visual content within information and communication systems.

Quan et al. [5] focused on embedding digital watermarks directly into the parameters of deep neural networks (DNNs) used for image processing. The authors demonstrated that DNNs can be protected from unauthorized use by embedding specially encoded watermarks into the model's parameters, which provides a mechanism for both model identification and proof of ownership.

Li and Yue [6] conducted a security analysis of a dual watermarking structure for multimedia data and proposed enhancements to the framework to protect privacy and authenticity. Their work highlights the effectiveness of combining visible and invisible watermarks to create multi-level protection systems for applications in digital archives and streaming services.

Chen et al. [7] proposed an adaptive watermarking method based on wavelet entropy optimization in the audio domain. Their approach considers the entropy characteristics of the signal across different scales, which allows for the dynamic identification of optimal embedding regions while minimizing the impact on perceptual audio quality.

Naseem et al. [8] integrated fuzzy logic into the watermark embedding process, proposing an intelligent decision-making model to optimize the placement of watermarks within images. Their method enhances information security by adapting to local content characteristics and considering the probability of potential attacks.

This research confirms that the most effective multimedia information protection systems are based on integrating adaptive strategies, statistical signal analysis, and artificial intelligence. This synergy ensures high robustness, transparency, and authenticity for digital watermarks within the evolving digital information environment.

3. Methods and models

This study integrates theoretical and applied methodologies, encompassing mathematical modeling, information security principles, and digital signal processing. The attack model incorporated a comprehensive set of transformations based on the discrete cosine transform (DCT) and the Fast Fourier Transform (FFT), geometric distortions such as scaling and rotation, StirMark-type benchmark attacks, and neural network-based reconstructions.

The adaptive embedding algorithm leverages the entropy characteristics, frequency-domain power, and texture features of the multimedia signal, which are extracted using techniques such as Gabor filters and wavelet analysis. Embedding regions are determined based on perceptual visibility models and weight functions derived from a trained convolutional neural network (CNN).

A Monte Carlo simulation with 1000 independent iterations was conducted to validate the method's effectiveness. Each iteration involved the random selection of a multimedia container (in JPEG or WAV format), the generation of a unique embedding configuration, the determination of a random embedding location, a variable embedding density (from 1 to 6), and a specific attack scenario. The digital watermark was embedded and subsequently extracted in each iteration, and the results were evaluated.

Performance was assessed using a suite of quality metrics: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Quality Index (Q-index), Bit Error Rate (BER), Normalized Cross-Correlation (NCC), and Learned Perceptual Image Patch Similarity (LPIPS). A successful extraction was defined as an iteration in which the recovery accuracy, τ, met or exceeded a threshold of 0.98.

4. Main material

Modern security tools and methods for ensuring the integrity of multimedia information are rapidly evolving in response to the escalating threats of unauthorized access, content modification, and copyright infringement within digital communication channels. A significant limitation of many existing solutions is their reliance on static architectures with fixed processing algorithms, which fail to account for the dynamic nature of the transmission environment or the specific content characteristics.

A comprehensive system for controlling the integrity of multimedia objects is typically implemented as a software-hardware architecture comprising several key functional modules. These include: an integrity verification module for authenticating digital signatures, calculating hash functions, and verifying embedded watermarks [6]; a watermark management module capable of adapting to the properties of the multimedia container and prevailing threats [8]; a secure storage module for managing metadata, cryptographic keys, version history, and access rights [9]; and a logging subsystem that records all system events in a secure, auditable format for subsequent analysis [4, 5, 10–12]. Interaction among these components is coordinated via a management interface or a multi-agent environment that facilitates integration with external security platforms, such as Security Information and Event Management (SIEM) systems, Digital Rights Management (DRM) frameworks, and blockchain-based storage solutions like Non-Fungible Tokens (NFTs).

Fig. 1 presents a contextual and structural Data Flow Diagram (DFD) model of an adaptive digital watermarking system designed to protect image, audio, and video content within information and communication systems. The architecture comprises five key functional subsystems: a control interface and API, a content analysis module, an adaptive embedding module, a verification module, and a secure repository for service data and logs [13]. The processing

workflow is initiated when user requests are received by a session manager, where they undergo initial validation. Subsequently, the data is forwarded to the content analysis module, which assesses the multimedia object's entropy, frequency-domain, and perceptual characteristics. Based on these parameters, the embedding module generates a digital watermark and adaptively inserts it into optimal container regions [4, 5, 7, 14]. The corresponding watermark metadata is stored in the secure repository, and all operational events are systematically logged.

To verify content integrity or authenticity, a user can initiate the verification process, during which the system extracts the embedded watermark, compares it against the reference value, and generates a corresponding response [15]. Within the diagram, data flows are denoted by symbolic labels (e.g., DataX, LogX, ResponseX), and the functional modules are visually demarcated by color-coded zones for enhanced clarity [16, 17]. The proposed architecture integrates adaptability, modularity, and a high level of information security, which are critical for operation within a dynamic digital environment.

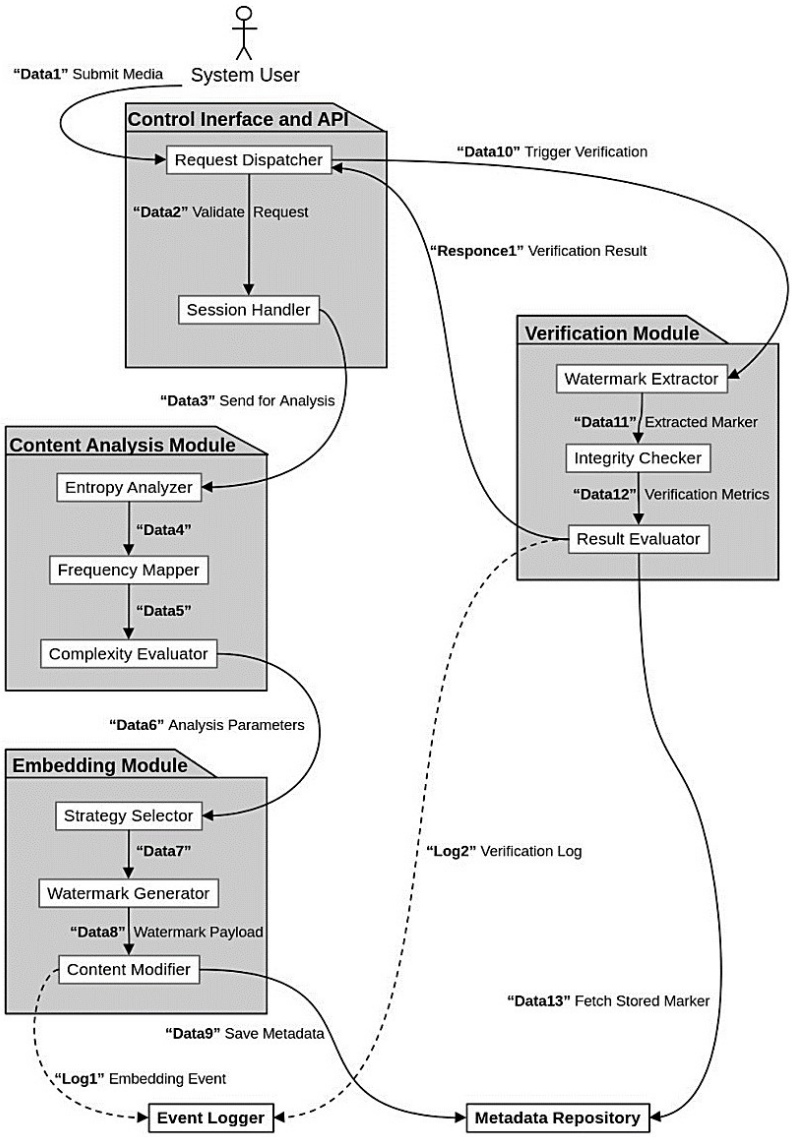

Figure 1: DFD model of an adaptive digital watermarking system for multimedia information.

The application of adaptive digital watermarking methods, which leverage perceptual analysis [3], wavelet transforms [7], artificial neural networks—specifically Convolutional Neural Networks (CNNs) [5] and Long Short-Term Memory (LSTM) networks—and fuzzy logic [8], facilitates the implementation of a context-aware, scalable, and flexible system for protecting multimedia information. The proposed model is highly effective in domains such as digital broadcasting [18],

video streaming, digital forensics, digital archiving, and the protection of digital art. In contrast to traditional centralized solutions, this system establishes a distributed, adaptive architecture where watermarking, identification, authentication, and integrity control are cohesively integrated into a singular digital information security ecosystem.

The escalating cybersecurity threats [19] to multimedia information necessitate a comprehensive risk analysis of unauthorized access, distortion, forgery, and illicit audio, video, and graphic content copying. This study presents a systematic classification of threats into primary categories and proposes a feature-based model [6] that enables the analysis of potential attacks without a complete formal description. This approach accounts for environmental dynamics, the variability of attack vectors, and the complexities of identifying threats within open information and communication systems.

Fig. 2 presents a generalized scheme of classification features for multimedia threats, illustrating a hierarchical structure of risks that affect multimedia information security within information and communication systems. The threats are categorized into four primary groups: by context of occurrence (e.g., intentional attacks, unintentional distortions), by channel of influence (e.g., network interference, hardware failures), by attack vector (e.g., content modification, extraction of hidden information, insertion of malicious watermarks), and by enabling technology (e.g., compression artifacts, AI-based reconstruction, format conversion). This classification framework enables a systematic analysis of the risks associated with multimedia processing and transmission. It facilitates the development of adaptive digital watermarking strategies capable of effectively countering a wide range of attacks in the contemporary digital environment.

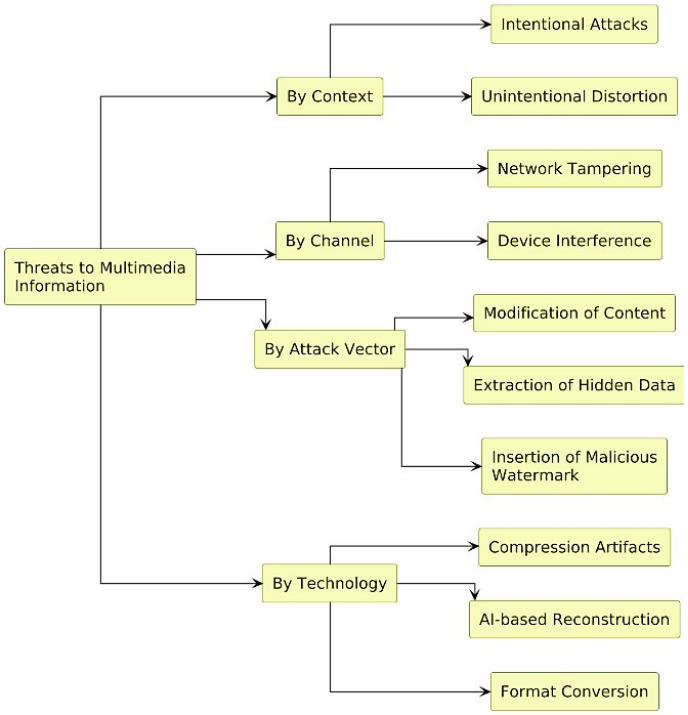

Figure 2: Structure of classification features of threats affecting the security of multimedia information in information and communication systems.

A formalized steganography model is defined as a set of two basic functions—embedding and extraction:

1. $F : M \cdot B \cdot K \longrightarrow B'$ is an embedding function that correlates a message $m \in M$, an empty container $b \in B$, and a secret key $k \in K$ with a modified container $b' \in B'$.
2. $F' : B' \cdot K \longrightarrow M$ is an extraction function that, given the modified container b' and key k recovers the original message m.

Thus, an adaptive steganographic system is defined as the five F, F', M, B, K, where M is a set of messages, B is a set of containers, K is a set of keys, F and F' are embedding and extraction algorithms, respectively. This allows us to formally describe the stage for generating a protected media object and the procedure for verifying integrity or authenticity. This approach ensures generalization of processes at the model level, which is necessary for building universal software solutions. In addition, the system structure allows you to set adaptation parameters depending on the type of content and threats. The formalization based on sets and functions also facilitates integration with cryptographic protocols and access control mechanisms.

A comparative analysis of patented and published solutions in digital watermarking has revealed several systemic limitations of traditional methods that restrict their practical application. Key disadvantages include the introduction of significant visual or acoustic distortions, the presence of detectable embedding artifacts vulnerable to steganalysis, the potential for extracting hidden data without key knowledge if the modified container is compromised, and a lack of robustness against watermark substitution or distortion resulting from minor edits to the multimedia file.

In contrast, modern adaptive embedding methods which leverage perceptual modeling [4], wavelet analysis [7], deep neural networks (CNNs, LSTMs) [5], and fuzzy logic [8] provide minimal distortion, a high degree of imperceptibility, resilience to modification attempts, and the ability to adapt based on the container's intrinsic characteristics contextually. This paves the way for developing reliable, invisible, and dynamically controlled digital watermarking systems suitable for deployment in open networks, streaming services, blockchain-based authentication, and digital forensics. The adaptability of such systems allows for the automatic adjustment of embedding parameters to suit different content types without compromising quality. Furthermore, using neural network models enables the system to learn from real-world data and incorporate complex perceptual features of signal processing, significantly increasing the watermark's reliability and expanding its scope of application within information and communication environments.

Effective digital multimedia watermarking systems must account for a wide range of potential attacks targeting both the steganographic methods and the embedded watermarks. Threats from passive (e.g., observation, steganalysis) and active (e.g., modification, deletion, substitution) adversaries operating within a dynamic digital environment pose significant challenges.

Fig. 3 illustrates the structural architecture of an adaptive digital watermark embedding system designed to protect image, audio, and video content within information and communication systems. The diagram outlines the primary stages of the watermarking lifecycle: message encryption using the Advanced Encryption Standard (AES) symmetric block cipher; integrity tag generation via a Hash-based Message Authentication Code (HMAC); adaptive embedding into the multimedia container; transmission over a channel susceptible to potential threats; and subsequent extraction, verification, and decryption on the recipient's side. The architecture also accommodates the integration of auxiliary components, including a Digital Rights Management (DRM) module, a Security Information and Event Management (SIEM) system, and an event logging subsystem. All data flows within the system are labeled with unique identifiers (e.g., Data1-Data11, Log1-Log4, Auth1) to provide clear visibility into the interaction logic and enhance the transparency of information process control. This comprehensive architecture ensures robust protection, scalability, and ease of integration into modern digital environments.

Assessing the resilience of such systems necessitates a comprehensive approach. This study employs attack models based on extended threat matrices, encompassing various types of interference, modification intensities, and access to keys and data [4, 5]. Evaluation methodologies include classical metrics such as BER, NCC, and PSNR, modern metrics derived from perceptual responses, receiver operating characteristic (ROC) curves, and simulation testing using adversarial attacks generated by neural networks. Additionally, scenarios of subtle influence are considered, where modifications do not directly lose the watermark but gradually degrade its detectability under challenging conditions.

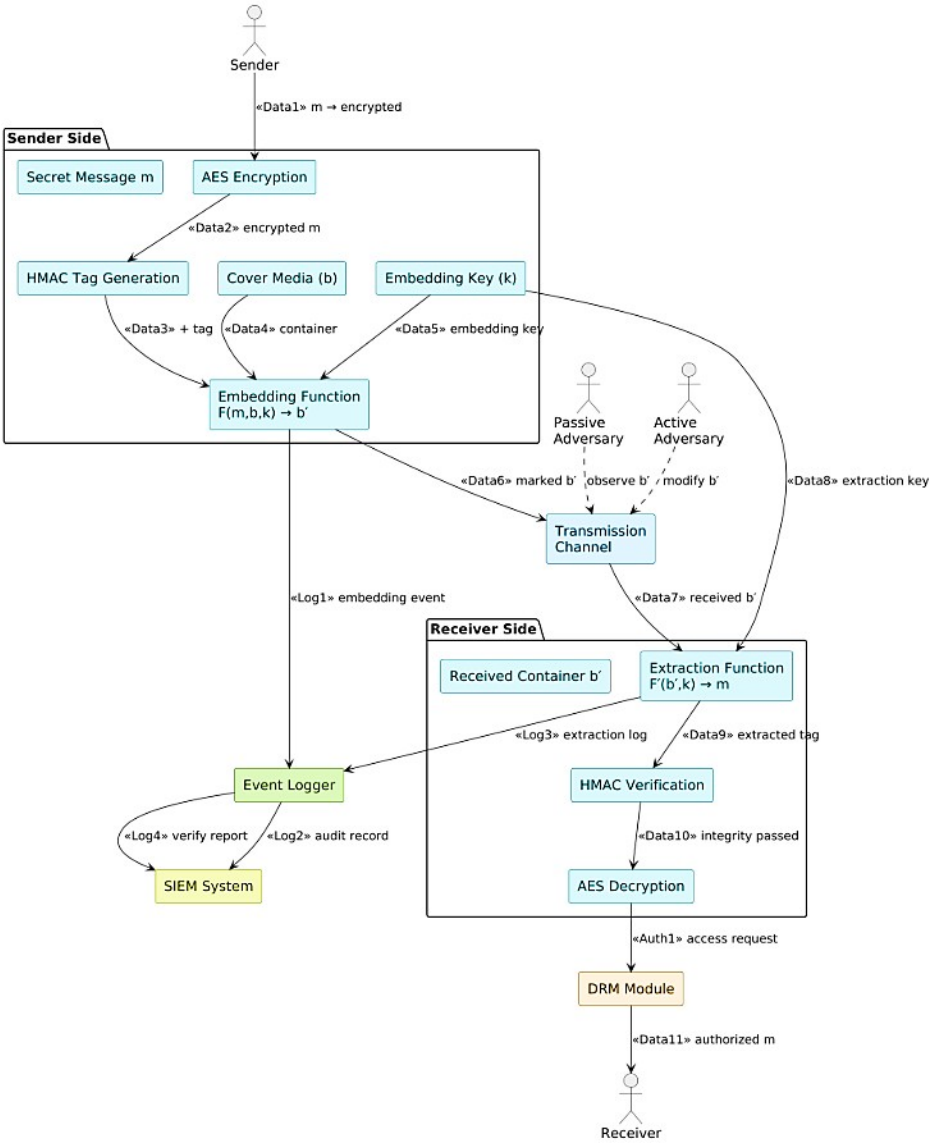

Figure 3: Architecture of an adaptive steganographic system with cryptographic protection and data flow monitoring.

Such comprehensive testing allows evaluating the system's limit states, watermark recovery capabilities, and false favorable rates. This holistic assessment covers functional stability indicators and the system's adaptive capacity for learning and self-correction in a real-world environment.

An analysis of modern cryptographic transformations used in multimedia information protection reveals several key disadvantages of classical systems. These include a lack of adaptation to content type, low resistance to perceptual attacks, the potential for reverse-engineering the watermark if the container is compromised, and a lack of flexible control over the watermark's behavior during dynamic data distribution in open networks. This research focuses on the integration of symmetric ciphers (e.g., AES, ChaCha20), keyless hash functions (e.g., SHA-3, BLAKE3), and key-dependent authentication functions (e.g., HMAC, KMAC) as mechanisms for verifying integrity, identification, and authenticity within the watermark's structure [6]. Accordingly, the primary objective of this study is to develop an adaptive digital watermarking architecture that provides a high level of imperceptibility, cryptographic security, scalability, and robust detection capabilities within a dynamic environment. Sub-objectives include constructing attack models, defining perceptual criteria for adaptation, developing embedding and extraction functions, and designing a software implementation that supports open APIs and intelligent logging.

As a result of this research, mathematical models and adaptive methods for monitoring the integrity of multimedia information, based on the covert embedding and extraction of digital watermarks, have been developed [7]. The core element of this framework is a model of the multimedia container's "naturalness," which provides a statistical assessment of changes introduced by the embedded watermark. This model accounts for both the media file type (image, audio, or video) and the specifics of its storage format, thereby enabling increased accuracy in detecting unauthorized modifications without significantly impacting the perceptual quality of the content.

A key feature of the model is the concept of hiding space, a linearized sequence of elements of a multimedia container suitable for marking, determined based on the signal's type, format, and perceptual significance [8]. For each container, the hiding space is analyzed and described by a parametric naturalness vector:

$$\vec{f} = \left(f_0, f_1, \ldots, f_n \right), n \in N, \tag{1}$$

where each parameter belongs to one of three groups.

Statistical analysis of paired elements of the hiding space—evaluates the distribution of differences between the high and low bits of the elements:

$$P_{ij} = P\left(s_i^H - s_i^L \right), \tag{2}$$

where $(s_i^H - s_i^L)$ are the high and low bits of the elements, respectively.

Frequency analysis of bit series—determines the probability of occurrence of a bit series of length l in the hiding space:

$$P\left(l_i \right) = \frac{n_i}{\sum n}, l_i \in \{1,2,\ldots,2^k\}. \tag{3}$$

Analysis of the lengths of identical bit sequences—the probability of a series with identical bits:

$$P\left(k_i \right) = \frac{m_i}{\sum m}, \tag{4}$$

where m_i is the number of series of length i.

Based on this model, adaptive methods for embedding and extracting digital watermarks have been developed that depend on the secret key $k \in K$, which uniquely determines how the mark is placed in the hiding space. The embedded bits are distributed according to the patterns generated from the key sequence, ensuring uniformity and attack resistance. This approach makes it impossible to reproduce or modify the mark without knowing the key and minimizes the likelihood of an attacker localizing the marking structure. In addition, the dependence of the embedding positions on the key ensures cryptographic reliability and makes it easy to scale the system to fit different container sizes. In the event of an attempt to remove or edit the watermark, the system reacts with a loss of correctness during authentication, which allows you to identify the fact of interference quickly.

The function describes the direct adaptive steganographic transformation:

$$F : M \cdot B \cdot K \longrightarrow B', b_i^{'} = \{ m_i, \text{if } k_{i-1} = \text{sh } b_i, \text{otherwise}, \tag{5}$$

where F is an adaptive embedding function that may depend on spectral (DCT), wave (DWT), or spatial (LSB) criteria, M is a set of messages to be embedded, B is a set of containers, K is a set of

keys, b_i is the element of the original container's hiding space, $b_i^{'}$ are elements of the modified container, m_i are bits of the embedded message, k_i are blocks of the key sequence generated from the secret key, sh mask template that defines the places for embedding. Thus, the adaptive steganographic system dynamically generates the space for embedding based on statistical and structural features of the signal, while ensuring a high level of transparency, integrity, and cryptographic strength when transmitting multimedia data in open networks.

Fig. 4 shows a spatial vertical model of the embedding F and extraction F', functions that implement adaptive digital watermarking in multimedia containers. Visually, the diagram is divided into three zones: input data (left), processing logic (center), and results (right). In the process of embedding, a message m is hidden in the elements of a container b_i using a key sequence k_i according to a template rule. The extraction of information follows a similar pattern, with the message being recovered from the modified container $b_i^{'}$. Data and key flows are defined and labeled for all stages, which ensures a transparent formalization of the process and increases the system's reproducibility.

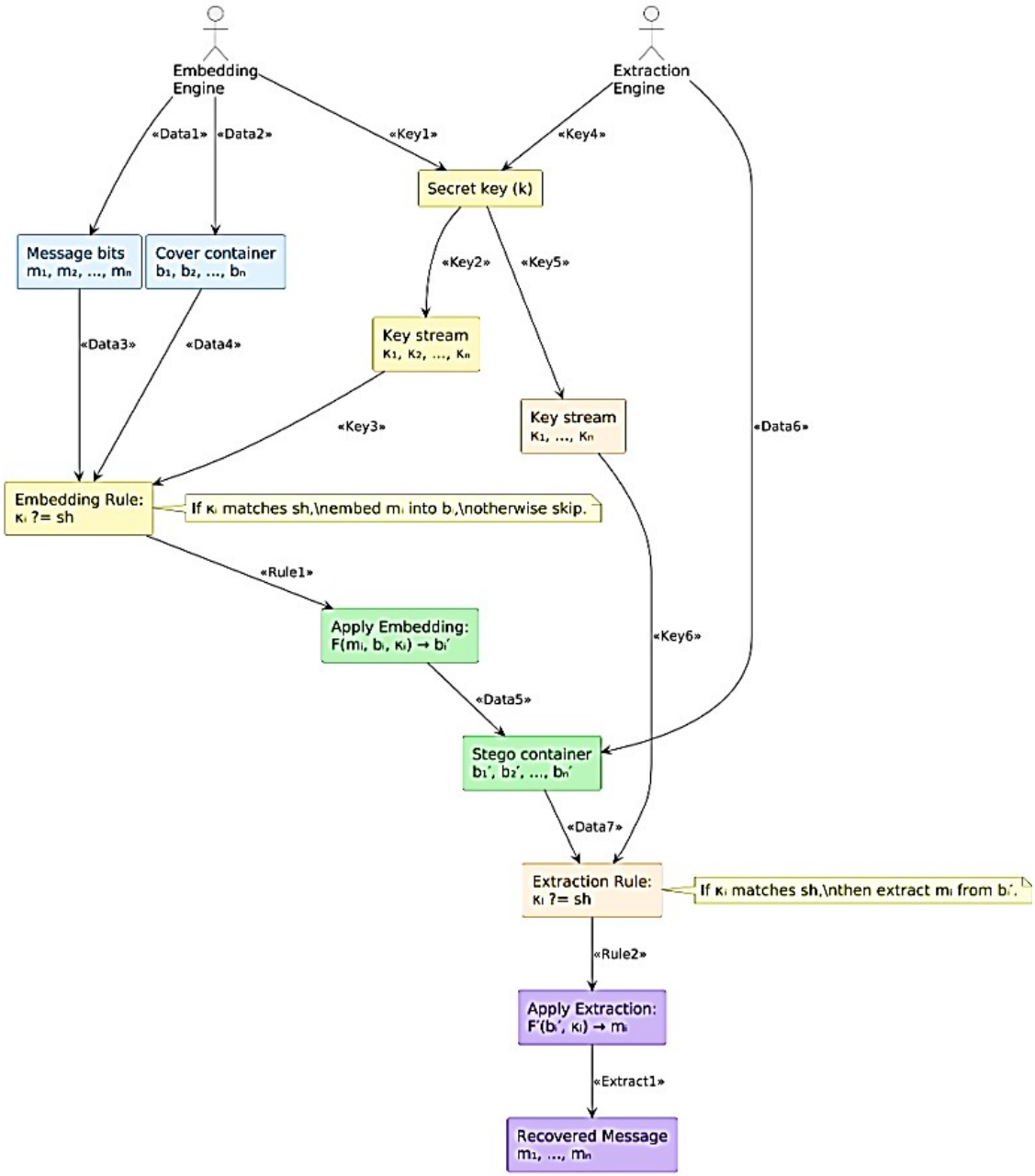

Figure 4: Model of functions F and F' of the adaptive digital watermarking system.

Fig. 5 presents a sequence diagram detailing the process of adaptively embedding a digital watermark into a multimedia container. The user initiates the procedure, after which the system loads the host container and the message to be embedded. A cryptographic key stream is then generated to determine potential embedding locations. A condition based on a predefined template is evaluated for each possible location. If this condition is satisfied, the corresponding message bit is embedded at that position within the container; otherwise, the area is left unmodified. A secure, watermarked container is produced upon completion of this iterative process and is ready for subsequent transmission or storage. The diagram illustrates the sequential interaction of the system's modules—including the key generator, template filter, embedding module, and container manager—which collectively implement the conditional logic of this adaptive watermarking scheme. This approach provides not only configurational flexibility but also enhanced resistance to detection due to the unpredictability of the embedding positions.

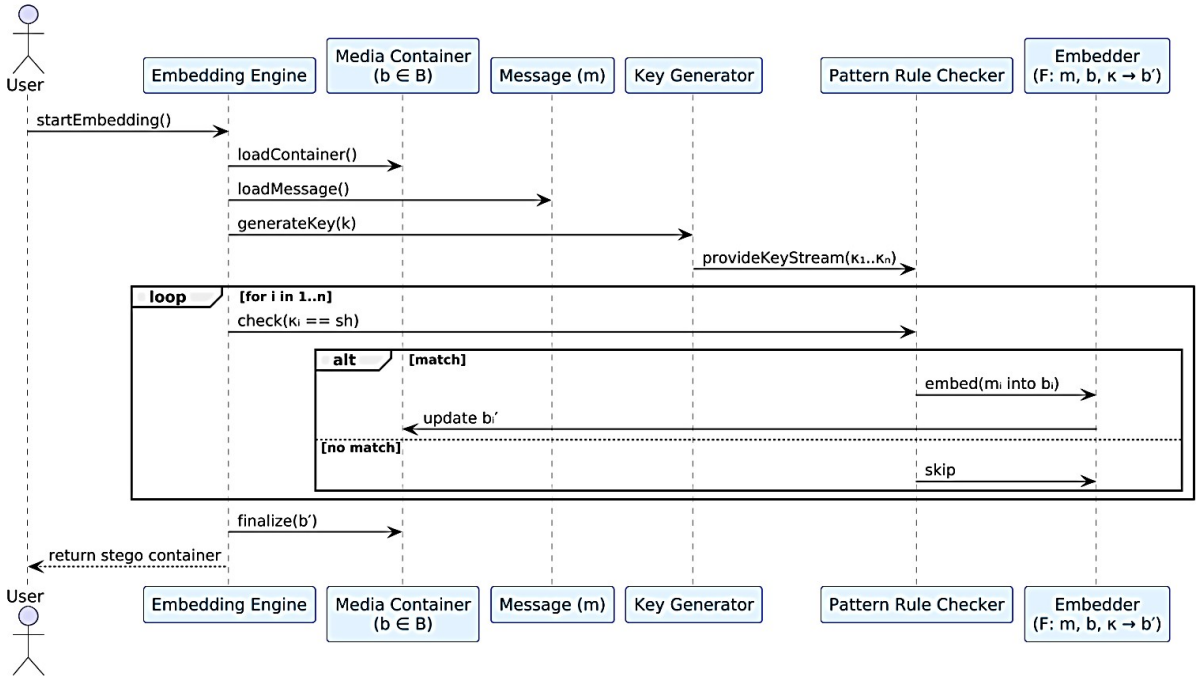

Figure 5: Diagram of the sequence of stages of embedding a digital watermark.

Integrity control is realized through adaptive embedding of digital watermarks, which allows you to verify the authenticity of a multimedia container without the need to store separate control hashes or reference copies. The method uses cryptographic hash functions that provide data verification in the presence of only a modified container and a secret key [8, 13]. This approach significantly reduces computational and resource costs, simplifies the integrity control procedure, and increases the system's adaptability to the dynamic conditions of the digital environment.

Solving the problem of building a model for assessing the distortions introduced during the embedding of a digital watermark and methods for their quantitative analysis is the content of a separate research stage. The quality of a multimedia container is assessed using the distance metric between the original (unmodified) container I and the modified (embedded) container O, which is formalized as [4, 20]:

$$q = K(I, O), \tag{6}$$

where K is the generalized similarity metric function (e.g., SSIM, PSNR, VMAF, NCC, etc.).

The proposed quality model is presented as a set of indicators:

$$S = \{ f_i(I, O) \vee i = 1, \ldots, n \}, \tag{7}$$

where n is the model dimension, f_i is the corresponding quality metric. For a specific type and format of a multimedia container (image, audio, video), the optimal subset of relevant criteria is selected:

$$\Theta = \{ f_i(I, O) \vee I, O \in B \}, \tag{8}$$

where B is a set of valid multimedia data formats.

To ensure cryptographic security, a key function is used G [6, 13]:

$$K \longrightarrow k = \{ k_1, k_2, \ldots, k_n \}, \tag{9}$$

$$k_i = HMA\, C_K \left(i \| t \| UID \right), i \in N, t = \text{timestamp}, UID = \text{user\_id} \}. \tag{10}$$

To guarantee confidentiality, the message m is encrypted before embedding using AES:

$$c = AES_k(m), c \longrightarrow \text{is embedded instead of } m. \tag{11}$$

The pull function $F' : B' \cdot K \longrightarrow M$ is defined as:

$$m_i = \{ F(b_i')', \text{if } k_{i-1} = sh \perp, \text{otherwise}, \tag{12}$$

where $\perp$ is a marker indicating the absence of an embedded bit in this element.

Verification is performed using the integrity function:

$$\text{Valid} = \{ true', \text{if } HMAC_K(c) = \text{stored\_tag false, otherwis} \tag{13}$$

A composition of functions can describe the complete adaptive labeling process:

$$W(M, B, K, sh) = \{ b_1', \ldots, b_n' \}, \tag{14}$$

$$b_i' = F(\text{Enc}(m_i), b_i, k_i), \tag{15}$$

where Enc is a function of message encryption before embedding.

After extracting the recovered message:

$$m_i = \text{Dec}(F'(b_i')), \tag{16}$$

where Dec is an AES decryption.

Reverse quality and compliance checks can be performed:

$$\text{Match}(m, \hat{m}) = \sum_{i=1}^{n} \delta(m_i = \hat{m}_i) / n \geq \tau, \tag{17}$$

where τ is a threshold value of recovery accuracy (for example, 0.99).

The proposed formalized approach provides a transparent mathematical model for operating an adaptive digital watermarking system. It demonstrates its practical suitability for deployment in dynamic information and communication systems [5, 18, 21]. Key application scenarios include video streaming platforms, digital archives, and distributed authentication infrastructures. A quantitative quality assessment model is essential for generating a comprehensive numerical characterization of the embedding's impact, which enables an objective determination of the degree of degradation in the perceptual quality of the content and provides a feedback mechanism for controlling the effectiveness of the adaptive watermarking process.

An architecture for an adaptive software framework for maintaining the integrity of multimedia information has been developed, founded upon a digital watermarking model [9, 10, 22–24]. This architecture employs software agents to implement the embedding of digital watermarks and to perform integrity verification, particularly in environments with an elevated risk of unauthorized modifications, copying, or loss of content authenticity. The framework's functional architecture is based on the interaction of six specialized agents, each performing a distinct role in protecting multimedia information [11, 25]. The Control and Management Agent coordinates the overall system operation, configures parameters, and monitors subsystem status. The Information Storage Agent provides secure storage for multimedia objects along with control signatures and metadata. Communication, request routing, and centralized processing logic are implemented by the Control Agent. The Registration Agent is responsible for registering new objects and embedding them with watermarks and integrity codes, while the Cloning Agent creates uniquely identified copies to track their distribution. The Integrity Analysis and Control Agent completes the architecture, which audits containers in both internal storage and external environments by comparing extracted watermarks with reference values to verify authenticity.

Each agent is constructed using a modular architecture, comprising a main software module and a set of functional components with a clear distinction between mandatory modules (required for basic operation) and optional modules (which can be connected based on media type, security policy, or user requirements) [10, 17, 24, 26]. This design ensures the framework's flexibility, scalability, and adaptability. Fig. 6 illustrates this component architecture, showing the six functional agents distributed across logically isolated zones. Color zoning is used within the diagram to visually demarcate each module's functional roles.

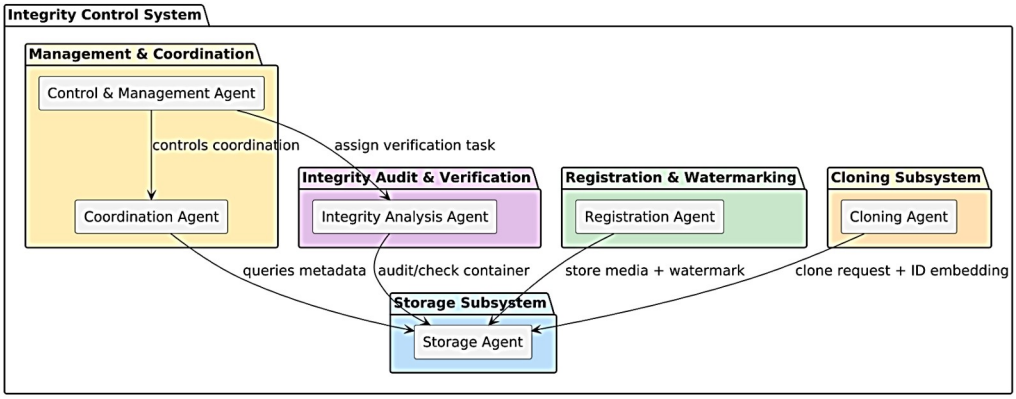

Figure 6: Agent-oriented architecture of the adaptive embedding system for digital watermarks.

A software framework has been developed to ensure the integrity of multimedia information using adaptive digital watermarking, with a focus on modern graphic (JPEG, PNG), audio (WAV, MP3), and video (MP4, MKV) formats [13, 17, 18, 25, 26]. The architecture of this framework is implemented using a modular approach and contemporary development tools, including Microsoft Visual Studio Code, the C++17/20 and Python programming languages, and the OpenCV, FFmpeg, and TensorFlow libraries [22, 23]. Scalability and flexibility are achieved through a containerized architecture based on Docker with support for open REST APIs.

Structurally, the framework is composed of four primary agents. A management and monitoring agent coordinates inter-component interaction, configures security settings, and maintains event logs supporting SIEM/SOAR systems [9, 11, 14]. The storage agent provides secure storage for media containers using platforms such as Amazon S3 or MinIO and performs integrity checks based on checksums [21]. A multimedia registration agent conducts the initial embedding of the digital watermark, accounting for the container's statistical characteristics, and generates control hash codes [14, 25–27]. Finally, an integrity control agent performs regular audits of content changes by comparing stored checksums with current ones using HMAC and SHA-256 algorithms [13, 27] and anomaly detection tools.

A suite delivers the system's functionality through specialized modules. A cryptographic protection module (crypto_module) implements adaptive encryption based on AES-256 and HMAC-SHA256, while a watermark insertion/extraction module (adaptive_stego) provides adaptive embedding using DCT, FFT, and LSB methods [24]. A container naturalness evaluation module (perceptual_model) analyzes perceptual quality using SSIM, PSNR, and the modern LPIPS metric, while a distortion evaluation module (distortion_eval) determines acceptable modification levels that do not compromise quality [14, 16, 20]. A key sequence generation module (keygen) produces cryptographically secure keys based on user identifiers, timestamps, and random variables. The entire system is engineered to ensure high stability, reliability, and adaptability for security measures in digital information and communication systems.

To evaluate the effectiveness of the developed method, a test sample was formed, comprising 1,000 JPEG images and 1,000 WAV audio files [7, 17]. Adaptive embedding of digital watermarks was performed with a variable insertion density ranging from 1 to 6 bits per block. The experimental results demonstrated that at an insertion density exceeding 4 bits per block, high perceptual quality is maintained, with the Structural Similarity Index Measure (SSIM) surpassing 0.98 and the Perceptual Evaluation of Speech Quality (PESQ) exceeding 4.1 [25]. These findings indicate that the embedded watermark has a minimal impact on the naturalness of the multimedia content.

Table 1
Dependence of multimedia naturalness on the density of digital watermark insertion

Insert density	Average SSIM	Violation of naturalness
2	0.995	none
4	0.986	none
6	0.958	insignificant

The results of the experimental study confirm that the proposed method demonstrates high efficacy with minimal impact on the perceptual quality of the multimedia content. This conclusion is supported by stable values for the Structural Similarity Index Measure (SSIM) and Perceptual Evaluation of Speech Quality (PESQ) metrics [20]. The adaptive approach facilitates an optimal balance between watermark robustness against modifications and preserving the perceptual quality of images, audio, and video [13, 18]. Consequently, the proposed methods provide reliable protection for multimedia content within digital information and communication systems without significantly degrading visual or auditory quality.

Fig. 6 presents a Data Flow Diagram (DFD) of the adaptive multimedia integrity control software framework, which is architected around the interaction of four specialized agents: a control and monitoring agent, a storage agent, a multimedia registration agent, and an integrity verification agent. The user initiates the configuration process via the control agent, which orchestrates the interaction among all other system components [10]. The registration agent is responsible for embedding a digital watermark using adaptive methods, including the discrete cosine transform (DCT), the fast Fourier transform (FFT), and the least significant bit (LSB) technique [14, 16]. The resulting control hash codes are transmitted to the storage agent, which records them in a secure file environment, such as Amazon S3 or MinIO [13]. The integrity verification agent conducts periodic audits of multimedia objects, employing HMAC-SHA256 cryptographic algorithms and artificial intelligence models to detect anomalies [18]. The results of these verifications are returned to the central management agent for analysis and subsequent action. The system's modular structure ensures flexibility, scalability, and automated quality control, enabling it to adapt to various multimedia data formats within information and communication systems.

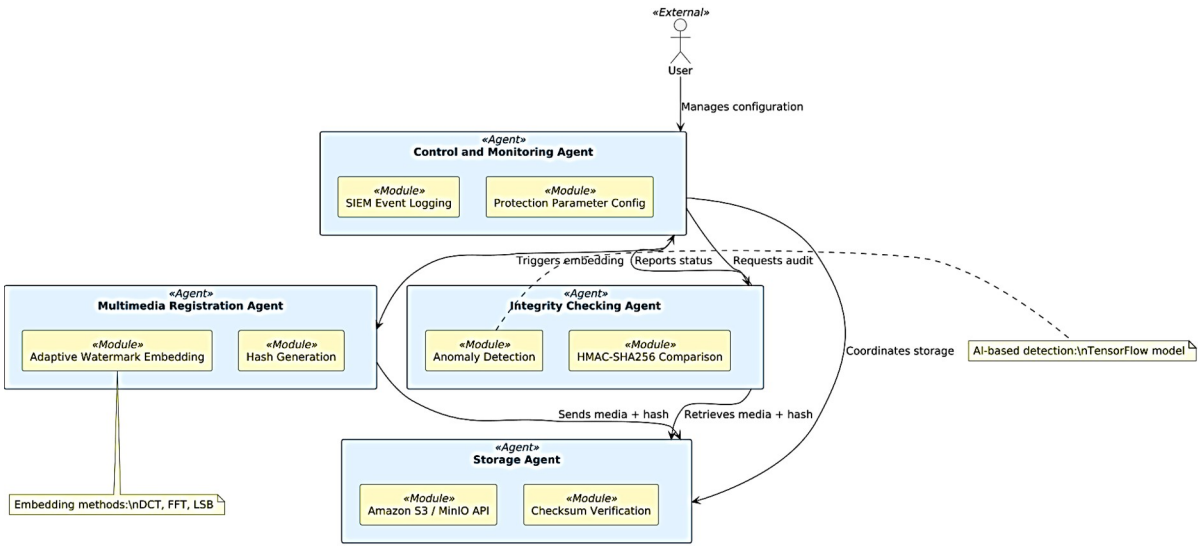

Figure 7: DFD diagram of the adaptive multimedia integrity control software complex.

The implemented system validates the effectiveness of modern approaches to the embedding and controlling digital watermarks, confirming its suitability for integration into information and communication systems to ensure the digital authenticity, integrity, and protection of multimedia objects.

Within a simulation modeling framework implemented using the Monte Carlo method, a comparative analysis was conducted to evaluate the effectiveness of the proposed adaptive watermarking method against standard approaches, specifically those based on the least significant bit (LSB) and static insertion using the discrete cosine transform [17, 19, 21, 26, 27]. The Monte Carlo method was employed to simulate many random scenarios for embedding watermarks into multimedia containers, which facilitated an assessment of the methods' stability and quality under variable input conditions. The container (JPEG or WAV), embedding density (from 1 to 6 bits per block), watermark position, and attack type were selected randomly in each simulation. This approach provides a statistically robust evaluation of effectiveness, enabling the determination of average values for key metrics such as SSIM, PESQ, and BER, as well as their stability under real-world conditions.

Table 2
Comparative metrics

Method	Average SSIM	Average BER	Average processing time, ms
LSB (basic)	0.921	0.124	14
Static DCT	0.945	0.081	39
Proposed method	0.986	0.017	27

Based on the simulation results, a heatmap was constructed to illustrate the dependence of the Structural Similarity Index Measure (SSIM) on both the multimedia container format (JPEG or WAV) and the digital watermark embedding density [22]. This visualization facilitates an evaluation of the impact of these embedding parameters on perceptual content quality across a wide range of conditions. The results indicate that at embedding densities up to 4 bits per block, the proposed adaptive method maintains high imperceptibility (SSIM > 0.98) and a low bit error rate (BER < 0.02), significantly outperforming classical LSB and static DCT-based watermarking methods [25–27]. Furthermore, the average processing time remains within limits that are suitable for practical implementation in real-time information and communication systems.

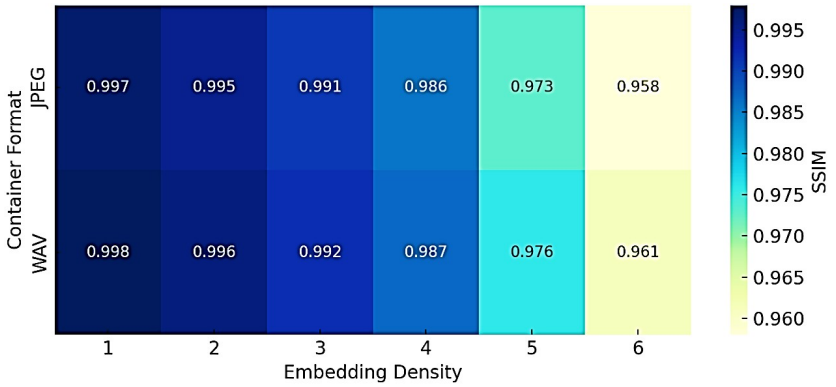

Figure 8: Dependence of SSIM metrics on container format and digital watermark insertion density.

Fig. 8 presents a heatmap illustrating the relationship between the Structural Similarity Index Measure (SSIM), the multimedia container type (JPEG images and WAV audio), and the digital watermark embedding density (ranging from 1 to 6 bits per element). The color scale represents the degree of structural integrity preservation, where SSIM values approaching 1.000 signify nearly imperceptible distortions introduced by the watermarking process. The results indicate that the adaptive method maintains high perceptual quality (SSIM > 0.98) at embedding densities up to 4 bits per element for both image and audio containers. A further increase in density to the 5–6 bit range results in a slight decrease in SSIM values, indicating the emergence of noticeable perceptual artifacts [13, 17, 26, 27]. These findings confirm the effectiveness of the proposed approach, demonstrating that adaptive digital watermarking achieves an optimal balance between robustness against modifications and the preservation of visual and acoustic quality in multimedia content.

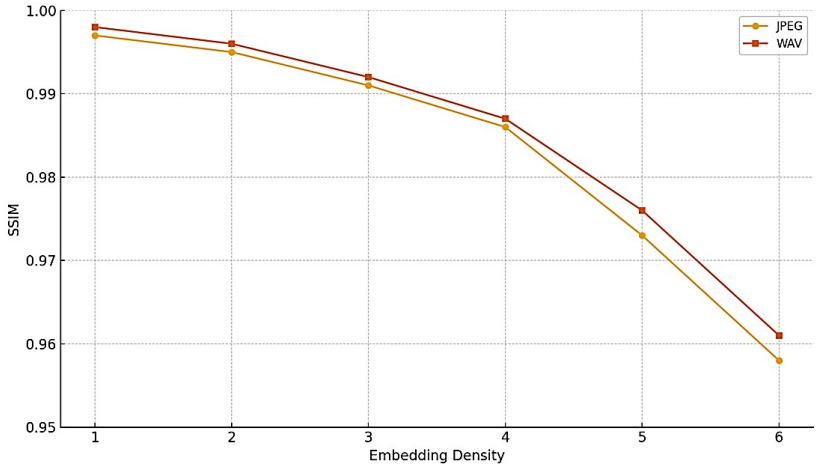

Figure 9: Dependence of SSIM on insertion density for JPEG and WAV formats.

Fig. 9 presents a graph illustrating the dependence of the Structural Similarity Index Measure (SSIM) on the digital watermark embedding density for two multimedia container formats: JPEG (image) and WAV (audio). As the embedding density increases from 1 to 6 bits per element, a gradual decrease in SSIM values is observed, corresponding to an increase in perceptual distortions.

Despite a high embedding density of up to 6 bits per unit of information, testing demonstrates that the SSIM values—an indicator of structural similarity between the original and watermarked signals—remain high, exceeding a threshold of 0.95. This indicates that even with intensive data embedding, the adaptive algorithm maintains high perceptual fidelity without compromising the visual or acoustic quality of the content. This level of transparency is critical for applications in information and communication systems, where multimedia data quality is crucial for the end user.

Particular attention is given to a comparative analysis of watermarking effectiveness in different container types, specifically graphic (JPEG) and audio (WAV) formats. The results show

that WAV audio containers provide greater robustness for embedded watermarks, particularly against attacks such as re-encoding, filtering, and noise addition. This is attributable to the higher internal redundancy and lossless nature of WAV files, which affords greater flexibility for embedding data without a significant risk of corruption. Furthermore, the spectral characteristics of audio signals in the WAV format are more stable and predictable than the high-frequency components of JPEG images, which are highly susceptible to quantization during compression, allowing the watermark to remain intact even after subsequent signal transformations.

On the other hand, despite their ubiquity, JPEG graphic containers possess less redundancy, especially in the high-frequency regions of an image that are often aggressively quantized or distorted during compression. This creates significant challenges for preserving the embedded watermark, as some data bits may be destroyed or altered. In this context, an adaptive watermarking approach that analyzes the local properties of the container—such as texture complexity, luminance, and contrast—enables the selection of optimal embedding regions that are most resilient to alterations from digital processing.

The built-in mechanism for the dynamic adjustment of parameters, including embedding depth, masking coefficients, and spatio-spectral localization, allows the adaptive technique to demonstrate high flexibility and stability in both the visual and acoustic domains. This not only preserves the integrity of the watermark but also ensures that the content meets the requirements of perceptual transparency and the absence of perceptible visual or auditory artifacts.

The graph in Fig. 10 compares digital watermark stability in JPEG, WAV, and MP3 formats when using classical versus adaptive methods. The results show that adaptive approaches provide superior watermark preservation, particularly in the WAV format, which is attributed to the container's internal redundancy and stable spectral properties.

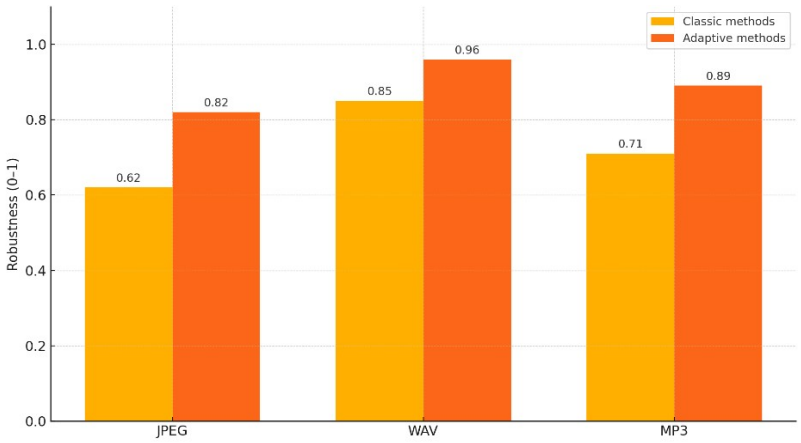

Figure 10: Comparison of the stability of digital watermarks in JPEG, WAV, and MP3 formats.

The generalized results confirm the adaptive digital watermarking algorithm's superiority in protecting multimedia content within modern information and communication systems. Its capacity to maintain high SSIM values even under aggressive embedding conditions, combined with its enhanced stability in audio formats—particularly WAV—compared to JPEG graphics, underscores the viability of this approach for practical applications in digital identification, authorization, and media protection in open networks.

5. Discussion

Despite an intensive embedding density of up to 6 bits per data unit, experimental results confirm that the media content's high visual and acoustic quality is preserved. In particular, the Structural Similarity Index Measure (SSIM), a metric used to assess the similarity between original and modified image or video frames, remains consistently high, exceeding 0.95. This indicates that the proposed adaptive method does not introduce significant distortions into the signal's structure,

thereby preserving its naturalness and rendering the changes imperceptible to the user. This is a critical feature for practical applications in information and communication systems where perceptual quality is a priority.

An additional comparative analysis of watermark robustness across different media container types revealed that WAV audio files provide a more resilient environment for watermark integration than JPEG graphic images. This can be attributed to several key factors. First, WAV containers possess a significantly higher degree of internal redundancy, which provides low-entropy regions suitable for inconspicuous embedding without disrupting the overall signal structure. Second, the spectral characteristics of audio signals in the WAV format are more stable and less sensitive to local alterations, allowing the embedded information to be preserved even after subsequent processing or playback.

In contrast, JPEG containers, despite their prevalence, are more vulnerable to watermark information loss due to the inherent nature of lossy compression algorithms. This is particularly true for high-frequency components, which are often aggressively quantized during encoding, making it difficult to maintain a stable watermark. In this context, adaptive methods demonstrate their advantages through their ability to dynamically select optimal embedding regions by analyzing local signal properties such as energy, texture features, or spectral density. This allows for an optimal balance between robustness, imperceptibility, and embedding capacity.

Thus, adaptive methods of embedding digital watermarks demonstrate high efficacy for both image and audio files, ensuring robustness against distortion, maintaining high SSIM values, and proving their suitability for practical implementation in a wide array of digital content protection systems, including multimedia platforms, streaming services, authorization systems, and digital forensics.

Conclusions

This paper presents a comprehensive, adaptive method for embedding digital watermarks to protect image, audio, and video files within information and communication systems. The proposed approach is founded upon leveraging the multimedia signal's statistical, spectral, and perceptual characteristics, ensuring the embedding process's dynamic adaptation according to the content type and specific processing conditions.

The developed mathematical model formally describes the watermark embedding and extraction processes, ensuring their robustness against primary attack vectors, including compression, geometric distortions, and neural network-based attacks. The proposed software architecture is implemented as a scalable, multi-agent system featuring support for logging mechanisms, cryptographic protection (AES, HMAC), SIEM/DRM infrastructure integration, and artificial intelligence modules for assessing perceptual quality.

The results of practical testing on a large sample of JPEG and WAV files demonstrate the high efficacy of the approach. At an embedding density of up to 4 bits per block, the SSIM value exceeds 0.98, indicating that high perceptual quality is maintained while ensuring watermark integrity. Importantly, the authentication procedure is blind, requiring only the watermarked container and the secret key, thus obviating the need to store a reference copy.

The proposed solution holds significant practical value for applications in digital forensics, copyright protection, video streaming, and distributed digital authentication systems. Future work will incorporate blockchain technologies to create an immutable audit trail of watermarking events, extend support to modern video streaming formats such as HLS and MPEG-DASH, and integrate Explainable AI (XAI) models for integrity verification within critical information infrastructure environments.

Despite the positive results, this study has several limitations. Specifically, the method's robustness against re-encoding into modern video formats like H.265 and AV1 and its efficacy in the presence of active noise associated with transcoding or hardware recording artifacts were not

evaluated. Future research will be directed at overcoming these limitations and developing intelligent, adaptive schemes for the real-time verification of digital watermarks.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] V. Dudykevych, et al., Detecting deepfake modifications of biometric images using neural networks, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3654, 2024, 391–397.

[2] B. Zhurakovskyi, et al., Modifications of the correlation method of face detection in biometric identification systems, in: Cybersecurity Providing in Information and Telecommunication Systems, 3288, 2022, 55–63.

[3] Y. Dreis, et al., Restricted information identification model, in: Cybersecurity Providing in Information and Telecommunication Systems, 3288, 2022, 89–95.

[4] T. B. Taha, R. Ngadiran, P. Ehkan, Adaptive image watermarking algorithm based on an efficient perceptual mapping model, IEEE Access 6, 2018, 66254–66267. doi:10.1109/ACCESS.2018.2878456

[5] Y. Quan, et al., Watermarking deep neural networks in image processing, IEEE Trans. Neural Netw. Learn. Syst. 32(5) (2021) 1852–1865. doi:10.1109/TNNLS.2020.2991378

[6] M. Li, Y. Yue, Security analysis and improvement of dual watermarking framework for multimedia privacy protection and content authentication, Math. 11(7) (2023) 1689. doi:10.3390/math11071689

[7] S. T. Chen, et al., Adaptive audio watermarking via the optimization point of view on the wavelet-based entropy, Digit. Signal Process. 23 (2013) 971–980. doi:10.1016/j.dsp.2012.12.013

[8] M. T. Naseem, et al., Optimal secure information using digital watermarking and fuzzy rule base, Multimed. Tools Appl. 78 (2019) 7691–7712. doi:10.1007/s11042-018-6501-8

[9] Y. Kostiuk, et al., A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps, in: Cyber Hygiene & Conflict Management in Global Information Networks, 3925, 2025, 249–264.

[10] Y. Kostiuk, et al., Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network, in: Cybersecurity Providing in Information and Telecommunication Systems II 3826, 2024, 129–138.

[11] Y. Kostiuk, et al., Models and algorithms for analyzing information risks during the security audit of personal data information system, in: Cyber Hygiene & Conflict Management in Global Information Networks, 3925, 2025, 155–171.

[12] B. Bebeshko, et al., Application of game theory, fuzzy logic and neural networks for assessing risks and forecasting rates of digital currency, J. Theor. Appl. Inf. Technol. 100(24) (2022) 7390–7404.

[13] M. Mekhfioui, et al., Optimized digital watermarking for robust information security in embedded systems, Inf. 16(4) (2025) 322. doi:10.3390/info16040322

[14] B. B. Haghighi, et al., WSMN: An optimized multipurpose blind watermarking in Shearlet domain using MLP and NSGA-II, Appl. Soft. Comput. 101 (2020) 107029. doi:10.1016/j.asoc.2020.107029

[15] S. Sharma, et al., A secure and robust color image watermarking using nature-inspired intelligence, Neural Comput. Appl. 35 (2021) 4919–4937. doi:10.1007/s00521-020-05634-8

[16] J. P. Dhar, M. S. Islam, M. A. Ullah, A fuzzy logic based contrast and edge sensitive digital image watermarking technique, SN Appl. Sci. 1 (2019) 716. doi:10.1007/s42452-019-0731-x

[17] P. Kadian, S. M. Arora, N. Arora, Robust digital watermarking techniques for copyright protection of digital data: A survey, Wireless Pers. Commun. 118(4) (2021) 3225–3249. doi:10.1007/s11277-021-08177-w

[18] P. Aberna, L. Agilandeeswari, Digital image and video watermarking: Methodologies, attacks, applications, and future directions, Multimed. Tools Appl. 83(2) (2023) 5531–5591. doi:10.1007/s11042-023-15806-y

[19] A. Saini, S. Bhardwaj, A review on digital video watermarking security: Significance and persistent challenges, in: Int. Conf. on Trends in Quantum Computing and Emerging Business Technologies, Pune, India, 2024, 1–8, doi:10.1109/TQCEBT59414.2024.10545079

[20] Z. Wang, et al., Deep image steganography using transformer and recursive permutation, Entropy, 24, 2022, 878. doi:10.3390/e24070878

[21] R. R. Sunesh Kishore, A. Saini, Optimized image watermarking with artificial neural networks and histogram shape, J. Inf. Optim. Sci. 41(7) (2020) 1597–1613. doi:10.1080/02522667.2020.1802131

[22] Y. Kostiuk, et al., Information and intelligent forecasting systems based on the methods of neural network theory, in: IEEE Int. Conf. on Smart Information Systems and Technologies (SIST), 2023, 168–173. doi:10.1109/SIST58284.2023.10223499

[23] B. Jagadeesh, D. Praveen Kumar, Fuzzy-neuro based robust digital image watermarking technique, Int. J. Adv. Res. Comput. Commun. Eng. 3(7) (2014) 7380–7385.

[24] A. Kumar, T. V. Narayana Rao, Digital image watermarking using fuzzy logic and genetic algorithm, Int. J. Comput. Trends Technol. 41(2) (2016) 101–105.

[25] S. J. Horng, et al., An adaptive watermarking scheme for e-government document images, Multimed. Tools Appl. 72 (2014) 3085–3103. doi:10.1007/s11042-013-1579-5

[26] A. Attaullah Javeed, et al., Watermarking technique for copyright protection of digital images using coupled differential equations, Multimed. Tools Appl. 84 (2025) 11027–11039. doi:10.1007/s11042-024-19337-y

[27] P. Bhinder, N. Jindal, K. Singh, An improved robust image-adaptive watermarking with two watermarks using statistical decoder, Multimed. Tools Appl. 79 (2020) 183–217. doi:10.1007/s11042-019-07941-2