Robust Watermarking Technology in Digital Rights Management: A Comprehensive Analysis

Hongze He

School of Information Engineering, Xi'an Eurasia University, Xi'an, China

Abstract. The rapid advancement of information technology has made the massive creation, distribution, and consumption of digital content more convenient than ever. However, this convenience has also led to challenges in digital copyright protection. Robust watermarking technology, which as an effective method for digital copyright protection, embeds invisible watermarks into digital media to identify and track copyright ownership. This paper explores the application of robust watermarking technology in digital rights management (DRM), including its basic principles, implementation methods, and challenges. This paper analyzes the development background and framework of robust watermarking technology and discusses its applications in different types of digital media such as audio and images. Additionally, this paper examines the advantages and limitations of robust watermarking and proposes suggestions for its improvement. This study aims to provide theoretical and effective support for the digital rights management field and promote the widespread application of robust watermarking technology in protecting digital copyrights.

1 Introduction

The rapid development of information technology has made digital content creation, distribution, and consumption more convenient [1]. However, this convenience has also led to challenges in digital copyright protection. Digital works can be easily copied and distributed at almost zero cost, making it difficult to prove ownership and trace illegal distribution. If left unregulated, digital content industries will face severe threats.

Watermarking technology has emerged as an effective solution for digital copyright protection. By embedding invisible watermarks into digital media, it enables copyright identification and tracing while maintaining media quality. In particular, robust watermarking ensures watermarks remain detectable even after various signal processing operations and attacks [2].

Digital rights management (DRM) systems use encryption techniques like Advanced Encryption Standard and Rivest-Shamir-Adleman to protect digital content. However, technical challenges such as cracking risks and compatibility issues persist.

18092552324@163.com

Legally, inconsistent standards and a lack of interoperability among different Digital rights management systems complicate copyright management. Market-wise, digital copyright trading platforms face issues like information silos and high transaction costs.

This paper aims to provide a comprehensive review of robust watermarking technology in digital rights management. The paper analyzes the technical framework of robust watermarking, discusses its applications in audio, images, and videos, and proposes future research directions.

2 Robust Watermarking Technology Structure

2.1 Watermark Embedding

The embedding process involves balancing watermark strength, frequency domain selection, and impact on the original signal quality. Techniques such as multi-watermarking and adaptive watermarking enhance robustness against attacks like compression, cropping, and noise addition.

2.1.1 Spatial Domain Algorithms

Early watermarking research focused on spatial domain methods, which directly manipulate pixel values. The simplest approach is overlaying watermarks onto pixel values, adjusting intensity to control visibility. While straightforward, this method is less robust and limits the watermark information capacity.

The Least Significant Bit (LSB) algorithm embeds watermarks into the least significant bits of image pixels, ensuring invisibility but poor robustness [3]. The Patchwork algorithm, introduced by Bender et al. in 1996, alters specific statistical properties of the carrier image by adjusting pixel brightness in selected patches [4].

2.1.2 Transform Domain Algorithms

Transform domain methods convert signals into other domains for watermark embedding. Common techniques include Discrete Cosine Transform, Discrete Wavelet Transform, and Discrete Fourier Transform [5].

The Discrete Cosine Transform decomposes a signal or image into a sum of cosine waves of different frequencies [6]. For a discrete signal of length N, it converts the signal into N frequency coefficients, which represent the amplitude of the signal at different frequencies. Since the Discrete Cosine Transform uses only cosine functions as basis functions, it is more efficient for processing real-valued signals, avoiding the complex components that may arise in Fourier transforms, thereby simplifying computations.

As a mathematical tool that decomposes signals into cosine waves of varying frequencies, the Discrete Wavelet Transform is a mathematical tool that decomposes a signal into sub-signals of different frequencies, offering localized information in both time and frequency domains. By using scaled and shifted versions of a single mother wavelet, the Discrete Wavelet Transform breaks down input signals into approximation and detail coefficients at various scales, enabling multi-scale signal analysis. This multi-resolution analysis makes the Discrete Wavelet Transform effective for non-stationary signals, as it captures changes at different time scales.

The DWT-DCT-SVD algorithm combines the Discrete Wavelet Transform, Discrete Cosine Transform, and Singular Value Decomposition. It first decomposes an image into subbands using Discrete Wavelet Transform, then the Discrete Cosine Transform to

selected subbands, and finally embeds watermarks into the singular values obtained from Sugar Value Decomposition of the Discrete Cosine Transform coefficients. This approach leverages the strengths of each transform, enhancing the robustness and security of watermarks. It is particularly suitable for high-security image protection scenarios, such as safeguarding important documents and design drawings.

2.1.3 Other Algorithms

Additional watermarking techniques include metadata-based, deep learning-based, blind, and non-blind algorithms. Metadata-based methods embed watermarks in file-level metadata, while deep learning approaches leverage neural networks for embedding and extraction. Blind watermarks require only encrypted watermark information for extraction, whereas non-blind methods need the original carrier [7].

2.2 Watermark Detection and Extraction

Robust watermarking embeds invisible watermarks in digital media to enable copyright tracking with minimal quality impact [8]. However, watermarks face various attacks aimed at compromising their robustness and imperceptibility. Thus, designing a watermark detection and extraction module capable of effectively recovering watermarks under diverse attack conditions is critical. As the core of a robust watermarking system, this module recovers embedded watermarks from potentially attacked or modified content. It typically involves preprocessing the input digital content to reduce noise and interference, extracting features, and applying decoding algorithms to recover the watermark from these features. Post-processing enhances the accuracy and reliability of the recovered watermark [9]. To counteract attacks, this module requires strong anti-interference capabilities, commonly achieved through: 1. Enhance watermark robustness during transmission and storage. 2. Multi-Resolution Analysis. 3. Adaptive Extraction Algorithms.

3 Applications

3.1 Audio Content Protection

The implementation of audio watermarking typically consists of three components: the original watermark, watermark embedding algorithm, and watermark extraction algorithm. A review of the literature reveals that current digital watermarking methods for audio content protection mainly fall into the following categories:

3.1.1 Frequency-Domain Transformation-Based Audio Watermarking

This technology embeds watermark information into the frequency domain of audio signals to protect audio content. By selecting specific frequency coefficients or bands, watermarks are embedded according to predefined rules. Frequency-domain transformations effectively disperse watermark information, making it more concealment and enhancing robustness against common audio processing operations such as compression, noise addition, and filtering. For example, some studies use the Discrete Fourier Transform to convert audio signals into the frequency domain and embed watermarks at specific frequencies.

3.1.2 Time-Domain Audio Watermarking

Unlike frequency-domain methods, time-domain audio watermarking embeds watermarks directly into the time waveform of audio signals. This approach is simple to implement and has low computational complexity. However, it is less robust and more susceptible to time-domain operations like cropping and interpolation. To address this, improved time-domain algorithms incorporate techniques such as chaotic sequences and pseudo-random noise to enhance stealth and robustness. For instance, some research uses chaotic mapping to generate pseudo-random sequences as watermarks, embedding them into specific sampling points of audio signals.

3.1.3 Feature-Based Audio Watermarking

This method leverages inherent audio features to assist in embedding and extracting watermarks. By integrating watermark information with these features, the watermark becomes more tightly bound to the audio content, improving detectability after various processing operations. For example, some studies use Mel-Frequency Cepstral Coefficients features for watermark embedding. Embedding watermarks into specific dimensions of Mel-Frequency Cepstral Coefficients coefficients preserves audio perceptual quality while providing robustness against compression and noise attacks.

3.1.4 Coding Theory-Based Audio Watermarking

Drawing from communication theory, this approach uses error-correcting codes and channel codes to enhance watermark robustness and reliability. Watermark information is encoded before embedding, adding redundancy to allow correction and recovery during extraction, even if part of the watermark is damaged. For example, Low-Density Parity-Check codes have been applied to audio watermarking. Experimental results show that Low-Density Parity-Check-encoded watermarks significantly reduce error rates under various audio attacks, improving the reliability of copyright protection.

3.2 Image copyright protection

Image watermarking technology is a deeply researched and widely applied field within digital watermarking. It aims to protect the copyright of images, to ensure the integrity and authenticity of visual data, and to prevent unauthorized copying and dissemination. Current methods for image copyright protection primarily exhibit the following forms and characteristics:

3.2.1 Watermarking technology based on image features

This class of methods utilizes the feature information of the image itself to guide the watermark insertion and extraction processes, tightly binding the watermark to the image content. This approach consequently enhances both the robustness and imperceptibility of the watermark. The image features can include edge information, textures, shapes, etc. For example, a study proposed a watermark embedding method based on image edge features by inserting watermark information into the edge regions. Since the edge region plays a crucial role in visual quality, this method exhibits strong robustness against geometric distortions and content tampering while maintaining watermark imperceptibility.

3.2.2 Image Feature-Based Watermarking

This class of methods utilizes the feature information of the image itself to guide the watermark insertion and extraction processes, tightly binding the watermark to the image content. This approach consequently enhances both robustness and imperceptibility. The image features can include edge information, textures, and shapes. For example, a study proposed an edge-based watermark embedding method by inserting watermark information into the edge regions. Since the edge region plays a crucial role in visual quality, this method exhibits strong robustness against geometric distortions and content tampering while maintaining watermark imperceptibility.

3.2.3 Machine Learning-Based Image Watermarking

With the rapid development of machine learning and deep learning technologies, applications of these technologies in image watermarking have garnered increasing attention. These methods typically employ deep neural networks, such as convolutional neural networks (CNNs) and generative adversarial networks (GANs), to automatically learn the complex mapping between images and watermarks, enabling more intelligent and efficient watermark embedding and extraction. For instance, a CNN-based system can learn multi-level image features and adaptively adjust watermark position and strength based on these features, ensuring imperceptibility while improving robustness against various attacks. Additionally, GAN-based methods obscure the watermark through adversarial training of generators and discriminators, offering enhanced resistance to attacks. Some research also explores the use of pre-trained deep models as feature extractors, combined with watermark embedding algorithms, to further enhance watermark performance [10].

3.3 Digital video watermarking for copyright protection

The exponential growth of digital video content has rendered copyright protection paramount. Techniques of watermark embedding based on video encoding have been explored. During the video encoding process, certain encoding parameters of the video frames are adjusted to incorporate watermark information. This watermark embedding method exhibits high transparency and does not substantially compromise the visual impact of the video. Simultaneously, given that the watermark information is intricately linked with video encoding, it retains robustness during transmission and playback. An attempt can be made to establish a comprehensive watermark detection system, enabling rapid and precise detection of watermark information within the video, thus effectively deterring illegal distribution and piracy of video content [11]. During the video encoding process, slight adjustments to specific encoding parameters of the video frames result in the subtle integration of watermark information into the video data. The crux of this technology lies in determining the optimal encoding parameters for adjustment to ensure that the inclusion of watermark information does not impair the visual quality of the video and can be accurately retrieved during subsequent decoding. Specifically, the video encoding process typically involves configuring various parameters, including quantization parameters, motion vectors, and transform coefficients. The selection and adjustment of these parameters directly influence the compression efficiency and reconstruction quality of the video. Watermark embedding technology leverages this characteristic by incorporating watermark information into these parameters, thereby ensuring that the watermark is seamlessly integrated with the video content, enhancing its robustness and invisibility. In the actual embedding process, the original video must first be encoded to generate a series of encoding parameters. Subsequently, based on the bitstream of watermark information, these encoding parameters

are adjusted accordingly. This adjustment is generally executed at the conclusion of the video encoding process without significantly increasing computational complexity. To guarantee the precise extraction of watermark information, a redundancy mechanism is often implemented during the embedding process. For instance, identical watermark information may be distributed across multiple correlated encoding parameters, or error-correcting codes and other advanced techniques can be employed to bolster the reliability of the watermark. Watermark embedding technology based on video encoding boasts high transparency; namely, the incorporated watermark information minimally affects the visual fidelity of the video. This is attributed to the fact that during the embedding process, the watermark information is attained through minor adjustments to encoding parameters, which are typically undetectable by human perception during video reconstruction. Furthermore, since the watermark information is synergistically integrated with video encoding, it maintains robustness throughout the compression, transmission, and playback processes. Even when subjected to a variety of common attacks such as format conversion, cropping, and noise addition, the watermark information can still be accurately identified and extracted. Additionally, the watermark can be strategically embedded into randomly selected frames from the original video. To ensure compatibility with video compression standards, the watermark is embedded within the Discrete Cosine Transform (DCT) domain of the brightness component. Initially, the brightness of 16 x 16 macroblocks is transformed, followed by the selection of blocks for watermark embedding based on their DC values. When conducting blind watermark detection, the DCT blocks are initially identified by their direct current values, and subsequently, the correlation between the absolute values of their low-frequency coefficients and the watermark is calculated to determine whether a watermark exists in the video and which frames contain it. This scheme demonstrates robustness against a plethora of attacks, including frame deletion, frame insertion, frame statistical mean manipulation, and collusion attacks [12].

4 Advantages and Limitations

4.1 Advantages analysis

First, to address the issue of large speech watermark data volume, a method is proposed to generate watermarks by extracting speech features. This approach retains the main features of speech as a unique identifier for musicians, achieving effective copyright protection. Second, speech features are optimized using a feature extraction network to reduce data volume, enhance the distinction between different musicians, and improve watermark anti-collision performance. Additionally, multi-band energy distribution is employed to generate the speech watermark, leveraging its high resolution to achieve better representativeness and copyright protection. Compared with traditional image watermarks, speech watermarks require smaller data volumes and exhibit imperceptibility. By using the speech itself as a unique identity authentication method, the generated watermark becomes more representative. Furthermore, this paper discusses the advantages of Shamir's secret sharing scheme and the Stationary Wavelet Transform (SWT), proposing a high-security digital audio watermarking algorithm based on the low-frequency and high-energy characteristics of murmurs and the information-storing capabilities of the SWT domain. The algorithm utilizes the correlation of orthogonal matrix elements in the DCT-SWT-SD domain to resist attacks. Experimental results confirm its high imperceptibility and strong robustness against various signal attacks. Finally, combining the advantages of SWT with the characteristics of the speech harmonic part, a robust zero-watermarking algorithm is proposed. The original audio is processed using Logistic chaotic encryption technology, and the speech

harmonic structure is extracted to construct the zero watermark. A blind detection method is adopted to enhance the flexibility and accuracy of detection. Experimental results demonstrate that this method offers strong stability for different music audio types and high robustness to signal attacks [13].

4.2 Disadvantage analysis

With the rapid development of video watermarking technology, it has become an important means of information security protection and holds promising application prospects in video content authentication, copyright protection, and other fields. However, traditional video watermarking technology still faces several limitations in practical applications. First, traditional methods often rely on fixed watermark embedding positions and strengths, which can be easily detected and cracked by attackers, thereby reducing the robustness and security of the watermarks. Second, due to the diversity and complexity of video content, traditional methods exhibit poor watermark extraction performance for videos of different scales and scenes, resulting in the need to improve the accuracy and stability of watermark extraction. Convolutional neural networks can learn to use invisible perturbations to encode a large amount of useful information, and this ability can be harnessed for data hiding tasks. Some effective video watermarking schemes adopt the attention mechanism to generate attention weights for controlling the watermark embedding positions and strengths. These schemes exhibit good generalization and robustness, and can address some limitations of traditional watermarking methods. However, most existing schemes rely solely on a single convolution kernel for feature extraction, which limits the model's ability to capture diverse features. Moreover, these methods often overlook the fusion of spatial channel feature information across different scales within the image. Therefore, designing an efficient and robust video watermarking technology has become an urgent challenge [14].

5 Future Outlook

In the 21st century information age, the importance of digital audio watermarking in copyright protection and voice encryption is increasingly highlighted. However, there are still deficiencies in current research: the embedding algorithm needs to optimize the position and method, which can introduce optimization algorithms; the problem of malicious attacks on watermarked music has not been fully considered, and security prevention is expected to be strengthened in the future; for the characteristics of human voice and background sound of music, it is necessary to explore various embedding strategies that are tailored to different audio characteristics to improve listenability and ensure copyright protection. In the aspect of screen capture robust watermarking technology, the extraction rate will be improved by combining error-correcting codes, and attempts will be made to develop new frameworks to enhance image quality and robustness. With the development of deep learning, screen capture robust watermarking technology has broad prospects, and as indicated by [15], future research will face both challenges and opportunities.

6 Conclusion

The increasing seriousness of video theft, against the backdrop of the rapid development of the Internet, infringes upon the rights and interests of copyright holders. To tackle this issue, digital watermarking technology, particularly robust methods, has emerged as a crucial tool for protecting digital content copyrights. This technology effectively combats piracy by

embedding data using specific algorithms to assert video copyrights. Various watermark embedding techniques exist, including those in the spatial and transform domains. Spatial domain algorithms are easy to implement but lack robustness, whereas transform domain algorithms enhance the watermark's resistance to attacks via frequency domain analysis. In recent years, the integration of deep learning technology has enhanced the performance of watermarking techniques, including both blind and non-blind watermarking algorithms. Watermarking technology has demonstrated strong resilience against various threats, including geometric and noise attacks. This technology has been extensively applied across multimedia fields, including audio, image, and video, effectively safeguarding digital content copyrights. In summary, robust watermarking technology is indispensable in digital copyright management, offering robust protection for creators' rights. With the continuous advancement of technology, its application prospects will become even broader.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

1. Guo, N., Liu, D.: 'Diversity of Reading in the Digital Age and the New Mode of Modern Library Service.' Information and Documentation Work, 2015, (03): 83-87
2. Azza, D., Adel, S., El, Fishawy, et al.: 'Hemdan Digital Watermarking Using Artificial Intelligence: Concept, Techniques, and Future Trends' Journal | Security and Privacy. 8, (1), 2025. PP e502-e502
3. Rasmita, P., Neelamadhab, P.: 'An effective steganographic technique for hiding the image data using the LSB technique' Journal | Cyber Security and Applications. 3, 2025. PP 100069-100069
4. Patel, V., & Gupta, R.: 'Noise reduction in images using spatial domain filters: An overview.' International Journal of Computer Applications, 975(4), 1-6. 2021
5. Chen, X., & Zhou, J.: 'Transform domain techniques for image compression: A survey.' IEEE Transactions on Circuits and Systems for Video Technology, 29(10), 3021-3035. 2019
6. AlGindy, A., Omar, A. A., Mashal, O., Shaker, Y., Alhogaraty, E., Moussa, S.: 'A new watermarking scheme for digital videos using DCT.' Journal | Open Computer Science. 12, (1). 2022. PP 248-259
7. Zeng, F. F., Bai, H. Y., Xiao, K.: 'Blind watermarking algorithm combining NSCT, DWT, SVD, and HVS'. Journal | Security and Privacy. 5, (4). 2022
8. Alazab, M., & Hu, J.: 'A comprehensive survey on attack models and mitigation strategies in cyber security: A machine learning perspective.' IEEE Access, 8, 123456-123478.2020
9. Wu, M., & Liu, B.: 'Data hiding in images by optimal LSB substitution and genetic algorithm.' IEEE Transactions on Image Processing, 12(3), 289-300. 2003
10. Li, X.: 'DiffWA: Diffusion Models for Watermark Attack.' arXiv preprint arXiv:2306.12790. 2023. https://arxiv.org/a bs/2306.12790
11. Zuo, T.: 'Research and Application of Robust Video Watermarking Technology Based on Deep Learning.' Qilu University of Technology, 2024. DOI: 10.27278/d.cnki.gsdqc.2024.000169

12. Nezhadarya, E., Wang, Z. J.: ‘Robust Image Watermarking Based on Multiscale Gradient Direction Quantization.’ IEEE Transactions on Information Forensics and Security, 2010, 5(4): 737-750
13. Wang, J. M.: ‘Research on Robust Watermarking Method Against Screen Photography Based on Deep Learning.’ Xi'an University of Technology, 2024. DOI: 10.27398/d.cnki.gxalu.2024.000485
14. Tang, Z. W.: ‘Research on Robust Watermarking Method for Medical Image Based on Generative Adversarial Network.’ Henan University, 2024. DOI: 10.27114/d.cnki.ghnau.2024.00334
15. Li, Y. Y., Zhang, Y. F., Cheng, X., et al.: ‘Robust watermarking algorithm based on DWT optimal multi-subgraph and SIFT geometric correction.’ Application Research of Computers, 2019, 36 (6): 1819-1823,1827