

Application of Multimedia Watermarking Technology in the Field of Information Security

Jiliang Bi, Jing Han

Xihua University, Chengdu, 610039, China

Abstract: This paper aims at comprehensively discussing the principle, methods, applications, challenges and future development of multimedia watermarking technology. In order to achieve this goal, this paper first introduces the basic concept and classification of multimedia watermarking technology, and then expounds in detail the core principles of spatial domain, frequency domain and mixed domain watermarking technology and the methods of watermark embedding and extraction. In terms of methods, this paper reveals their technical differences in robustness, invisibility and capacity through in-depth analysis of the characteristics of watermarking technology in different domains. In terms of application, the article shows the extensive application of multimedia watermarking technology in copyright protection, content authentication, covert communication and multimedia data integrity and authenticity verification through specific case analysis, highlighting its important value in the field of information security. Generally speaking, this paper systematically analyzes the principle, method and application of multimedia watermarking technology, which provides an important theoretical basis and practical guidance for further research and development in this field.

Keywords: Multimedia; Watermarking technology; Information security.

1. Introduction

With the rapid development of information technology, the problem of information security has become increasingly prominent, which involves a wide range of fields and has far-reaching influence [1]. At the same time, multimedia technology has been widely used in various fields because of its intuitive, interactive and large information capacity [2]. However, the easy replication and dissemination of multimedia data also bring new challenges to information security [3]. Therefore, how to effectively protect the copyright and information security of multimedia data while ensuring its wide dissemination and utilization has become an urgent problem [4].

In this context, multimedia watermarking technology came into being. As an effective information hiding technology, multimedia watermarking technology can embed specific tag information into multimedia data without affecting the use value of multimedia data [5]. These tag information can be copyright information, identity identification, secret messages, etc., which are used for extraction and verification when necessary, so as to realize various security requirements such as copyright protection, content authentication, covert communication, etc. [6].

Therefore, studying the application of multimedia watermarking technology in the field of information security not only has important theoretical value, but also has extensive practical significance [7]. Through the in-depth research and application of multimedia watermarking technology, we can effectively crack down on piracy and safeguard the legitimate rights and interests of creators; It can ensure the integrity and authenticity of multimedia data and prevent it from being maliciously tampered with or forged; It can also realize covert communication and secret information transmission, and provide effective technical support for military, intelligence and other special fields.

2. Overview of Multimedia Watermarking Technology

2.1. The definition of multimedia watermarking technology

Multimedia watermarking technology is an information hiding technology, which embeds specific tag information (watermark) into multimedia data (such as images, audio, video, etc.) to achieve copyright protection, content authentication, data integrity verification and other purposes [8]. These embedded watermark information is usually invisible and will not affect the normal use of multimedia data, but it can be extracted and verified by a specific detection algorithm. The core of multimedia watermarking technology lies in how to realize effective embedding and reliable extraction of watermark information on the premise of ensuring the quality and availability of multimedia data.

2.2. Development course of multimedia watermarking technology

The development of multimedia watermarking technology can be traced back to the early 1990s, when it was mainly used in the fields of image processing and digital audio. With the rapid development of multimedia technology and network communication technology, the application scope of multimedia watermarking technology is expanding, and it gradually involves video, animation, three-dimensional model and other data types [9]. At the same time, multimedia watermarking technology is constantly facing new challenges and demands, such as resisting various attacks, improving watermark capacity and embedding efficiency. In order to meet these challenges, multimedia watermarking technology has done a lot of research and innovation in algorithm design, watermark embedding and extraction methods, and gradually formed a relatively perfect theoretical system and technical framework.

2.3. Basic principles and classification of multimedia watermarking technology

The basic principle of multimedia watermarking technology can be summarized as follows: embedding specific watermark information in multimedia data, so that these information can be extracted and verified by specific

detection algorithms without affecting the normal use of multimedia data [10]. According to the different embedding methods and application scenarios, multimedia watermarking technology can be divided into spatial domain watermarking technology, frequency domain watermarking technology and mixed domain watermarking technology, as shown in Table 1.

Table 1. Classification of multimedia watermarking technology (A)

Watermarking technology	Embedding mode	Characteristic	Advantage	Disadvantage
Spatial domain watermarking technology	Watermark information is directly embedded in the spatial domain of multimedia data.	The embedding process is simple and direct.	Easy to realize Small changes to the original data	Poor robustness Vulnerable to various attacks.
Frequency domain watermarking technology	Transform multimedia data into frequency domain and embed watermark information in frequency domain.	It is robust and can resist some common attacks.	Resist common attacks Suitable for scenes requiring high security.	The computational complexity is high. Changes to the original data may be large.
Mixed domain watermarking technology	Combining the characteristics of spatial domain and frequency domain, watermark information is embedded in multiple domains at the same time.	The advantages of various domains can be comprehensively utilized to improve the robustness and invisibility of the watermark.	Comprehensive utilization of the advantages of each domain High robustness and invisibility	The algorithm design and implementation are complicated. May lead to long processing time.

In addition, according to the uses and characteristics of watermarks, multimedia watermarking technology can also be divided into visible watermarks and invisible watermarks,

robust watermarks and fragile watermarks, as shown in Table 2.

Table 2. Classification of multimedia watermarking technology (B)

Watermark classification	Definition	Main application	Characteristic requirements
Perceptible	Embedding visible watermark information in multimedia data	Identification of copyright information, content authentication	Watermark should have certain visibility, but it will not affect the main content and experience of data.
Invisible watermark	Embedding invisible watermark information in multimedia data	Covert communication, data integrity verification	Watermark should be completely invisible, which will not affect the perceptual quality and normal use of data.
Robust watermarking	Watermarking that can resist various common attacks.	Copyright protection and content authentication	Watermark should be stable and reliable, and can be detected even if the data is compressed, added with noise and cut.
Fragile watermark	Watermark that is sensitive to data changes and can be detected.	Data integrity verification, tampering detection	Watermark should be very sensitive to any change of data. Once the data is tampered or forged, watermark should be able to be detected and reacted immediately.

3. Core Methods and Technologies of Multimedia Watermarking Technology

3.1. Multimedia watermarking technology

The core methods and technologies of multimedia watermarking technology mainly involve the process of embedding and extracting watermarks, which can be divided into spatial domain, frequency domain and mixed domain watermarking technology according to different processing

domains.

(1) Spatial domain watermarking technology

Spatial domain watermarking technology is one of the earliest watermarking embedding methods. In this method, watermark information is directly loaded on the pixel or sample value of multimedia data. For images, this may involve modifying the brightness or color value of pixels; For audio, it may be a modified waveform sample. The advantage of spatial domain watermarking technology lies in its intuition and easy realization. However, its main disadvantage is poor robustness, because watermark information is easily affected

by common signal processing operations such as compression, filtering and noise addition.

(2) Frequency domain watermarking technology

Frequency domain watermarking technology is a more robust watermarking embedding method. In this method, multimedia data is first transformed into frequency domain (such as using discrete cosine transform DCT, discrete Fourier transform DFT, etc.), and then watermark information is embedded into frequency coefficients. Because many common signal processing and attack operations have relatively little influence in frequency domain, frequency domain watermarking can usually provide better robustness. However, the disadvantage of this method is that the computational complexity is high, and more precise control may be needed to ensure the invisibility of the watermark.

(3) Mixed domain watermarking technology

Mixed domain watermarking technology combines the advantages of spatial domain and frequency domain, aiming at embedding watermark information in multiple domains at the same time to enhance robustness. For example, some methods may first embed a weak watermark in the spatial domain, and then embed a stronger watermark in the frequency domain. In this way, even if the watermark in one domain is destroyed by an attack, the watermark in another domain can still be detected. The challenge of mixed domain watermarking technology is how to balance the watermark strength in different domains to ensure the overall invisibility and robustness.

3.2. Watermark embedding and extracting method

Watermark embedding is a process of integrating watermark information into multimedia data, while watermark extraction is a process of recovering watermark information from multimedia data that may have been attacked. Embedding methods usually involve minor modification of multimedia data to contain watermark information while maintaining the perceptual quality of the data. The extraction method needs to be able to detect and extract the watermark reliably, even though the multimedia data has undergone various forms of processing and attacks. The design of embedding and extracting algorithms usually needs to consider the key factors in Table 3:

Table 3. Key factor

Key factor	Describe
Robustness	Watermark should be able to resist common signal processing operations and malicious attacks, and maintain its stability and detectability.
Invisibility	The multimedia data embedded with watermark should be indistinguishable from the original data in perception, which will not affect the normal use of data and user experience.
Capacity	Watermarking system should be able to embed enough information to meet the application requirements, while balancing the relationship between capacity, robustness and invisibility.
Security	Watermarking system should be able to prevent unauthorized deletion or tampering and protect the integrity and reliability of watermark.

4. Application Case Analysis of Multimedia Watermarking Technology in The Field of Information Security

As an effective means of information security, multimedia watermarking technology plays an important role in copyright protection, content authentication, covert communication and the integrity and authenticity verification of multimedia data. The following are case studies of these application fields.

4.1. Copyright protection and content authentication

In the digital content industry, copyright protection is a crucial task. Multimedia watermarking technology provides an effective means for copyright owners to trace and prove copyright ownership by embedding copyright information in digital works. For example, in the film industry, producers can embed watermarks containing copyright information into copies of movies. Once piracy is discovered, the source of piracy can be traced by extracting watermark information, thus safeguarding the legitimate rights and interests of copyright owners.

In addition, multimedia watermarking technology can also be used for content authentication. By embedding fragile watermark, we can detect whether multimedia data has been tampered or forged. For example, in news photography, a photographer can embed a fragile watermark containing information such as shooting time and place into a photo. In this way, if the photo is tampered with in the process of communication, the authenticity of the photo can be verified by detecting the integrity of the watermark.

4.2. Covert communication and the transmission of secret information

Another application field of multimedia watermarking technology is covert communication and secret information transmission. By embedding secret information into multimedia data, the covert transmission of information can be realized. This technology has important application value in military, intelligence and other special fields. For example, in military communication, watermarks containing important instructions or information can be embedded into publicly available images or videos, and then transmitted through public networks. Because of the concealment of watermark, it is difficult for the enemy to detect the existence of secret information, thus ensuring the safe transmission of information.

4.3. Integrity and authenticity verification of multimedia data

Multimedia watermarking technology can also be used to verify the integrity and authenticity of multimedia data. During the storage and transmission of digital files, multimedia data may be damaged or distorted due to various reasons (such as noise, compression, transmission errors, etc.). By embedding robust watermark, we can detect whether the data has changed and verify the integrity of the data. For example, in medical image diagnosis, doctors can embed watermarks containing patient information and diagnosis results into image data. In this way, even if errors or distortions occur during data transmission, the authenticity and integrity of image data can be verified by extracting

watermark information, thus ensuring the accuracy of diagnosis.

4.4. Specific application case analysis

Film industry: In the process of film production and distribution, producers can use multimedia watermarking technology to embed copyright information and anti-counterfeiting marks to combat piracy. At the same time, by embedding the fragile watermark in the movie, we can detect whether the movie has been illegally edited or tampered with.

Music industry: In the release and sale of music works, multimedia watermarking technology can be used to embed copyright information and singer logos to protect the legitimate rights and interests of music works. In addition, by embedding watermark information into music files, covert transmission and secret communication of music can be realized.

Image processing: In the field of news photography and artistic creation, photographers and artists can use multimedia watermarking technology to embed shooting information, creation time and author identification. This can not only protect the copyright of the work, but also verify the authenticity and integrity of the picture. At the same time, covert watermarking can also be used for covert communication and secret information transmission of pictures.

5. Conclusions

This paper comprehensively discusses the definition, development, basic principles and classification of multimedia watermarking technology, and deeply analyzes its core methods and technologies, including spatial domain, frequency domain and mixed domain watermarking technology, as well as watermark embedding and extraction methods. At the same time, through the analysis of specific application cases, it shows the extensive application of multimedia watermarking technology in the field of information security, such as copyright protection and content authentication, covert communication and secret information transmission, integrity and authenticity verification of multimedia data, etc.

Although the multimedia watermarking technology has made remarkable progress, with the rapid development of multimedia technology and the changing application requirements, there are still many problems and challenges to be solved in this field. Future research will pay more attention to improving the robustness and invisibility of watermark

technology and explore new watermark embedding and extraction algorithms to adapt to more complex and diverse application scenarios. At the same time, with the continuous development of artificial intelligence, big data and other technologies, the combination of multimedia watermarking technology and these advanced technologies will become an important research direction in the future, and it is expected to realize a more intelligent, dynamic and standardized watermarking system. In addition, how to solve the legal and ethical challenges faced by multimedia watermarking technology and protect users' privacy and copyright interests will also be a key issue for future research.

References

- [1] Zhao Ying. Research on the application of image information security based on digital watermarking technology [J]. *Informationization Research*, 2021(001):047.
- [2] Luo Qin. Analysis of the application of digital watermarking technology in electronic information security [J]. *China Strategic Emerging Industries*, 2018, 000(014):172.
- [3] Liao Jiwang. On the application analysis of digital watermarking technology in network information security [J]. *Computer fans*, 2018(6):1.
- [4] Zhao Wenpeng, Li Zichen, You Fucheng, et al. Research on histogram shift security reversible image watermarking algorithm [J]. *Information Technology and Network Security*, 2020, 39(9):5.
- [5] Qi Yanbo, Du Qingzhi. Robust audio watermarking algorithm based on centroid and ASVD [J]. *Information Security and Communication Security*, 2023(3):93-102.
- [6] Gan zhichao, Liu Dan. digital image watermarking forgery technology based on deep learning [J]. *industrial control computer*, 2023, 36(8):127-129.
- [7] Zhao Danyao. Research on information security based on computer network and its protective countermeasures [J]. *Journal of Multimedia and Network Teaching in China (last issue)*, 2020(06):252-253.
- [8] Tian Yuanrun, Li Pengxian. Research on the characteristics of contemporary multimedia news and the direction of technical improvement [J]. *Journalism and Communication Science*, 2023, 11(4):4.
- [9] Sun Na. Application of digital watermarking technology in digital archives protection [J]. *Business Culture*, 2021, 000(003):P.128-129.
- [10] Zhang Jichuan. Application of digital watermarking in information security [J]. *Information and Computer*, 2020, 32(6):2.