Research on the Application of Digital Watermarking Technology in Video Data Traceability

Xiaoming Fan*, Lei Song, Shuo Bao
Beijing Police College, Beijing, China
** Corresponding Author*

Abstract: Artificial intelligence technology represented by "deep fake" provides convenience for criminals to forge identities and confuses the public, which has a great impact on the credibility of video data and great harm to society. As an information hiding technology, digital watermarking can embed specific information into the target data without affecting the quality of the data itself, which is an important means of data right confirmation and source tracking, and has important application value in video data traceability. This paper focuses on the application of digital watermark technology in video data traceability, empirically evaluates and analyzes the application effect of digital watermark technology in video data traceability, and puts forward corresponding improvement suggestions, which provides a new reference for the construction of network trusted video system.

Keywords: Video Data; Digital Watermark; Video Traceability

1. Introduction

With the development of we media and online video technology, online infringement incidents of video occur from time to time, and issues such as copyright protection, ownership identification, and source tracking of digital video content have received more and more attention. Among the many technologies, digital watermarking technology can realize the confirmation and traceability of video data by embedding additional watermark information in the video. Without affecting the original video content, this technology provides an effective protection for the original video content and greatly improves the security capability of video data.

2. Digital Watermarking

Digital watermarking[1] is a method of embedding hidden information into digital media, which can track and verify the ownership, source, or content of data without affecting the quality of the data itself. The technology was first proposed by the NSA (National Security Agency) to protect sensitive electronic documents and communications. At present, digital watermarking has been widely used in various digital contents such as digital audio, video[2], image, document or software model[3]. It is also one of the research hotspots of current data security technology. It is a key technology in the fields of copyright protection, trusted authentication, data traceability, and is also one of the research hotspots of current data security technology.

Different from the watermark attributes, extraction methods and embedded methods, digital watermarks can be divided into multiple divisions. In terms of watermark attributes, it can be classified from embedded capacity, watermark detection, and watermark algorithm. From the perspective of embedded capacity, digital watermarks can be divided into zero water marks and non-zero watermarks. Among them, the zero watermark does not modify the original data during the digital watermark embedding process, and the non-zero watermark needs to be modified by modifying the watermark embedding.

From the perspective of watermark perceptibility, digital watermarks can be divided into visible watermarks and invisible watermarks, both of which have their own strengths and are widely used. From the perspective of the algorithm robustness of digital watermarking, digital watermarks are divided into robust watermarks, semi-fragile watermarks and fragile watermarks. Among them, robust watermark means that the embedded watermark is not vulnerable to attacks, while the vulnerable watermark also

has its unique advantages in multimedia modification and attack detection.

In terms of watermark extraction, digital watermarks are roughly divided into two categories: content-based and stream-based. Among them, the content-based watermarking algorithm can be divided into airspace watermarking algorithm and transformation domain watermarking algorithm. The spatial domain algorithm directly modifies the image data, while the transformation domain algorithm transforms the signal from the spatial domain to the frequency domain and calculates, and then performs the inverse transformation. The former is difficult to balance both invisibility and robustness, while the latter meets the needs of both invisibility and robustness by indirectly modifying the watermark data.

In terms of watermark embedding, there are roughly three kinds of digital watermarks: blind watermarks and non-blind watermarks. Among them, blind watermarks do not need to know the original image when extracting the watermark, while non-blind watermarks require the original watermark logo when extracting the watermark.

3. Video Data Traceability

3.1 Data Traceability

Data traceability[4] generally refers to the technology of tracking and reproducing the original data and evolution process before the origin of the target data, that is, the data generated in each link of the life cycle of the target data in the generation, circulation, and demise of the target data is associated and traced. This technology first appeared in databases and other fields with relatively high requirements for data authenticity. With the development of the network, network deception often appears, the public's demand for data authenticity is getting higher and higher, and data traceability technology has expanded to many fields involving computers and networks. At the same time, with the development of cryptography technology and information technology, the traceability technology of network data has also entered a new stage of development[5].

In practical applications, data traceability is an important technology for data protection and an effective way to reduce the risk of data leakage, such as digital copyright protection[6], data content forgery identification[7], etc. In real life, data traceability is also common. For example, the traceability of a certain express item is the traceability of the flow data of the target item. Generally, it is possible to check whether there is damage by looking at the circulation process of the item. Another example is the traceability of a software product, that is, the traceability of the data generated, circulated and died by the product. Generally, the credibility of the software can be evaluated by looking at the development and circulation process of the software.

3.2 Video Data Traceability

Video data traceability[8], which refers to tracking or verifying the source of the target video, generally involves analyzing and tracing the video data to determine its source, production time, modification history, and tampering traces, in order to verify the authenticity and credibility of the video data.

In practice, video data traceability is mainly used for video source traceability and video forensics[9]. Among them, video source tracing mainly focuses on identifying and tracking the source device information of the video, and pays attention to the originality of the video. Video forgery forensics mainly focuses on the identification of the authenticity of the video, and pays attention to whether it has been forged or tampered with. The commonly used forensics approach for forgery is to embed invisible watermarks in videos, making it impossible for general editing and encoding to completely erase them. This technology is also known as watermark tracking.

3.3 Typical Approach

At present, the typical methods of data traceability are the annotation method[10], workflow log method[11] and reverse query method[12]. The annotation method obtains the traceability of data by looking at the annotation of the target data, such as the 7W model proposed by Sudha[13], which is simple, effective and widely used. Among them, 7W corresponds to 7 factors such as What, Where, Who, When, Which, Why, How, etc., which contains the most important information of the original data, such as background, author, time, source, etc. In practice, labels and data are

propagated together and can be used to trace the historical state of the data. Theoretically, the 7W model can help data users confirm information rights, and retrospectively confirm the authenticity of data, data responsible persons and data modification traces in the process of generating and circulating target data.

It is simple to use the annotation method to trace the data, but it needs to provide additional storage space for the annotation information. Therefore, in the case of large data volume, the reverse query method is generally used for data traceability. The inverse query method, also known as the inverse function method, is the core of which is to construct an inverse function, and then use the function to inverse the query to trace the original data. This method is based on relational algebra, and the data elements such as the source of the data (Why) and the source of the data are inverted through the relationship between the data. This method is more complex than the annotation method, but requires less storage space than the annotation method.

For the workflow log method, it is necessary to first establish a workflow traceability management system, annotate and record the data traceability information in the form of metadata, and design the record management of the information as the core function of the query engine, so that users can complete data traceability through the parsing of workflow log files, such as data verification and dependency mining. This method has high requirements for users in all links of data flow, and there are many limiting factors in promotion and use.

4. Traceability of Video Data through Digital Watermarking Technology

4.1 Main Idea

In video data traceability, digital watermarking technology can be used to mark and trace information such as the origin and production time of a video to verify the authenticity and credibility of the video.

During the specific implementation, in the data generation or modification phase, the tag information can be embedded into the video data by direct embedding or transformation domain embedding. For example, tag information can be embedded in locations such as low-frequency components or invisible areas of the target video to enhance traceability without compromising the quality and look and feel of the target video. In the data usage stage, watermark extraction can be realized with the help of digital signal processing, mathematical modeling, image recognition and machine learning to achieve authenticity identification and source traceability of video data.

The technical principle is shown in Figure 1. Among them, V represents the original video, W represents the original watermark information, K represents the key, $G(\cdot)$ represents the watermark embedded algorithm, $D(\cdot)$ represents the watermark extraction algorithm, V_w represents the video embedded in the watermark, and W_v represents the watermark information extracted from V_w.

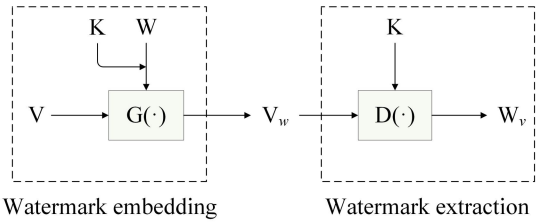

Figure 1. Principle of Video Watermarking Technology

In order to improve the safety of watermarks, when using $G(\cdot)$ to embed the original watermark W into the original video V, the key K needs to be introduced to ensure that the digital watermark is not tampered with or forged. In the watermark extraction session, the video V_w embedded with the watermark will be sent to the watermark extraction module $D(\cdot)$, and the watermark W_v extraction will be completed in combination with K.

4.2 Advantages and Disadvantages

4.2.1 Advantages

Digital watermarking technology has the advantages of concealment, robustness, high security, and easy operation in video traceability.

Good concealment: This technology embeds marker information into unperceived areas of

the video, with good concealment and invisibility.

Strong robustness: This technology has a certain robustness for video compression, editing and transformation operations, even if the video data is modified to a certain extent, it can still be extracted.

High security: This technology uses encryption algorithms to protect the embedded marker information and ensure that the digital watermark is not tampered with or forged, thereby enhancing the credibility and authenticity of the video data.

Easy to operate: Digital watermarking technology is simple to apply, easy to operate, and does not require too much expertise and technical support.

4.2.2 disadvantages

However, digital watermarking technology also has the disadvantages of limited embedding and easy tampering.

Easy tampering: Although digital watermarking technology has a certain robustness, it still has a certain tolerance for some high-intensity tampering operations.

Limited amount of information embedding: Digital watermarking technology has certain restrictions on the amount of information embedding, and cannot embed too much marking information, otherwise it will affect the quality of video data.

Transcoding restrictions: Digital watermarking technology has certain restrictions on the compression and transcoding of videos, which may affect the extraction of digital watermarks.

Professional countermeasures: Digital watermarking technology has professional countermeasures, such as masking attacks, jamming attacks, and cutting attacks, which require targeted technical measures to prevent and respond.

In summary, digital watermarking technology has certain advantages and disadvantages in video traceability, and needs to be reasonably selected and applied according to actual needs and technical conditions.

In the current era of social media and the Internet, video has become an important way for people to obtain information, spread opinions and express themselves, but it also brings many risks of damage to rights and interests. At this point, digital watermarking technology can effectively reduce such risks.

4.3 Typical Applications

4.3.1 Fake composite video

Fake composite video refers to the combination or modification of multiple videos or audios from different sources through technical means to create a false video content. For example, an image of a person's face can be embedded in a targeted video to fake a video of that person making inappropriate remarks. Such videos can have consequences such as reputational damage to specific people, and may even cause public incidents and have a negative impact on society.

For the above situation, digital watermarking technology can be used in the target video to ensure the integrity and authenticity of the video. In order to more effectively protect the privacy of the user, when the watermark is embedded, the original watermark information is usually encrypted or randomly processing, and then embedded into the designated point specified in the target carrier. In this process, digital watermarks can help investigators to track the real source of the video, and confirm the identity of the producer, and provide the infringement providing video confirmation evidence.

4.3.2 Traffic law enforcement video screening

In traffic law enforcement, monitoring videos are usually used to record illegal behaviors and provide evidence for law enforcement agencies. However, these videos may be tampered with or forged, which affects the credibility of the law enforcement department. Using digital watermarking technology, users can embed the unique digital identifier in traffic law enforcement videos to help the video confirmation and provide investigators with powerful video traceability support.

4.3.3 We media videos infringe on reputation

At present, with the development of we media platforms, infringement cases of using video to damage citizens' reputations also frequently appear. Such as deliberately fabricating facts, publicly spreading rumor-mongering videos, etc. Such videos, in serious cases, may cause hype, cause adverse social impact, and even affect public order. Using digital watermarking technology, self-media videos can embed a unique digital identifier (i.e., watermark), which will help investigators target the publisher, producer, etc. of the video after the infringement of others' reputation, so as to facilitate the investigation of subsequent cases.

5. Experiment and Results Analysis

5.1 Environment Settings

In order to verify the application effect of digital watermarking technology in video data traceability, this paper builds a relevant experimental platform, using Windows 10 system and installing OpenCV, FFmpeg, Python and other operating environments. The video dataset UipjDATA was collected and organized, and the accuracy rate and anti-counterfeiting rate were used as the evaluation indicators.

5.2 Apply Performance Analysis

Based on UipjDATAS, this paper uses DWT algorithm[14] to evaluate the application effect of digital watermark in video traceability. Experiments include evaluation of robustness, marker information extraction, tamper detection, and more. The results are shown in Table 1.

Table 1. Application Effect Evaluation and Comparison

Evaluation object	Test content	Results
Robustness	Can the watermark be correctly extracted after the video is transformed	96%
Tag information extraction	Extraction rate of digital watermark marking information	98%
Tamper Detection	Can digital watermarks detect tampering behavior such as masking, shearing	effectively

The above results show that the video digital watermark has certain robustness and detection capabilities, which can provide effective support for video traceability and data right confirmation.

5.3 Applicability Analysis

In order to verify the applicability of digital watermarking technology to different videos, this paper divides UipjDATA into nine subsets and performs a comparative analysis of watermark extraction rate based on bit rate, video format and resolution, and the results are shown in Table 2.

Table 2. Suitability Evaluation Comparison

Datas	Resolution	Bitrate	Video format	Watermark extraction rate (%)
Data1	480p	500kbps	-	72.2
Data2	720p	1Mbps	-	85.3
Data3	1080p	2Mbps	-	96.7
Data4	-	-	MP4	91.9
Data5	-	-	AVI	88.4
Data6	-	-	FLV	94.0
Data7	480p	-	-	91.5
Data8	720p	-	-	95.1
Data9	1080p	-	-	91.8

As can be seen from the test results in Table 2, digital watermarking performs well on video datasets with high bitrates, different formats and resolutions, but slightly worse on low-bitrate video datasets.

5.4 Security Performance Analysis

In addition, this paper also evaluates the concealment, false positive rate, and anti-counterfeiting ability of video watermarks, and the results are shown in Table 3.

Table 3. Performance Evaluation of Watermarks

Evaluation object	Test content	Results（%）
Concealment	The probability that an attacker will successfully detect a digital watermark without knowing the watermarking algorithm	12.1
Misjudgment rate	The probability that normal modification behavior will be misidentified as tampering	5.3
Anti-counterfeiting capability	The probability of successful spoofing by the attacker	9.8

From the above results, it can be seen that the digital watermarking technology represented by DWT still has certain deficiencies in concealment, false positive rate and anti-counterfeiting ability, and faces some problems and challenges, and it is necessary to introduce better algorithm models to improve its support ability for video right confirmation and traceability. Fortunately, in recent years, digital watermarking technology based on deep

learning has been greatly developed[15,16], which will surely provide more effective technical support for video traceability.

6. Conclusion

As a widely concerned self-certification identification technology, digital watermarking technology can embed copyright information, unique identification information and other elements that are conducive to confirmation and traceability into video data in a visible or invisible way, and has important application value in the fields of data confirmation and forensics traceability. With the rapid growth of the number of online videos, piracy, malicious forgery and other behaviors are also spreading and growing, and their harm is increasing day by day. Practice shows that digital watermarking technology can effectively protect the integrity and authenticity of video data, prevent piracy, abuse and malicious modification, and provide key evidence and clues for data traceability, providing strong support for investigation and handling. In the next step, we can combine artificial intelligence and machine learning technology to further improve the embedding quality and attack resistance of video watermarks, and continuously improve the effectiveness and applicability of digital watermarks in video data traceability.

References

[1] Li Y, Wang H, Barni M. (2021) A survey of deep neural network watermarking techniques. Neurocomputing, 461: 171-193.

[2] Wang Y F, Zhou Y M, Qian Z X. (2022) Review of robust video watermarking. Journal of Image and Graphics, 27 (01):27-42.

[3] Xia D, Wang L, Song Y. (2023) Review of deep neural network model digital watermarking technology. Science Technology and Engineering, 23 (5): 1799-1811.

[4] Herschel M, Diestelkämper R, Ben Lahmar H. (2017) A survey on provenance: What for? What form? What from?. The VLDB Journal, 26: 881-906.

[5] Wang F, Zhao H. (2020) Research and practice progress on data traceability. Advances in Information Science, 13 (00): 313-353.

[6] Chen S, Zhang L. (2022) Analysis of the development of digital copyright protection in the context of Metaverse. Media, 384 (19): 78-80.

[7] Yang F, Shen S, Shen D. (2022) Method on multi-granularity data provenance for data fusion. Computer Sience, 49 (05): 120-128.

[8] Chen B. (2019) Digital video source identification and forgery detection technology for safe cities. Xidian University.

[9] Kaur H, Jindal N. (2020) Image and video forensics: A critical survey. Wireless Personal Communications, 112: 1281-1302.

[10] Li Y. (2007) Data provenance's annotation schema and description model. Data Analysis and Knowledge Discovery, 7: 10-13.

[11] Deng Z, Wei Y. (2014) Study on the method of provenance in science workflow for data publishing. Library & Information, 3: 61-66.

[12] Fan H. (2002) Tracing Data Lineage Using Automed Schema Transformation Pathways. Springer-Verlag, 2002: 50-53.

[13] Ram S, Liu J. (2009) A New Perspective on Semantics of Data Provenance. SWPM, 2009.

[14] Liu Q, Yang S, Liu J. (2020) A discrete wavelet transform and singular value decomposition-based digital video watermark method. Applied Mathematical Modelling, 85: 273-293.

[15] Zhang Y, Chen K, Zhou G. (2021) Research progress of neural networks watermarking technology. Journal of Computer Research and Development, 58: 964-976.

[16] Li Y, Tondi B, Barni M. (2021) Spread-transform dither modulation watermarking of deep neural network. Journal of Information Security and Applications, 63: 103004.

