Research on Content Authentication Strategies for Library-Museum-Archive Video Resources Based on Semi-Fragile Watermarking: Postprint

Authors: Zhu Guang, Feng Mining

Date: 2017-11-08T00:00:00+00:00

Abstract

【目的】Design a semi-fragile watermarking algorithm with improved security and real-time performance in big data environments to protect the authenticity and integrity of library and archive video resources. 【应用背景】Ensure robustness of video resources against conventional video operations and meet the real-time requirements for content authentication of library and archive video resources. 【方法】Employ quantization modulation to embed binary watermark images for copyright verification, embed index watermarks in video key frames to detect inter-frame tampering, and perform XOR operations on the least significant bits of video frames to generate authentication watermarks for detecting intra-frame tampering. 【结果】The watermarking algorithm can effectively perform copyright verification and content authentication on video resources, exhibits good transparency, demonstrates strong robustness against conventional video operations, and maintains PSNR above 33. The tampering localization time is approximately 5s, showing good real-time performance. 【结论】This research contributes to protecting the authenticity and integrity of library and archive video resources, and promotes sharing and service integration of library and archive information resources in big data environments.

Full Text

Content Authentication for Video Resources of Libraries, Museums and Archives with Semi-fragile Watermarking

Zhu Guang[1],[2], **Feng Mining**[1]
[1](School of Economics and Management, Nanjing University of Information Science & Technology, Nanjing 210044, China)
[2](School of Information Management, Nanjing University, Nanjing 210093, China)

Abstract

[**Objective**] This study designs a semi-fragile watermarking algorithm with improved security and real-time performance for the big data environment to protect the authenticity and integrity of video resources from libraries, museums, and archives (LAM). [**Context**] The algorithm ensures robustness against conventional video operations while meeting the real-time requirements for content authentication of LAM video resources. [**Methods**] We employ quantization modulation to embed binary watermark images for copyright verification, insert index watermarks into video key frames to detect inter-frame tampering, and generate authentication watermarks through XOR operations on the least significant bits of video frames to detect intra-frame tampering. [**Results**] The watermarking algorithm enables effective copyright verification and content authentication of video resources with good transparency, maintaining a Peak Signal-to-Noise Ratio (PSNR) above 33. Tamper localization time is approximately 5 seconds, demonstrating good real-time performance. [**Conclusions**] This research contributes to protecting the authenticity and integrity of LAM video resources and promotes information resource sharing and service integration in the big data environment.

Keywords: Libraries, Museums and Archives; Video Resources; Content Authentication; Semi-fragile Watermarking; Real-time Performance
Classification Number: G250.76

Introduction

With the advent of the big data era, information service institutions such as libraries, museums, and archives have been digitizing their collections to promote collaborative resource development and sharing. Benefiting from advances in multimedia technology and the proliferation of high-speed broadband networks, vivid and engaging LAM video resources have become the preferred choice for users to browse and collect. However, in big data sharing environments, malicious groups without legitimate authorization may tamper with and forge LAM video resources for various purposes, seriously threatening the authenticity and integrity of video content and infringing upon the legitimate rights and interests of original creators and providers. Due to limitations of the human visual system, effective content authentication of tampered video resources is impossible, while content authentication techniques based on hash functions and cryptography offer low security and cannot determine the location of tampering. Therefore, effective authentication of LAM video resources has become an urgent problem. This paper applies semi-fragile watermarking technology to the content authentication of digital video resources from libraries, museums, and archives. Considering the characteristics of LAM video resources and the real-time demands of big data environments, we propose a semi-fragile watermarking algorithm that combines DCT (Discrete Cosine Transform) quantization coefficients and least significant bit (LSB) perturbation. This approach effectively addresses the shortcomings of existing authentication technologies in terms of

robustness and real-time performance, providing a new solution for content authentication of digital video resources.

Digital watermarking is an emerging information security technology that embeds identification information (digital watermarks) into digital resources through frequency domain transformation. Current research on digital watermarking in LAM institutions primarily focuses on copyright protection, employing robust watermarks. In the content authentication process for LAM video resources, two categories exist based on authentication objectives: "complete-level authentication" and "content-level authentication." Complete-level authentication prohibits any alteration of video data, with the detection system rejecting any minor modification. Content-level authentication emphasizes protecting the information conveyed by the video rather than its specific representation. Consequently, any operation that preserves resource content is considered acceptable and will not trigger rejection. LAM video resource authentication belongs to content-level authentication. During network transmission and sharing, videos undergo format conversion, lossy compression, and other operations, requiring watermarks to maintain robustness against these operations while sensitively detecting malicious tampering and content replacement. Such watermarks, more robust than fully fragile watermarks, are called semi-fragile watermarks.

Existing research on semi-fragile watermarking includes: Qi et al. proposed an image content authentication strategy by modifying the encoding of singular value quantization coefficients to embed semi-fragile watermark information. Ono et al. developed a semi-fragile watermarking algorithm for two-dimensional barcodes, embedding watermark identifiers into mid-high frequency wavelet coefficients of barcode images and detecting coefficient modifications for content authentication. Shi et al. presented a motion-object-based watermarking scheme for video content authentication, using video frame index numbers as reversible watermarks to detect temporal tampering, and embedding content contour information and motion object details as another watermark for tamper detection and localization. Masoumi et al. utilized CDMA technology to embed watermarks into mid-frequency wavelet coefficients of video motion scenes, with watermark modifications detecting malicious content tampering. Horng et al. analyzed the temporal characteristics of digital video, using intra-frame or inter-frame prediction modes from H.264/AVC compression as feature sequences embedded as authentication watermarks into the compressed video stream. Zhao et al. proposed a block compressive sensing-based semi-fragile zero-watermarking algorithm that divides images into sub-blocks, observes each block according to compressive sensing theory, and uses the observed feature values as semi-fragile zero-watermark information.

In summary, existing semi-fragile watermarking authentication strategies primarily focus on digital images. Most video semi-fragile watermarking algorithms have high computational complexity, making it difficult to meet real-time requirements for video content authentication in big data environments

and hindering promotion and application in libraries, museums, and archives. Moreover, existing algorithms do not consider the characteristics of LAM video resources—low resolution, fixed format, and small data volume—and lack application specificity. Therefore, building upon relevant research and focusing on algorithm effectiveness and real-time performance, this paper proposes a semi-fragile video watermarking algorithm based on DCT quantization coefficients and LSB perturbation. The algorithm uses quantization modulation to embed binary watermark identifiers for copyright determination, inserts index watermarks in video key frames (I-frames) to detect inter-frame tampering, and generates authentication watermarks through XOR operations on LSBs of video frames to detect intra-frame tampering, thereby authenticating the authenticity and integrity of LAM video resources.

Malicious tampering of LAM video resources mainly includes spatial domain tampering and temporal domain tampering. The former refers to malicious alteration and attacks on video frame image content, while the latter refers to temporal attacks such as frame deletion, frame reorganization, and frame replacement. Therefore, three types of watermarks must be embedded: binary watermark images for copyright identification, index watermarks for inter-frame tamper localization, and authentication watermarks for intra-frame tamper localization. The algorithm flow is shown in Figure 1 [Figure 1: see original paper].

3. Methodology

3.1 Watermark Embedding

We first embed binary watermark images for copyright authentication of LAM video resources and insert index watermarks for inter-frame tampering authentication and localization. Index watermark information uses DCT coefficient Hash values and video frame sequence numbers to detect temporal attacks and tampering. The specific steps are as follows:

(1) Obtain the luminance component of the original video key frame and perform 8$×$8 block DCT transformation to acquire the corresponding DCT coefficients.

(2) Scramble the binary watermark image using Arnold transformation (with key K1) to ensure watermark security, map the scrambled image into a binary watermark sequence, use a spreading coefficient to map the one-dimensional sequence into a spread spectrum watermark matrix, and then perform 8$×$8 block DCT transformation on the matrix.

(3) Embed watermark information using quantization modulation and calculate the Hash value of the DCT coefficients from the watermarked video frame. When video content suffers malicious tampering, DCT coefficients change, causing the Hash value to change accordingly.

(4) Use key K2 to select a quantization coefficient from the 8$×$8 block, extract its least significant bit, combine the LSB with the Hash value and video frame sequence number, and replace the LSB of the block' s quantization coefficient with this combined bitstream to complete index watermark embedding.

The authentication watermark is used for intra-frame tamper localization in video resources, with the following process:

(1) Select the original video frame image, divide it into 2$×$2 blocks, and define x_i as pixel values. Set the least significant bits (LSB) of each sub-block' s pixels to zero, obtaining $x_i' = \lfloor x_i/2 \rfloor \times 2$.

(2) According to the singular value perturbation theorem, generate watermark information through XOR operations on image block singular value norms. First, calculate and round the singular value norm of the image block as shown in formula (1), where $\lfloor \cdot \rfloor$ denotes floor rounding: $N = \lfloor \|S\| \rfloor$.

(3) Perform XOR operations on the 8 bit planes of mN to generate watermark information. The watermark is closely linked to each block' s pixels, enhancing sensitivity to malicious tampering. The rule is shown in formula (2), where b_i is the i-th bit of mN, wf is the generated watermark information, and w_i is the i-th bit of the watermark pixel value: $wf = b_1 \oplus b_2 \oplus \cdots \oplus b_8$.

(4) Embed the watermark information into the LSB of the corresponding sub-block pixels and recombine the sub-blocks to obtain the watermarked video frame image.

3.2 Watermark Extraction and Authentication

The watermark extraction and authentication process proceeds as follows:

(1) Extract the luminance component of the watermarked video key frame and perform 8$×$8 block DCT transformation.

(2) Calculate the DCT quantization coefficient in the 8$×$8 block using key K2, extract the corresponding coefficient' s LSB stream (including the DCT coefficient Hash value, frame sequence number, and original LSB of the DCT quantization coefficient).

(3) Perform inverse DCT on the quantization coefficients and apply Arnold inverse scrambling to the watermark sequence using key K1 to obtain the extracted binary watermark image for copyright authentication. Simultaneously, if the extracted Hash value matches the original Hash value, the

video resource has not been maliciously tampered with. If the two Hash values differ, the extracted frame sequence number is used to detect frame deletion, addition, or replacement between key frames.

To extract authentication watermark information for intra-frame tamper localization, first divide the watermarked video frame image into 2$×$2 blocks and obtain the LSB values of each pixel in the sub-block, defined as l_i. Following the same steps as embedding, perform singular value transformation, norm rounding, and pixel XOR operations on the sub-block to extract the authentication watermark wf. Compare wf with l_i; if they match completely, the video frame has not been tampered with. If any values differ, the video frame has been tampered with, and the tampered location is marked.

4. Experimental Results and Analysis

Using Matlab 2010 as the simulation platform, we validated the effectiveness of the watermarking algorithm on multiple video resources. Ten representative test videos were selected: Peking Opera videos "Peach Blossom Hotel," "Yu Tang Spring," "Huashan Love and Hate," and "Daughter of a Noble House" from the Nanjing Library video repository; "Brocade Museum," "Treasure Gallery," and "Lacquerware Gallery" from the Nanjing Museum video exhibition; and "Four-legged Censer," "Guanyin Seated Statue," and "White Sand Teapot" from the Nantong Museum collection. All videos are in WMV format, with frame screenshots shown in Figure 2 [Figure 2: see original paper].

4.1 Security Analysis

The security of a watermarking algorithm depends on keys rather than the algorithm itself. This paper uses key K1 for Arnold scrambling; without knowledge of K1, the correct watermark image cannot be obtained. Key K2 is used to select quantization coefficients, preventing watermark attacks by malicious actors unaware of K2. Therefore, the security of our semi-fragile watermarking algorithm depends entirely on keys K1 and K2, while the algorithm flow can be fully disclosed.

4.2 Feasibility Analysis

Feasibility analysis of semi-fragile watermarking authentication includes false alarm probability analysis and missed detection probability analysis. False alarm probability refers to cases where the video has not been tampered with but the detection indicates tampering. In our algorithm, when the LSB of any sub-block in the video frame remains unchanged, the extracted watermark matches the original watermark information. Therefore, the algorithm' s false alarm probability (FAP) is 0.

Missed detection probability refers to cases where tampering occurs but is not detected. For the extracted watermark information wf and extracted LSB bitmap

l_i, the probability that $wf = l_i$ is 1/2 for each bit. To determine that a video has not been tampered with, $wf_i = l_i$ (for $i = 1, 2, 3, 4$) must hold. Therefore, the probability that a tampered 2$×$2 video frame block is not detected as tampered is 2^{-4}. If a frame contains m 2$×$2 sub-blocks, the missed detection probability is $P_M = 2^{-4m}$. Malicious tampering with too few blocks cannot achieve its purpose, and when m is sufficiently large, the algorithm' s missed detection probability becomes negligible.

4.3 Transparency Analysis

To further verify the effectiveness of our watermarking scheme for LAM video content authentication, we analyze transparency, robustness, tamper localization accuracy, and real-time performance. Transparency means that visual quality should not significantly degrade after watermark embedding. The objective metric for transparency is Peak Signal-to-Noise Ratio (PSNR), where higher values indicate better transparency. If $I(i, j)$ represents an original video frame and $I'(i, j)$ represents the watermarked frame, PSNR is calculated as [21]: PSNR=10 MN max[(I(i, j))] [I(i, j) I (i, j)]

Figure 3 [Figure 3: see original paper] shows the 7th frame before and after watermark embedding. Visual quality is not significantly affected, and the human visual system cannot perceive the watermark' s presence. Table 1 presents PSNR values for the ten test videos. Figure 4 [Figure 4: see original paper] compares the transparency of our algorithm with those in references [11-12], demonstrating that our algorithm achieves better transparency.

4.4 Robustness Analysis

Our semi-fragile video watermarking authentication algorithm belongs to "content-level authentication" and must maintain robustness against common operations during network transmission and sharing, such as noise addition, MPEG compression, and filtering. Robustness means that the watermark can still be clearly extracted after conventional video operations to verify copyright ownership [22]. The evaluation metric is Normalized Correlation (NC), which measures similarity between original and extracted watermark images. If $W(i, j)$ is the original watermark and $W'(i, j)$ is the extracted watermark, NC is calculated as: W(i, j)W (i, j) [W(i, j)]

Ten common video operations were used to validate robustness, as listed in Table 2 . Table 3 shows NC values for the ten test videos after different attacks. Using "Peach Blossom Hotel" as an example, clear watermark images can still be extracted after video attacks, as shown in Figure 5 [Figure 5: see original paper]. Experimental results demonstrate that our video watermarking algorithm exhibits strong robustness against common operations including MPEG compression, filtering, and noise attacks.

Figure 6 [Figure 6: see original paper] compares the robustness of our method with algorithms from references [11-12] using "Peach Blossom Hotel" as the test

video, confirming that our algorithm achieves higher robustness.

4.5 Tamper Localization Analysis

Malicious tampering generally includes frame deletion, frame replacement, and modification of video frame content. Temporal attacks such as frame deletion and replacement can be detected and localized using frame sequence numbers, with results shown in Figure 7 [Figure 7: see original paper].

Using "Daughter of a Noble House" as an example, we analyzed spatial domain tampering (frame content modification) localization for LAM video resources. The tampered video frame shows no visual difference from the original, but tamper localization results are shown in Figure 8 [Figure 8: see original paper].

4.6 Real-time Performance Analysis

We calculated the average tamper localization time for the ten test videos and compared it with references [11-12], as shown in Table 4 . Results demonstrate that our algorithm offers better real-time performance and is more suitable for big data environment applications.

Conclusion

Addressing the content authentication requirements for authenticity and integrity of LAM video resources in big data sharing environments, this paper designs a semi-fragile watermarking algorithm that embeds copyright watermarks, index watermarks, and authentication watermarks for copyright verification and tamper localization. Theoretical analysis and simulation experiments demonstrate that our video watermarking algorithm achieves high security and feasibility, strong robustness against common video operations, and effective content authentication without degrading visual quality. Additionally, low computational complexity supports real-time application in big data environments. Consequently, our content authentication strategy contributes to protecting the authenticity and integrity of LAM video resources and promotes information resource sharing and service integration.

Future research will focus on designing universal video watermarking algorithms applicable to multiple video formats and introducing Web Service architecture and intelligent agent technology to avoid redundant development.

References

[1] Zhu Xuefang. On the Digitalized Construction and Service Integration of the Information Resources of Libraries, Museums and Archives [J]. Information and Documentation Services, 2011(5): 57-60.
[2] Yu Y H, Zhang L. Research on a Provable Security RFID Authentication Protocol Based on Hash Function [J]. Journal of China Universities of Posts and

Telecommunications, 2016, 23(2): 31-37.
[3] Liu H, Xiao D, Zhang R, et al. Robust and Hierarchical Watermarking of Encrypted Images Based on Compressive Sensing [J]. Signal Processing: Image Communication, 2016, 45: 41-51.
[4] Hao Shibo, Zhu Xuefang. An Image Zero-Watermarking Algorithm Using Block Compressive Sensing for Libraries, Museums and Archives [J]. New Technology of Library and Information Service, 2014(6): 87-93.
[5] Zhu Guang. Copyright Protection Scheme of Color Images for Libraries, Museums and Archives Based on Zero-Watermarking [J]. New Technology of Library and Information Service, 2015(12): 89-94.
[6] Zhang Junliang, Zhu Xuefang. The Implementation of Copyright Protection for Digitalizing Ancient Books Image Based on Binary Image Watermarking [J]. New Technology of Library and Information Service, 2010(9): 79-83.
[7] Zhu Xuefang. Application of Image Watermarking in Digital Archives Development [J]. Archives Science Bulletin, 2010(5): 72-75.
[8] Loukhaoukha K, Refaey A, Zebbiche K. Comments on "Homomorphic Image Watermarking with a Singular Value Decomposition Algorithm" [J]. Information Processing & Management, 2016, 52(4): 644-645.
[9] Chen Mingqi, Niu Xinxin, Yang Yixian. The Research Developments and Applications of Digital Watermarking [J]. Journal of China Institute of Communications, 2001, 22(5): 71-79.
[10] Xu D W, Wang R D, Shi Y Q. An Improved Reversible Data Hiding-Based Approach for Intra-frame Error Concealment in H.264/AVC [J]. Journal of Visual Communication and Image Representation, 2014, 25(2): 410-422.
[11] Qi X J, Xin X. A Singular-value-based Semi-fragile Watermarking Scheme for Image Content Authentication with Tamper Localization [J]. Journal of Visual Communication and Image Representation, 2015, 30: 312-327.
[12] Ono S, Maehara T, Minami K. Coevolutionary Design of a Watermark Embedding Scheme and an Extraction Algorithm for Detecting Replicated Two-dimensional Barcodes [J]. Applied Soft Computing, 2016, 46: 991-1007.
[13] Shi Y J, Qi M, Yi Y G, et al. Object Based Dual Watermarking for Video Authentication [J]. Optik, 2013, 124(19): 3827-3834.
[14] Masoumi M, Amisi S. Content Protection in Video Data Based on Robust Digital Watermarking Resistant Intentional and Unintentional Attacks [J]. International Arab Journal of Information Technology, 2012, 11(2): 204-212.
[15] Horng S J, Farfoura M E, Fan P Z, et al. A Low Cost Fragile Watermarking Scheme in H.264/AVC Compressed Domain [J]. Multimedia Tools and Applications, 2014, 72(3): 2443-2462.
[16] Zhao Chunhui, Liu Wei. Block Compressive Sensing Based Image Semi-fragile Zero-watermarking Algorithm [J]. Acta Automatica Sinica, 2012, 38(4): 609-617.
[17] Li Shuzhi, Zhang Xiang, Deng Xiaohong, et al. Reversible Video Watermarking Algorithm for H.264/AVC Based on Mode Feature [J]. Journal of Image and Graphics, 2015, 20(10): 1285-1296.
[18] Ghazy R A, Amoon M, Abdallah H A, et al. Block Based Embedding of Encrypted Watermarks Using Singular Value Decomposition [J]. Optik, 2014,

125(20): 6299-6304.
[19] Rastia P, Samieib S, Agoyic M, et al. Robust Non-Blind Color Video Watermarking Using QR Decomposition and Entropy Analysis [J]. Journal of Visual Communication and Image Representation, 2016, 38: 838-847.
[20] Dutta T, Gupta H P. A Robust Watermarking Framework for High Efficiency Video Coding (HEVC) -Encoded Video with Blind Extraction Process [J]. Journal of Visual Communication and Image Representation, 2016, 38: 29-44.
[21] Lu Z M, Zheng W M, Pan J S, et al. Multi-Purpose Image Watermarking Method Based on Mean-Removed Vector Quantization [J]. Journal of Information Assurance and Security, 2006, 1(1): 33-42.
[22] Jiang Gangyi, Li Wenfeng, Yu Mei, et al. Robust Video Watermarking in H.264/AVC Compressed Domain [J]. Optics and Precision Engineering, 2015, 23(1): 260-270.

Author Contributions

Zhu Guang: Algorithm design, paper writing.
Feng Mining: Paper revision, data collection.

Conflict of Interest

All authors declare no conflict of interest.

Supporting Data

Supporting data is available in the online version of the journal at http://www.infotech.ac.cn.
[1] Zhu Guang. Program Code.txt. Watermarking algorithm related code.
[2] Zhu Guang, Feng Mining. Transparency Comparison Data.xls. Transparency experimental data.
[3] Zhu Guang, Feng Mining. Robustness Comparison Data.xls. Robustness experimental data.
[4] Zhu Guang, Feng Mining. Real-time Performance Comparison Data.xls. Real-time performance experimental data.

Note: Figure translations are in progress. See original paper for figures.