J. Vis. Commun. Image R. 42 (2017) 161–172

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

A practical design of digital watermarking for video streaming services ☆

Po-Chyi Su [a], Tien-Ying Kuo [b,*], Meng-Huan Li [a]

[a] Dept. of Computer Science and Information Engineering, National Central University, Taoyuan, Taiwan
[b] Department of Electrical Engineering, National Taipei University of Technology, Taipei, Taiwan

ARTICLE INFO

Article history:
Received 18 March 2016
Revised 8 September 2016
Accepted 26 November 2016
Available online 28 November 2016

Keywords:
Digital watermark
Videos streaming
Digital rights management
Copyright protection
Tracking

ABSTRACT

A practical design of digital watermarking for video streaming services is proposed in this research. The information of a legitimate recipient is represented as a watermark, which is embedded in the video stream to serve as a cue to trace the recipient in case a clone of the video is illegally distributed. The watermark signals are designed to embed in some areas of video frames to benefit the video stream server, as the result of only partial actions required, including decoding, processing and re-encoding. The invariance of feature points and the self-similarity of hidden signals are further exploited to enable watermark detection without involving the original video. The watermark can decently survive transcoding processes and geometrical modifications of frames. The experimental results demonstrate the advantages of the proposed scheme in terms of watermark visibility, capacity and detection methodology.

1. Introduction

Nowadays video streaming services become increasingly popular as richer varieties of media data, such as news, entertainment and educational contents, are widely accessible to viewers. Video viewers are surely pleased with such convenient services over network, even if they may pay subscription fees for commercial contents of videos. Lucrative markets with new business models of video streaming commerce can thus be created. However, the concerns about illegally spreading copyrighted videos are raised, which keep the content owners/creators from adopting the technology of video streaming, and will limit its scope of applications.

Digital Rights Management (DRM) [1] is considered an important mechanism to protect the copyright of videos and ensure the applicability of video streaming. DRM can encrypt and protect video contents via cryptographic techniques before transmission. The right of conditional access is granted to legitimate recipients with decryption keys for descrambling videos to watch at the receiver end. Nevertheless, if certain recipients break the rules maliciously, the subscribed content could be deliberately deciphered and redistributed without any control. Digital watermarking [2] is proposed as a remedy for the deficiency of conditional access in DRM. A digital watermark is an imperceptible signal embedded into multimedia data carrying the necessary information related to owners, users or contents. Since the digital watermark is embedded and tied closely with the media, it can serve as the final line of defense when the cryptographical tool of DRM fails. One function of digital watermarking is tracking which recipient illegally distributes the copyrighted media [3]. A possible scenario is described as follows. Before transmitting a copyrighted video to a legitimate recipient, the content owner embeds the identity of the recipient into the video as a watermark. The watermark is not sensible to viewers or recipients since it is embedded in an imperceptible way complying with the human perceptual system. The watermark can be detected by computing devices, and the information of it can be extracted to distinguish a large number of potential users. The embedded watermark is hard to be removed and should resist content-preserving video processing, such as transcoding, geometrical transformations of frames, and temporal modifications, etc. Once an illegal copy is found on the Internet or any storage devices, a unique watermark can be detected from it to unambiguously trace the origin of illegal distribution. This strategy can intimidate recipients' intention of spreading the contents around if they know that such a mechanism exists.

Since digital videos are always compressed before transmission or storage, it is preferable to directly apply digital watermarking to the compressed video bit-streams. The earliest work may be traced back to the research of Hartung and Girod [4], who analyzed the design criteria of digital watermarking in raw and compressed videos. Various watermarking schemes tailored to MPEG-2 [5–11], MPEG-4 [12–14] and H.264/AVC [15–19] were also proposed with varying target applications, including copyright declaration, hardware control, broadcast monitoring and content authentication. Such issues as robustness, perceptual quality,

☆ This paper has been recommended for acceptance by Zicheng Liu.
* Corresponding author.
E-mail address: tykuo@ntut.edu.tw (T.-Y. Kuo).

http://dx.doi.org/10.1016/j.jvcir.2016.11.018
1047-3203/© 2016 Elsevier Inc. All rights reserved.

capacity and false detection are taken into consideration in these methods to meet the associated requirements. Although it is possible to directly modify these algorithms to develop a watermarking scheme for tracking the recipients, some challenges still exist. First, many existing schemes are designed to operate with the raw video frames, but the availability of which could be a problem in streaming services. Most video owners obviously treasure their raw contents very much, and they are always reluctant to give away the valuable raw data to the streaming services, let alone the impractically huge size of volume.

Besides, in such applications, each video for a certain recipient will be embedded with a unique watermark, and thus each video has to be encoded and processed separately. The computational load of video server will be increased severely in proportional to the number of recipients. Although it may be possible to shift this task load from servers to receivers or set-top boxes, complexity is still an issue as the receiver is usually a resource limited device due to the cost concern. Additional loads caused by watermark embedding could vastly affect routine operations of video processing and decoding at the receivers. Embedding the watermark directly into a compressed bit-stream is certainly another more feasible approach to leverage server complexity. However, it requires more careful and complicated designs, given the fact that the issues about robustness and capacity of watermarking in compressed videos are very challenging.

In this research, we propose a practical user specific watermarking scheme for digital video streaming, in which XVID MPEG-4 is employed as an exemplar codec. In order to avoid heavy computational burden in the watermark embedding, the video stream is partially decoded for the subsequent processing to avoid large-scale transcoding. The proposed scheme employs the feature or interest point extraction to facilitate the watermark detection without involving the original video. Multiple bits can be embedded for differentiating users. Robustness against possible frame or resolution changes is considered to make the scenario of watermarking feasible. The paper is organized as follows. Section 2 presents the proposed framework and Section 3 describes the details of design. Experimental results with discussions are shown in Section 4, followed by the conclusions in Section 5.

2. Basic framework

The considered scenario in this research is illustrated in Fig. 1. The content owners provide or archive the original videos, which have been stored in compressed form. The video server will distribute the content to its subscribers, *i.e.*, User $A, B, \ldots, F$. To enforce extra control over the distributed content, the server may be responsible for embedding a watermark representing each legitimate subscriber into the video so that the videos for different subscribers, which look the same though, are actually different from each other. The other possible way is to apply the watermark embedding in the set-up box of the video receiver, *e.g.*, User C in Fig. 1. The benefit of such a strategy is that the transmitted videos for users are the same but different videos will be generated after the processing of the secured set-up box. No matter the embedding is applied in the server's or receiver's side, the complexity of embedding process has to be constrained. Now, User E in Fig. 1 chooses to illegally share the video with Users X, Y and Z. If an illegal copy is found on the Internet, the watermark extractor, which may be managed by the content owner or a third party, will help to retrieve the information of User E for tracking down the source of re-distribution.

Fig. 2 shows the flowchart of watermark embedding, which is applied by the video server as an example. The proposed design tends not to embed the signals into all the frames or every part of a frame, with the reasons described as follows. First, the watermark embedding may degrade the perceptual quality and increase the length of video bit-stream more or less so it has to applied with care when necessary. Although embedding the signals all over the video can facilitate the watermark detection, negative effects may hinder normal usage of watermarked videos. Second, if every part of the video is embedded with a watermark, the server has to prepare a unique video stream for each user. The entire operations, including data processing and transmission, will become complicated and the computational load of the stream server can be a major concern in this application. Therefore, the proposed scheme chooses to apply the scene change detection in the compressed domain to determine key frames, which will be embedded with the watermark. In these key frames, the signal is embedded into certain local areas, instead of the entire frame. This strategy helps to make "drift errors", which are caused by using different reference data generated in the watermark embedding process, less obvious to the human eyes. Furthermore, we may only process the associated data in the compressed bit-stream for the watermark embedding. In other words, the input to the embedder is a compressed bit-stream and only the data related to the information hiding will be expanded for modification.

The selection of local areas for watermarking is based on the extraction of feature or interest points, which helps to locate the same positions for the watermark embedding and detection. In the proposed scheme, the complexity in the server side is our major concern. Therefore, a better solution would be allowing the server side to select any frame and any area to embed the watermark signals and asking the watermark detector to spend

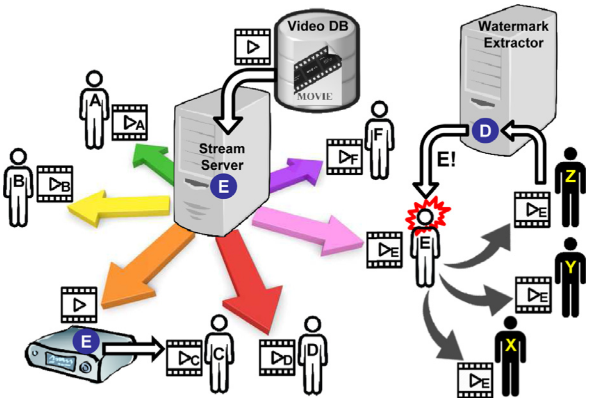

Fig. 1. The considered scenario.

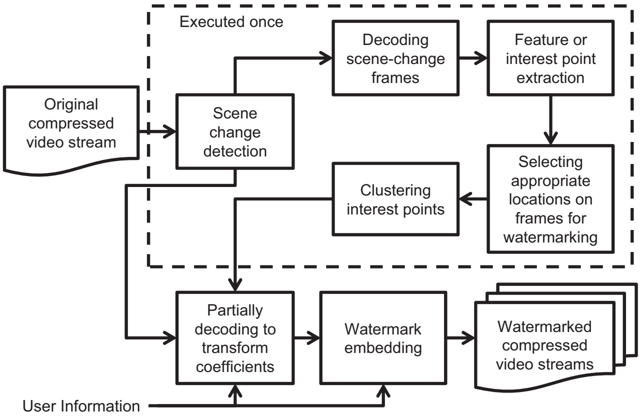
Executed once
Decoding scene-change frames
Feature or interest point extraction
Original compressed video stream
Scene change detection
Selecting appropriate locations on frames for watermarking
Clustering interest points
Partially decoding to transform coefficients
Watermark embedding
Watermarked compressed video streams
User Information

Fig. 2. The flowchart of the watermark embedding.