J Real-Time Image Proc
DOI 10.1007/s11554-013-0335-4

ORIGINAL RESEARCH PAPER

Video watermark application for embedding recipient ID in real-time-encoding VoD server

Takaaki Yamada · Michiro Maeta · Fuminori Mizushima

Received: 17 September 2012 / Accepted: 28 February 2013

Abstract A previously developed system for embedding watermarks in video content in real time has been improved by incorporating real-time transcoding, which enables embedding of watermarks specific to the recipient. That is, watermarks are used as fingerprints. When a play command is received from a customer, the system decodes the requested video content into frame images in the server. The frame images are then watermarked, encoded, and streamed to the customer in real time. Prototype testing demonstrated that use of this watermarking method is feasible for video-on-demand service; that is, up to 20 individually watermarked videos can be concurrently streamed to customers. Visibility testing showed that the quality of the watermarked images was practical to some degree. Robustness testing showed that the embedded watermarks were practically robust against encoding. Use of this system should help deter the illegal copying and distribution of video content.

Keywords Video watermark · Real-time processing · Fingerprinting · Copyright protection · Video-on-demand

T. Yamada (✉)
Yokohama Research Laboratory, Hitachi, Ltd.,
Yokohama, Japan
e-mail: takaaki.yamada.tr@hitachi.com

M. Maeta · F. Mizushima
Hitachi Government & Public Corporation System Engineering,
Co., Ltd., Tokyo, Japan
e-mail: maeta@gp.hitachi.co.jp

F. Mizushima
e-mail: mizushima-f@gp.hitachi.co.jp

1 Introduction

Digital video content can be easily distributed over the Internet due to the widespread use of broadband networks and highly efficient computers. Recent developments in network services have led to the introduction of various digital content distribution services such as video-on-demand (VoD). However, the growing availability of video content online is exacerbating the problem of copyright violation. For instance, the various video sharing services that provide a huge amount of video data worldwide is that they enable illegal copies to be distributed anonymously [1], making it difficult to prevent illegal user behavior.

This illegal copying and distribution of video content damage the sales of the original content through commercial services. One way to limit the extent of the damage is to find the illegally distributed copies and delete them so that they are not redistributed. The ability to identify illegal copiers would help deter moral users from making and distributing illegal copies. Moreover, the victimized copyright holders could make compensation claims against illegal copiers. Identifying illegal copier would thus help reduce the damage. How to identify the illegal copiers is an important issue for content distribution services, and various approaches to this problem have been investigated, including fingerprinting [2], broadcast encryption [3], and traitor tracing [4] based on coding theory.

A well-known solution to the problem is to embed the recipient's ID information into the content in the form of a digital watermark, that is, use watermarks as fingerprints [5, 22]. This solution requires creating video watermarks that are imperceptible to the human eye and robust against image processing. Many algorithms have been developed for general-purpose video watermarking in both the pixel and frequency domains [6–10].

Published online: 24 March 2013