Chapter XVI
Digital Video Authentication

Pradeep K. Atrey
University of Winnipeg, Canada

Abdulmotaleb El Saddik
University of Ottawa, Canada

Mohan Kankanhalli
National University of Singapore, Singapore

ABSTRACT

Digital video authentication has been a topic of immense interest to researchers in the past few years. Authentication of a digital video refers to the process of determining that the video taken is original and has not been tampered with. This chapter aims to provide an overview of digital video authentication systems and a universal review of the associated methods. The chapter not only establishes the importance of authenticating a video in various application scenarios; it also identifies key properties and design issues that should be considered while designing a video authentication system. The benign and tampering operations that characterize the security and robustness aspects of a typical video authentication system are described. The past works related to video authentication, based on digital signature and digital watermarking, have been described; and the emerging trends in this area of research have also been identified.

1. INTRODUCTION

The last decade has witnessed a tremendous growth in the use of digital video in various applications such as electronic media, surveillance, advertising and the entertainment industry. Digital video has many advantages over its counterpart, analog video, such as better picture quality, sharper images, better color reproduction, and better immunity to signal problems in recording. In digital form, a video can be easily transported over the Internet and it facilitates easy editing and copying. On the other hand, the ease of modifying a digital video is sometimes considered as a disadvantage since a video in digital form is so vulnerable that it can be easily tampered with.
Moreover, detecting manipulations in a video is often found difficult. This concern has generated significant interest among the multimedia research community to focus on investigating techniques for authenticating a digital video.

By definition, authentication is a process that provides some means to guarantee that the entities are who they claim to be (i.e. entity authentication), or that the information has not been manipulated by unauthorized parties (i.e. data authentication) (Menezes, 1997). In the context of multimedia, video authentication refers to a process that ascertains the integrity of a given digital video and detects if it has been tampered with in any way. In other words, a video authentication system ensures the integrity of digital video, and verifies that the video taken into use has not been corrupted.

The need for authenticating a digital video is further argued by providing the following examples:

a) In the recent years, several cases have been reported where a video recording of a political leader receiving a bribe was made public. However, in the absence of a foolproof method to authenticate the video, it is hard to trust such reports. On the other hand, criminals get away from being punished because the video showing their crime can not be proved conclusively in the court of law.

b) In surveillance camera systems, the video captured by the cameras are often used as evidence in the post-incident investigation process. In such scenarios, it is hard to ascertain that the digital video produced as evidence is the one that was actually shot by the camera.

c) In a sensitive scenario where a video is produced as a witness in the court of law, even a small alteration may not be acceptable. However, there are some scenarios where some editing also may be allowed while keeping in tact the authenticity of the video.

For example, a journalist, after shooting a video, may need to perform some editing before broadcasting it on a news channel. In such a case, a video-authentication system should be able to allow editing on the video up to a certain level ensuring the authenticity of the video.

d) A video viewer (or a consumer) who receives video through a communication channel cannot ensure that the video being viewed is really the one that was transmitted (by a producer). There may be eavesdroppers who can alter the video content intentionally to harm the interest of both the producer and consumer.

e) Video authentication is also important in an advertisement monitoring scenario where a commercial company or an individual can automatically identify, in real time, whether or not a specified TV channel is playing their video advertisement for the stipulated time. A TV channel may cut a few frames to gain more time and money.

The above examples establish that there is a compelling need that videos, wherever they are and in whatever form, should be made authentic before use.

The goal of this chapter is to provide readers with a good understanding of a typical video authentication system, its properties and design issues, and a review of video authentication techniques. An ideal video authentication must be able to detect tampering. In addition, it should also be able to localize the altered regions and recover the losses due to tampering (Celik, 2002; Sun, 2002). The tampering could be of two types: spatial tampering and temporal tampering. Spatial tampering refers to spatial attacks such as region tampering, whereas inter-frame alterations such as frame adding, replacement, dropping, or re-ordering are temporal attacks. In addition to the detection of tampering, a video authentication system should be robust to benign operations such as affine transformation and compression.