Chapter 45
Video Authentication: An Intelligent Approach

Saurabh Upadhyay
Saffrony Institute of Technology, India

Shrikant Tiwari
Indian Institute of Technology (BHU), India

Shalabh Parashar
HCL Technologies, India

ABSTRACT

With the growing innovations and emerging developments in sophisticated video editing technology, it is becoming highly desirable to assure the credibility and integrity of video information. Today digital videos are also increasingly transmitted over non-secure channels such as the Internet. Therefore, in surveillance, medical, and various other fields, video contents must be protected against attempts to manipulate them. Video authentication has gained much attention in recent years. However, many existing authentication techniques have their own advantages and obvious drawbacks. The authors propose a novel authentication technique that uses an intelligent approach for video authentication. This chapter presents an intelligent video authentication algorithm for raw videos using a support vector machine, which is a non-linear classifier, and its applications. It covers both kinds of tampering attacks, spatial and temporal. It uses a database of more than 2000 tampered and non-tampered videos and gives excellent results with 98.38% classification accuracy. The authors also discuss a vast diversity of tampering attacks, which can be possible for video sequences. Their algorithm gives good results for almost all kinds of tampering attacks.

INTRODUCTION

With the rapid development and innovation in digital information technologies, video applications are infiltrating into our daily lives at breakneck speed, from traditional television broadcasting to Internet/Intranet, wireless communication and consumer products such as VCD/DVDs and smart phones. Though this immense development in digital information technology has brought us in the new era of powerful

DOI: 10.4018/978-1-5225-3822-6.ch045

information, we are having some severe challenging issues related with the information. One of them is credibility of the information. Today, editing or modifying the content of a digital video can be done efficiently and seamlessly, and the credibility of the digital data decreases significantly (Friedman, 1993). To ensure the trustworthiness, authentication techniques (Lin & Chang, 2001; Naor & Pinkas, 1997; Perrig, Canetti, Tygar, & Song, 2000) are needed for verifying the originality of video content and preventing the forgery. Building a mechanism that enables media authenticity verification, is basically needed in court of law where digital media might be used as evidence against potential criminals. A possible scenario that justifies the need of such a mechanism is a case where a defendant claims that an incriminated media was fabricated.

So the video authentication is a process which ascertains that the content in a given video is authentic and exactly same as when captured. For verifying the originality of received video content, and to detect malicious tampering and preventing various types of forgeries, performed on video data, video authentication techniques are used.

These techniques also detect the types and locations of malicious tampering. In fact a wide range of powerful digital video processing tools are available in the market that allow extensive access, manipulations and reuse of visual materials (Hauzia & Noumeir, 2007). Since different video recording devices and close circuit television camera system become more convenient and affordable option in the private and public sectors, there is a corresponding increase in the frequency in which they are encountered in criminal investigations[1]. The video evidences have significant role in criminal investigations due to their ability to obtain detailed information from their own. And they have tremendous potential to assist in investigations. Therefore, it would be necessary to take utmost care to make sure that the given video evidence, presented in the court, is authentic.

MOTIVATION BEHIND VIDEO AUTHENTICATION

In some applications the authenticity of the video data is of paramount interest such as in video surveillance, forensic investigations, law enforcement and content ownership (Upadhyay, Singh, Vatsa, & Singh, 2007). For example, in court of law, it is important to establish the trustworthiness of any video that is used as evidence. As in another scenario, for example, suppose a stationary video recorder for surveillance purpose, is positioned on the pillar of a railway platform to survey every activity on that platform along a side. It would be fairly simple to remove a certain activity, people or even an event by simply removing a handful of frames from this type of video sequences. On the other hand it would also be feasible to insert, into this video, certain objects and people, taken from different cameras and in different time. A video clip can be doctored in a specific way to defame an individual. In the recent years, several cases have been reported where the eminent personalities of the society were caught in illegal activities in the video recordings made by so called journalists. However in the absence of foolproof techniques to authenticate the video it is difficult to trust on such reports. On the other hand criminals get free from being punished because the video (used as evidence), showing their crime cannot be proved conclusively in the court of law. In the case of surveillance systems, it is difficult to assure that the digital video produced as evidence, is the same as it was actually shot by camera. In another scenario, a news maker cannot prove that the video played by a news channel is trustworthy; while a video viewer who receives the video through a communication channel cannot ensure that video being viewed is really