Chapter 5
An Improved Fingerprinting Algorithm for Detection of Video Frame Duplication Forgery

Yongjian Hu
University of Warwick, UK, & South China University of Technology, China

Chang-Tsun Li
University of Warwick, UK

Yufei Wang
South China University of Technology, China

Bei-bei Liu
South China University of Technology, China

ABSTRACT

Frame duplication is a common way of digital video forgeries. State-of-the-art approaches of duplication detection usually suffer from heavy computational load. In this paper, the authors propose a new algorithm to detect duplicated frames based on video sub-sequence fingerprints. The fingerprints employed are extracted from the DCT coefficients of the temporally informative representative images (TIRIs) of the sub-sequences. Compared with other similar algorithms, this study focuses on improving fingerprints representing video sub-sequences and introducing a simple metric for the matching of video sub-sequences. Experimental results show that the proposed algorithm overall outperforms three related duplication forgery detection algorithms in terms of computational efficiency, detection accuracy and robustness against common video operations like compression and brightness change.

INTRODUCTION

Due to the popularity of camcorder and multimedia cell phone, digital video is more and more widely used in our everyday life and work. The rising of video sharing sites on Internet makes the spread of digital video easy and fast. The forgery of digital video is also facilitated by a variety of video editing software, which may cause serious forensic problems if the tampered videos are used in legal evidence, news reports or security monitoring tapes. Since the detection of video forgery

DOI: 10.4018/978-1-4666-4006-1.ch005

is challenged by the huge amount of digital video data, the research of accurate and rapid forgery detection algorithms is of paramount significance.

There are various ways of tampering with digital videos, inspiring a wide range of detection approaches, such as the algorithm based on compression and quantization (Wang et al., 2006, 2009; Su et al., 2011), effect of interlacing (Wang et al., 2007a), characteristic of noise (Hsu et al., 2008; Kobayashi et al., 2010), fusion of features (Chetty et al., 2010) and so on. Some algorithms detect the forgery based on the artifacts brought by tampering, such as the motion-compensated edge artifacts (Su et al., 2009), the ghost shadow artifacts (Zhang et al., 2009) and so on. Among various tampering approaches, frame duplication is a simple but the most widely used one, so the detection of frame duplication has attracted lots of attention from researchers. Wang et al. (2007b) proposed a frame duplication detection algorithm based on correlation coefficient matrix. While achieving satisfactory detection accuracy, the algorithm requires heavy computational load due to the large amount of correlation calculation. To reduce the computational cost, Lin et al. (2011) proposed to use histogram difference (HD) instead of correlation coefficients as the detection features. However, the HD features do not show strong robustness against common video operations or attacks. In practical applications, both computational efficiency and robustness must be taken into account. To satisfy these requirements, we aim at designing a fast and robust duplication detection algorithm. This work focuses on improving fingerprints representing video sub-sequences and introducing a simple metric to judge whether two video sub-sequences are matched.

The remainder of this paper is organized as follows: First, we will review two related frame duplication detection algorithms. Our proposed detection algorithm will be elaborated afterwards. Then we present the results of comparative experiment and discussion. Finally we will conclude the paper in the last section.

RELATED WORKS

Wang et al. (2007b) proposed a frame duplication detection algorithm. The video is first divided into overlapping sub-sequences, with only one different frame between adjacent sub-sequences. For each sub-sequence, they computed the correlation coefficient between each pair of frames, composing a correlation coefficient matrix that carries the temporal information of this sub-sequence. To judge whether two sub-sequences are duplicated, the correlation coefficient between the matrixes of these two sub-sequences are calculated and compared with a threshold. If the coefficient exceeds the threshold, the two sub-sequences may be duplicated. To confirm the duplication, spatial information is used for further detection. Specifically, they divided the two frames into non-overlapping blocks and calculated the correlation coefficient between each pair of blocks in corresponding positions. They recorded the number of block pairs having large correlation coefficients. If the number exceeds a predefined threshold, they considered the two frames were duplicates of each other, which indicated that the video had undergone duplication forgery. However, the calculation of correlation coefficient is known to be time consuming; and moreover, the correlation coefficient was employed twice to represent the temporal and spatial information, respectively. As a result, their algorithm requires a heavy computation load.

The algorithm proposed by Lin et al. (2011) has similar pre-processing operation to that of Wang's (2007b). The video is also divided into overlapping sub-sequences with only one different frame between adjacent sub-sequences. For each sub-sequence, the histogram difference (HD) rather than the correlation coefficient between each two adjacent frames is calculated:

$$HD = \frac{1}{N_{bin}} \sum_{i=1}^{N_{bin}} \begin{vmatrix} h_R^q(i) - h_R^t(i) \end{vmatrix} + \begin{vmatrix} h_G^q(i) - h_G^t(i) \end{vmatrix} + \begin{vmatrix} h_B^q(i) - h_B^t(i) \end{vmatrix} \quad (1)$$