Title: Detection of Inter-Frame Forgeries in Digital Videos

Authors: Sitara K., B.M. Mehtre

PII: S0379-0738(18)30280-9
DOI: https://doi.org/10.1016/j.forsciint.2018.04.056
Reference: FSI 9323

To appear in: *FSI*

Received date: 1-12-2017
Revised date: 21-4-2018
Accepted date: 23-4-2018

Please cite this article as: K.Sitara, B.M.Mehtre, Detection of Inter-Frame Forgeries in Digital Videos, Forensic Science International https://doi.org/10.1016/j.forsciint.2018.04.056

Detection of Inter-Frame Forgeries in Digital Videos

Sitara K.[a,b,*], B. M. Mehtre[a]

[a] Centre of Excellence in Cyber Security, Institute for Development and Research in Banking Technology (IDRBT), Established by Reserve Bank of India, Hyderabad, India
[b] School of Computer and Information Sciences (SCIS), University of Hyderabad, Hyderabad, India

Highlights

- Tamper footprints from spatio-temporal and compression domains are used.
- Frame shuffling detection, an unresolved problem in the literature is addressed.
- Frame shuffling is an anti-forensic approach against frame duplication detection.
- False positives in inter-frame video forgery detection due to camera zooming are reduced.

Abstract

Videos are acceptable as evidence in the court of law, provided its authenticity and integrity are scientifically validated. Videos recorded by surveillance systems are susceptible to malicious alterations of visual content by perpetrators locally or remotely. Such malicious alterations of video contents (called video forgeries) are categorized into inter-frame and intra-frame forgeries. In this paper, we propose inter-frame forgery detection techniques using tamper traces from spatio-temporal and compressed domains. Pristine videos containing frames that are recorded during sudden camera zooming event, may get wrongly classified as tampered videos leading to an increase in false positives. To address this issue, we propose a method for zooming detection and it is incorporated in video tampering detection. Frame shuffling detection, which was not explored so far is also addressed in our work. Our method is capable of differentiating various inter-frame tamper events and its localization in the temporal domain. The proposed system is tested on 23586 videos of which 2346 are pristine and rest of them are candidates of inter-frame forged videos. Experimental results show that we have successfully detected frame shuffling with encouraging accuracy rates. We have achieved improved accuracy on forgery detection in frame insertion, frame deletion and frame duplication.

Keywords: Digital multimedia forensics, Video forensics, Video tampering detection, Video forgery, Video anti-forensics, Video Compression, Frame deletion, Frame duplication, Frame insertion, Frame shuffling

1. Introduction

Availability of economical hardware and simple video processing software tools have made the task of video recording and editing effortless. A video subjected to content alteration with an intention of viewer deception is considered as a forged or tampered or doctored video. A perpetrator can easily manipulate the viewers' thoughts and decisions using a tampered video.

As data transfer rates have increased enormously and is inexpensive, circulating or sharing videos has also become easy. Nowadays, the phenomenon of "videos going viral" is very common in many of the social media platforms. Checking the genuineness of these videos is a challenge for investigating agencies and journalists. Even for a layman, ensuring the trustworthiness of a video before forwarding it to his/her peers is equally