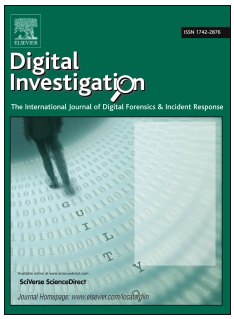
Accepted Manuscript



Detection of upscale-crop and splicing for digital video authentication

Raahat Devender Singh, Naveen Aggarwal

PII: S1742-2876(17)30010-5

DOI: 10.1016/j.diin.2017.01.001

Reference: DIIN 657

To appear in: *Digital Investigation*

Received Date: 24 January 2016

Revised Date: 20 October 2016

Accepted Date: 11 January 2017

Please cite this article as: Singh RD, Aggarwal N, Detection of upscale-crop and splicing for digital video authentication, *Digital Investigation* (2017), doi: 10.1016/j.diin.2017.01.001.

Detection of Upscale-Crop and Splicing for Digital Video Authentication

Raahat Devender Singh, Naveen Aggarwal
University Institute of Engineering and Technology, Panjab University, Chandigarh, 160014, India.

Abstract

The eternal preoccupation with multimedia technology is the precursor of us becoming a civilization replete with astonishing miscellanea of digital audio-visual information. Not long ago, this digital information (images and videos especially) savored the unique status of 'definitive proof of occurrence of events'. However, given their susceptibility to malicious modifications, this status is rapidly depreciating. In sensitive areas like intelligence and surveillance, reliance on manipulated visual data could be detrimental. The disparity between the ever-growing importance of digital content and the suspicions regarding their vulnerability to alterations has made it necessary to determine whether or not the contents of a given digital image or video can be considered trustworthy.

Digital videos are prone to several kinds of tamper attacks, but on a broad scale these can be categorized as either inter-frame forgeries, where the arrangement of frames in a video is manipulated, or intra-frame forgeries, where the content of the individual frames is manipulated. Intra-frame forgeries are simply digital image forgeries performed on the individual frames of the video. Upscale-crop and splicing are two intra-frame forgeries, both of which are performed via an image processing operation known as resampling. While the challenge of resampling detection in digital images has remained at the receiving end of much innovation over the past two decades, detection of resampling in digital videos has been regarded with little attention. With the intent of ameliorating this situation, in this paper, we propose a forensic system capable of validating the authenticity of digital videos by establishing if any of its frames or regions of frames have undergone post-production resampling. The system integrates the outcomes of pixel-correlation inspection and noise-inconsistency analysis; the operation of the system as a whole overcomes the limitations usually faced by these individual analyses. The proposed system has been extensively tested on a large dataset consisting of digital videos and images compressed using different codecs at different bit-rates and scaling factors, by varying noise and tampered region sizes. Empirical evidence gathered over this dataset suggests good efficacy of the system in different conditions.

Keywords: Digital Video Forensics; Surveillance Video Authentication; Pixel Correlation; Noise Inconsistency; Sensor Pattern Noise.

1. Introduction

Over the past few years, we have witnessed an unprecedented growth in the availability and usage of portable and inexpensive multimedia devices like mobile phones and digital cameras. Along with other more practical devices like surveillance and intelligence systems, these paraphernalia represent a few manifestations of the perpetual technological revolutions that facilitate uninhibited creation and dispensation of incredible amounts of digital images and videos. The proliferation of digital content in our everyday lives has been conducive to our dependence on this data to portray 'reality' in the fields of intelligence services, journalism, insurance claim investigations and legal proceedings. Meanwhile, convenient and highly powerful content editing software such as Adobe Photoshop, Adobe Premiere, Sony Vegas and Lightworks allow novice individuals to tamper* with digital data in numerous ways with little effort [1, 2].

More often than not, tampered digital content is virtually indistinguishable from any authentic content and can cause unimaginable damage in situations where consequential decisions are based entirely on the visual contents of digital images and videos. For instance, digital videos are increasingly being used as video evidence in the court of law and any malicious alteration in the footage being used as evidence could affect the decisions of the court, which in turn could have serious implications. Similarly, several other sensitive areas such as law enforcement, politics and defense planning stand to lose a lot from 'untrustworthy evidence'. The malleability of digital data impairs our common sense assumptions about its validity and dependability as a depiction of reality. It is therefore paramount to determine if the given digital evidence is in actuality what it purports to be, before we decide to place our faith in the legitimacy of its contents.

In this paper, we present a system that can help detect traces of *upscale-crop* (frame-level forgery) and *splicing* (region-level forgery) in digital videos. Upscale-crop is a kind of intra-frame forgery where the outer parts of video frames are cropped out so as to remove evidence of some incriminating event in those portions of the frames. Afterwards, the cropped frames are enlarged so as to maintain a consistent resolution across the entire video. Examples of upscale-crop have been provided in Fig. 1.

** Technically, a 'forgery' refers to something that is falsely made with the intent to deceive whereas 'tampering' refers to the intentional modification of structure or composition of something that would render it harmful. Albeit being subtly different, in this paper, as in the literature, these terms are used synonymously.*