International Journal of Digital Crime and Forensics
Volume 12 • Issue 1 • January-March 2020

A Novel Video Forgery Detection Model Based on Triangular Polarity Feature Classification

Chee Cheun Huang, Institute for Infocomm Research, A*STAR, Singapore, Singapore
Chien Eao Lee, Institute for Infocomm Research, A*STAR, Singapore, Singapore
Vrizlynn L. L. Thing, Institute for Infocomm Research, A*STAR, Singapore, Singapore

ABSTRACT

Video forgery has been increasing over the years due to the wide accessibility of sophisticated video editing software. A highly accurate and automated video forgery detection system will therefore be vitally important in ensuring the authenticity of forensic video evidences. This article proposes a novel Triangular Polarity Feature Classification (TPFC) video forgery detection framework for video frame insertion and deletion forgeries. The TPFC framework has high precision and recall rates with a simple and threshold-less algorithm designed for real-world applications. System robustness evaluations based on cross validation and different database recording conditions were also performed and validated. Evaluation on the performance of the TPFC framework demonstrated the efficacy of the proposed framework by achieving a recall rate of up to 98.26% and precision rate of up to 95.76%, as well as high localization accuracy on detected forged videos. The TPFC framework is further demonstrated to be capable of outperforming other modern video forgery detection techniques available today.

KEYWORDS

Frame Deletion, *Frame Insertion*, *Inter-frame Forgery Detection*, *Precision Rate*, *Recall Rate*, *Video Forensic*

INTRODUCTION

Technology advancements in computing and video processing technologies in recent years have enabled the emergence of newer and more sophisticated video editing software tools. With the fact that most of these video editing software tools can be easily accessible online at practically no cost, it is not surprising that criminal acts associated with video forgery such as on surveillance videos are increasingly becoming more prevalent nowadays.

Criminal may be using video forgery as a way to get acquitted on the basis that the video evidences presented in court could not prove that they have performed the crime at a particular time or place. In criminal court cases particularly related to sensitive or high-profile cases, it is likely that a video that is modified or edited even slightly will be deemed as unacceptable to be used as evidence in the court. It is therefore imperative that a highly accurate forgery detection system is developed to ensure the authenticity of the videos used as evidences in court.

Detection of video forgery can be classified into intra-frame or inter-frame forgery detection. In intra-frame forgery detection, the aim is to locate the forged portions or regions within the image associated with a particular video frame whereas in inter-frame forgery detection, the aim is to locate forged frames within the full video sequence (Milani et al., 2012; Kingra, Aggarwal, & Singh, 2016).

DOI: 10.4018/IJDCF.2020010102

Criminal video forgery acts are usually associated with inter-frame forgeries especially on frame insertion and deletion forgeries. This is due in part to the relative ease of performing inter-frame forgery with any basic video editing software as compared to intra-frame forgery.

This article proposes a novel Triangular Polarity Feature Classification (TPFC) video forgery detection framework for video frame insertion and deletion forgeries. The proposed algorithm has high precision and recall rates, and is considerably less complex in the system architecture design compared to other more common forgery detection systems based on optical flow consistency as detailed in Chao, Jiang, and Sun (2013) or systems based on evaluation of coding standards that usually involve more complex optimization algorithms such as those detailed in Wang and Farid (2007) and Aghamaleki and Behrad (2016). The lower complexity associated with the proposed algorithm will naturally lead to the advantage of faster processing time in authenticating video evidences in real-world court case scenarios where it is common that a large number of videos may need to be authenticated under a limited time constraint. Other important criteria such as robustness, localization capability and threshold-less system design were also considered in the proposed framework. The good performance of the system together with practical considerations of having a robust, threshold-less and computational efficient algorithm design makes the proposed approach a welcoming addition to the arsenal of algorithms available today for real-world inter-frame forgery detection.

RELATED WORK

In the following subsections, a review of the existing techniques for inter-frame video forgery detection will be presented. These techniques are broadly aggregated into three main categories; (1) camera-based detection techniques, (2) coding-based detection techniques and (3) content inconsistencies detection techniques (Milani et al., 2012; Kingra et al., 2016). Limitations and challenges associated with these techniques will be discussed in the last subsection.

Camera-based Detection Techniques

Camcorders will usually leave a trace or footprint in the recorded videos that could be used for video forgery detection. In particular, Kurosawa, Kuroki, and Saitoh (1999) demonstrated Charge Coupled Device (CCD) Fingerprint method for camera identification based on the usage of fixed pattern noise generated from dark currents on CCD chips. The video sequences however must be recorded in dark places for the method to work. Hsu, Hung, Lin, and Hsu (2008) performed correlation analysis on temporal noise residue based on Gaussian Mixture Model (GMM) technique. The approach however was designed to detect temporal copy-paste inpainting and may not be applicable for inter-frame forgery detection. Kobayashi, Okabe, and Sato (2009, 2010) evaluated video authenticity by detecting inconsistencies in Noise Level Functions (NLFs). Limitations are that they were developed to detect forgery in static scene, and any alteration of brightness of forged region in the video may affect fitting of NLF.

Coding-based Detection Techniques

Camera coding standard can introduce self-generated artifacts that can be used to aid in the video forgery detection (Milani et al., 2012; Kingra et al., 2016). Particularly, Wang and Farid (2006) performed forgery detection on doubly compressed Moving Picture Experts Group (MPEG) video sequence. As MPEG videos perform compression by partitioning video frames into Group Of Pictures (GOP) structure, the resulting motion error from inter-frame forgery will be periodic in nature, occurring in all subsequent GOPs after frame insertion or deletion point. The technique however can only be used for fixed GOP encoding and is unable to detect deleted frames with multiple GOP length. Wang and Farid (2007) performed forgery detection in interlaced and deinterlaced video by utilizing disturbance detection techniques. The approach however is computationally costly, developed mainly for intra-frame forgery detection and may not work well for low quality video. Aghamaleki