Graphics Forgery Recognition using Deep Convolutional Neural Network in Video for Trustworthiness

Neeru Jindal, Thapar University, Patiala, India
Harpreet Kaur, Thapar Institute of Engineering and Technology, Patiala, India

ABSTRACT

Doctored video generation with easily accessible editing software has proven to be a major problem in maintaining its authenticity. This article is focused on a highly efficient method for the exposure of inter-frame tampering in the videos by means of deep convolutional neural network (DCNN). The proposed algorithm will detect forgery without requiring additional pre-embedded information of the frame. The other significance from pre-existing learning techniques is that the algorithm classifies the forged frames on the basis of the correlation between the frames and the observed abnormalities using DCNN. The decoders used for batch normalization of input improve the training swiftness. Simulation results obtained on REWIND and GRIP video dataset with an average accuracy of 98% shows the superiority of the proposed algorithm as compared to the existing one. The proposed algorithm is capable of detecting the forged content in YouTube compressed video with an accuracy reaching up to 100% for GRIP dataset and 98.99% for REWIND dataset.

KEYWORDS

Accuracy, Batch Normalization, DCNN, Decoders, Doctored Video, Inter-Frame, Tampering, YouTube Compressed Videos

1. INTRODUCTION

Videos demonstrations have proved to be a productive way of sharing sentiments and thoughts. The extensive creation of reasonable-priced and portable video capturing devices, like digital cameras and cell phones, has activated a rapid improvement in the generation of visual data. Various key fields like journalism, justice courtrooms, worldwide conferences use videos as a means of communication. But the guarantee about the validation of such content can never be provided. The utilization of high-quality software tools which can easily alter the content within the videos has interrogated the genuineness of the videos so far. Hence the necessity of such a field arose which effortlessly detects the alterations in the videos if any.

Researchers in premature time came up with active forensics methods like digital watermarking or digital signatures to defend the truthfulness of visual information (Su & Li 2017). Though these methods require some early source data related to capturing forgery, so the detection becomes a challenging task. Passive forensics methods depicted our concern towards it in the past few decades. Passive clears its meaning by blindly examining the binary information with no external data required (Lin & Chang 2012). These methods proved efficient for the images but the challenge for detecting

DOI: 10.4018/IJSI.2020100106

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
doctored encoded videos stood still in terms of more accuracy and authenticity. Moreover, the forged exposure for the videos with high resolution and long length with the traditional methods showed low-performance measures and less efficient.

Deep Learning has gain recent significance in building an effective and highly accurate framework by working on large set databases. Deep convolutional neural networks (DCNN) fall in the deep research field of artificial intelligence which is largely utilized to categorize images and grouping them by means of similarity in features so extracted and finally performing further investigations within the images like object or pattern recognition, forgery detection, and localization.

This paper has focused on to improve the accuracy of inter frame Video forgery detection using DCNN. Broadly, video-forgery is of two types either intra-frame of inter-frame forgery. When the genuine contents of distinct frames are altered, it is considered as an intra-frame forgery. Some of the frames as an example of such video dataset by Image Processing Research Group (GRIP) (2018) are given in Figure 1. Whereas, in inter-frame video forgery, the alteration is done within the sequence of frames. Figure 2 shows the specimen from inter-frame forged video dataset by Reverse Engineering of Audio-Visual Content Data (REWIND) (2017).

With alteration in videos, the new relationship gets added in between the section of the original frame and that of the inserted section which helps in forgery detection (CMFD). Replicated fragments can accomplish any shape and can exist at any position, so it turns out to be computationally an expensive job to locate all possible forged frames with specific shapes and dimensions. Guo-Shiang Lin et al. (2011) cleared this idea by introducing a scheme for detecting frame duplication by finding the difference in the histogram of two end-to-end frames. The similarity of the patches is evaluated by using a block-based procedure that measures the spatial correlation of respective frames between the fake clip and the original one. Wang et al. (2007) worked on this similarity impression. They defined a matrix on the temporal correlation that symbolizes the similarities between all sets of frames in a sequence which are utilized to distinguish replicated frames from original ones in input video. This method was only able to detect static forgeries and for some videos, accuracy wasn’t appreciable.

Dai-Kyung Hyun et al. (2013) used the analogous concept of correlation and applied it on the basis of noise. They presented a forensic method to perceive modifications in surveillance videos using sensor pattern noise (SPN). The algorithm recognizes partially altered regions by omitting the high-frequency components in the given video using a scaling factor on the basis of noise correlation. But this method also focused on detecting partial static forgeries. Jie Xu et al. (2016) explained

Figure 1. Top four figures show the original frames and bottom four are forged frames from GRIP video dataset
Communication and Awareness Patterns of Distributed Agile Teams
www.igi-global.com/chapter/communication-and-awareness-patterns-of-distributed-agile-teams/135220?camid=4v1a

ART-Improving Execution Time for Flash Applications
Ming Ying and James Miller (2011). International Journal of Systems and Service-Oriented Engineering (pp. 1-20).
www.igi-global.com/article/art-improving-execution-time-flash/55059?camid=4v1a