International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Image and video forgery detection

Neeraj Chindhade

Department of Computer Engineering G. E. Society's R.H.Sapat College Of Engineering

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Computerized Videos duplicate move falsification location is a slanting theme in interactive media crime scene investigation. Securing recordings and other computerized media from altering has become a reason of concern. Video duplicate move falsification has progressively gotten a sort of cybercrime that is utilized to utilizing recordings for different malevolent purposes, for example, giving phony confirmations in court rooms, spreading counterfeit bits of gossip, utilizing it to malign an individual. A great deal of approaches have been proposed for distinguishing the follows left by any phony caused because of the duplicate move activity. Right now, we direct a review on these current methodologies which are applied for the discovery of duplicate – move recordings and furthermore for the distinguishing proof fabrication in the pictures. In a portion of the current techniques, the issue of duplicate move video fabrication has been tended to utilizing various procedures. Strategies, for example, commotion buildup, movement and splendor slopes, optical stream strategies understand just piece of the entire issue. This review examinations the current arrangements and what they offer to address this issue.

Keywords: *Information Security,Copy-move forgery detection, image forensics, segmentation, Video Forgery Detection, Temporal Tampering, Estimation, Double Compressio*

Introduction

strategies is continually expanding the trouble in recognizing the legitimate video from the altered one. For instance, Figures 1(a) and 1(b) show the casings from manufactured and unique video separately. In this fabrication, the thought process is to make an uncertainty in the passageway of the individual. A few fraud identification strategies have been proposed till date [1, 2, 3, 4, 5, 6, 7]. In the procedure proposed in [1] the fundamental thought is that, in a recompressed video the measurements of quantized or converse quantized coefficients display a deviation from that of unique video. What's more, this distinction in measurements is used to recognize twofold pressure. In [2, 3], commotion attributes are utilized to identify phony. In [4, 6] the creators present a strategy to identify twofold pressure by catching vacant receptacles displayed in the circulation of quantized coefficients in a recompressed video. In any case, the method proposed in [6] can just identify a twofold compacted I outline in factor bit rate mode just for example steady quantization scale factor. In [5], the creators utilize fleeting and spatial relationship all togetherto distinguish duplications. The methods proposed in [1, 4, 6] can't distinguish in the event that one or on the other hand more B or P outlines are bona fide or fashioned. This is especially important, as in situations, for example, video observation, eReplaceable Image File position (EXIF) is a metadata header containing shot-related camera settings, for instance, opening, introduction time, ISO speed, etc. These settings can impact the photo content from different points of view. We explore the basic EXIF-Image association and propose a novel model, which partners picture true uproar features with a couple routinely used EXIF features [6]. By arranging each EXIF feature as a weighted mix of different picture quantifiable commotion features, we initially select a diminished picture true disturbance feature set using back to back floating forward assurance [7]. The shrouded relationship as an game plan of backslide loads is then disentangled using a least squares game plan. With the progress of photo adjusting gadgets, electronic changes of cutting edge pictures for misdirecting purposes transform into a straightforward task. Existing tackles picture change acknowledgment have picked up a lot of thought in the late years. Various sorts of picture regularities began from different pieces of cutting edge still camera (DSC) system have been shown and perceived for criminological purposes, for instance, chromatic variety [1] in optical system, we examine a novel connection between's image verifiable disturbance features and Exchangeable Image File position (EXIF) header features for recognizing picture control.

Literature Survey

- According to the application requirements of authenticity and integrity of video sequence, the research topic of video objects removal detection and localization is discussed. We propose a three step framework for the purpose of locating the tampered objects in video sequences with a moving background which is captured by a moving camera. At the end, we give out the research challenges.
- Digital technology enabled tampering of digital videos much easier using sophisticated image/video editing software. As a result, the integrity of image/video content can no longer be taken for granted and a number of forensic related issues arise paving the way for many security concerns. So detection of video forgery has become a critical requirement to ensure integrity of video data. A video forgery detection and localization method based on statistical moment features and normalized cross correlation factor is proposed. The features from predictionerror array are calculated for each frame block (set of a certain number of continuous frames in the video). The normalized cross correlation of those features between duplicated frame blocks will be high as compared to other non-duplicated ones. By using calculated threshold, based on mean-squared error, the duplication is confirmed. The location of duplicated block is also found using the algorithm. Compared to existing video forgery detection results, better true positive rates are attained.
- Nowadays videos are widely used in every aspect of society such as transport, security, justice identification and so on. Thus, the authenticity and integrity of video are very important. This paper proposes a new method to detect forgeries of video with statics background. In general, adjacent frames in a video with the same background have strong correlation. If the video being tampered, the continuity of the frames correlation will be disturbed. In this method, pixel lines are obtained by intercepting the sequence of video frames in the horizontal or vertical direction. Every four continuous pixel lines make up a pixel belt. Then, by using the histogram intersection method, the correlation between pixel belts will be calculated. The simulations show that if the video tampered, there will be outliers exist in the correlation coefficients. Simulation results demonstrate that the method of this paper can detect the forgery and locate its position.
- Double compression detection is a predominant problem in video forensics. Due to the rapid growth of image/video editing software and multimedia sharing websites, it has become extremely easy to manipulate multimedia data, many times done with malicious intention. One such problem is an intentional modification to videos by carrying out recompression of its (selective) frames. In this paper, we present a forensic solution to detect double compression based forgery in MPEG videos (one of the most commonly used video formats in today's date) as well as to localize the exact region of tampering within the frames. We present a deep learning architecture for the above, which utilizes the video I-frames and the artifacts introduced into those due to double quantization. The proposed method is evaluated using a publicly available standard video dataset to demonstrate the experimental results. Our experimental results prove the efficiency of the proposed technique.
- Technological advancement of various video and image processing tools has made tempering of digital video easy and faster. This review paper focuses on passive techniques that are employed for detecting forgeries in a digital video. Passive forgery detection techniques are methods used for detecting the authenticity of a video without depending on pre-embedded information. The techniques exploit the use of statistical or mathematical properties that are distorted as a result of video tempering for forgery detection. Passive video forgery detection approach has a great prospect in multimedia security, information security and pattern recognition. In this paper, we divide passive techniques for video forensics into three categories; Statistical correlation of video features, frame-based for detecting statistical anomalies, and the inconsistency features of different digital equipment. The discussion also covers the trends, limitations and idea for improvements of passive forgery detection techniques.
- In this paper, we propose a novel technique to detect double quantization, which results due to double compression of a tampered video. The proposed algorithm uses principles of estimation theory to detect double quantization. Each pixel of a given frame is estimated from the spatially colocated pixels of all the other frames in a Group of Picture (GOP). The error between the true and estimated value is subjected to a threshold to identify the double compressed frame or frames in a GOP. The advantage of this algorithm is that it can detect tampering of I, P or B frames in a GOP with high accuracy. In addition, the technique can also detect forgery under wide range of double compression bitrates or quantization scale factors. We compare our experimental results against popular video forgery detection techniques and establish the effectiveness of the proposed technique
- Now a day's, digital pictures and video (recordings) hold high signiflcance since they have turned into the fundamental wellspring of data. With video and picture altering tools made it simple to altering of media content The prerequisite of validating the honesty of contents of digital videos ranges from a person to associations, barrier and security setups to law authorization organizations. So, there is need of researching viable video forgery detection procedures. In this paper, there is an outline of forgery detection techniques that have been proposed in the literatura and also there is a comparative studies of surveyed techniques and goes for featuring the difficulties and brings out opportunities in the field of forgery detection.

• This paper presents a method to automatically and efficiently detect face tampering in videos, and particularly focuses on two recent techniques used to generate hyperrealistic forged videos: Deepfake and Face2Face. Traditional image forensics techniques are usually not well suited to videos due to the compression that strongly degrades the data. Thus, this paper follows a deep learning approach and presents two networks, both with a low number of layers to focus on the mesoscopic properties of images. We evaluate those fast networks on both an existing dataset and a dataset we have constituted from online videos. The tests demonstrate a very successful detection rate with more than 98 percent for Deepfake and 95 percent for Face2Face.

System Architecture / System Overview

Advanced recordings have become a significant part of our lives of late, from an individual critical to observation recordings which can be introduced in a court as a proof now.

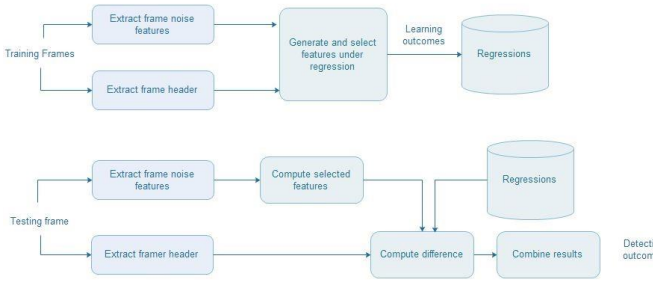

Fig. 1. System Architecture

This video proof can be significant for the official courtroom and the agents to comprehend the occasions as they happened. According to the chart we have to transfer the video then our framework will separate the clamor and headers from the edges ,after that the relapse procedure happen because of which we came to realize the that video is imitation identified or not. At that point the ouput is show to client. Video Forgery Detection is a significantly emerging discipline in Image Processing that acts as a countermeasure to intentional misuse of visual data like videos and different digital editing tools.Video Forgery Detection's aims to establish the authenticity of a video and to expose the potential modifications and forgeries that the video might have undergone. Undesired post processing operations or forgeries generally are irreversible and leave some digital footprints. Video forgery detection techniques scrutinize these footprints in order to differentiate between original and the forged videos. When a video is forged some of its fundamental properties change and to detect these changes is what is called as Video Forgery Detection techniques used for. Thus it is the scientific understanding and skill required to amplify and authenticate
video recordings.

Algorithm

The proposed system first train a machine learning model to preprocess the dataset of videos.

• Data collection and training: The first module deals with the code(algorithm) to import the video and process it (into grayscale) for which a learning model is used. The Logistic regression is used to create the model for training the data sets. The data sets are collected from Surrey University Library for Forensic Analysis (SULFA) and then trained.

Applying Optical Algorithm to determine consistency and feature extraction: After conversion into grayscale we apply the optical flow algorithm to determine the consistency in the frames. Also the image block processing concept is used for breaking the frame in a smaller size for edge detection.

• Applying GLCM and clustering the features: The third module consists GLCM algorithm to do the texture analysis and determining any tampering in the video frame.The K-nearest neighbour algorithm is used for classification
and clustering of video frames that are similar.

• Predicting if the video is forged or not: The fourth module uses deep learning algorithms like SVM, Na¨ıve bayes are used for prediction of whether a video is forged or nonforged.

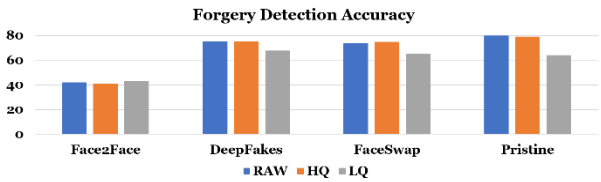

Fig. 2. Forgery Detection Accuracy

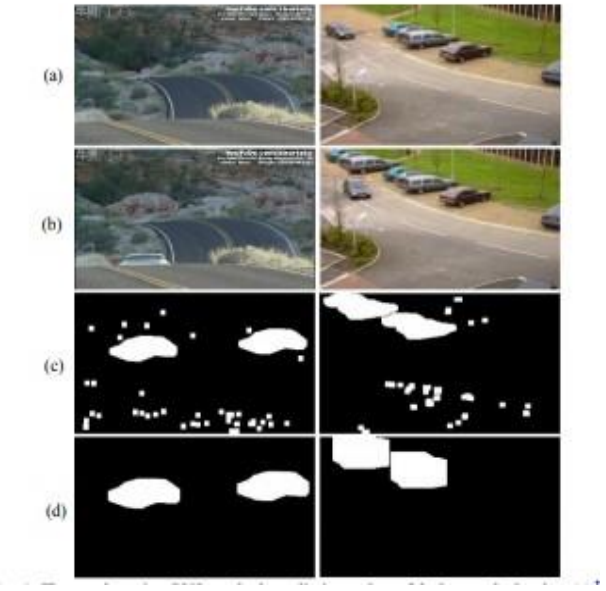

Fig. 3. Detection outcomes

Video imitation and other sight and sound falsification procedures has impacted the quick ascent in a wide range of attainable changes which is in business, in particular edge eradication, outline consideration and packing of recordings. Duplicate move fabrication is additionally a piece of these adjustments that is turning out to be normal nowadays. It is generally straightforward in its activity, yet to perceive duplicate move fabrication since they moved items and edges have a place with a similar video. Various types of procedures have been executed also, conveyed to perceive any sort of edge duplicate move phonies, it is named picture trademark based and video trademark based. The calculations that are a piece of computerized picture trademark based recognize and afterward chip picture normal for each casing to distinguish connection counting dim qualities, surface, clamor and various methods of shading.

Existing System

Computerized video crime scene investigation targets approving the validness of recordings by recuperating data about their history. In a duplicate glue imitation, an area from a video is supplanted with another locale from a similar video. Since the duplicated part originate from a similar video, its significant properties, for example, commotion, shading palette and surface, will be good with the remainder of the video and in this way will be progressively hard to recognize and distinguish these parts. framework pack the edge and optical stream is utilized to distinguish the progression of the moving items and the falsification object. In any case, the filter strategy is utilized to distinguish the key highlights of the first casing and the phony casing.

Mathematical Model

- System Description :

S = (I,O,F)
Where,
S = System
I =(V) are set of Inputs
Where ,
V = Videos
O = (O) are set of outputs
Where ,
O = Forgery Detection and location
F = (EV , FX , OL , PP)
Where ,
EV = Extract Frames from input videos
FX = Features extractions like DCT ,DWT …etc
OL = Overlapping block matching
PP = Post processing

- Success Conditions :

Video Forgery detection , Location details, Proper database.

- Failure Conditions : Video corrupt , internet connection

Conclusion

A perfect duplicate move falsification discovery calculation ought to be ready to find some kind of harmony between the effectiveness, vigor also, materialness under various degrees of imitation. In the study, we surveyed the systems different imitation identification procedures. The proposed framework manages identification of Video fabrication location. This strategy guarantees that any sort of phony or altered video is distinguished rapidly and recognized as a fashioned video. In recently proposed methods like utilizing commotion relationship, brilliance angles and watermarking the calculations just tackled piece of the issues as for video imitation. Utilizes Deep learning calculations to find some kind of harmony between proficiency, strength and appropriateness. The present calculation is material to just recordings. In the future this can be reached out to pictures, sound clasps and so on.

References

[1]. H. Yin, W. Hui, H. Li, C. Lin, and W. Zhu, "A Novel Large-Scale Digital Forensics Service Platform for Internet Videos," IEEE Transactions on Multimedia, vol. 14, pp. 178-186, 2012.
[2]. . Stutz, F. Autrusseau, and A. Uhl, "Non-blind structure-preserving substi-¨ tution watermarking of H. 264/CAVLC inter-frames," IEEE Transactions on Multimedia, vol. 16, pp. 1337-1349, 2014.
[3]. M. Kobayashi, T. Okabe, and Y. Sato, "Detecting Video Forgeries Based on Noise Characteristics," in Advances in Image and Video Technology,Third Pacific Rim Symposium, PSIVT 2009, Tokyo, Japan, pp. 306317,2009.
[4]. S. Milani, M. Fontani, P. Bestagini, M. Barni, A. Piva, M. Tagliasacchi,et al., "An overview on video forensics," APSIPA Transactions on Signal and Information Processing, vol. 1, pp. 1229-1233, 2012
[5]. X. Feng, I. J. Cox, and G. Doerr, "Normalized energy density-based forensic detection of resampled images," IEEE Transactions on Multimedia, vol. 14, pp. 536-545, 2012.
[6]. S. A. H. Tabatabaei, O. Ur-Rehman, N. Zivic, and C. Ruland, "Secure and robust two-phase image authentication," IEEE Transactions on Multimedia, vol. 17, pp. 945-956, 2015.
[7]. M. Kobayashi, T. Okabe, and Y. Sato, "Detecting video forgeries based on noise characteristics," in Advances in Image and Video Technology,ed: Springer, pp. 306-317, 2009.
[8]. C.-C. Hsu, T.-Y. Hung, C.-W. Lin, and C.-T. Hsu, "Video forgery detection using correlation of noise residue," in Multimedia Signal Processing, 2008 IEEE 10th Workshop on, pp. 170-174, 2008.
[9]. W. Wang and H. Farid, "Exposing digital forgeries in video by detecting double quantization," in Proceedings of the 11th ACM workshop on Multimedia and security, pp. 39-48, 2009.
[10]. W. Chen and Y. Shi, "Detection of double mpeg compression based on first digit statistics," Lecture Notes in Computer Science, Digital Watermarking, vol. 5450, pp. 16-30, 2009.
[11]. J. Yang, T. Huang, and L. Su, "Using similarity analysis to detect frame duplication forgery in videos," Multimedia Tools and Applications, pp.119, 2014.
[12]. Y.Xu,M.Zhou,W.Meng and L.Ma, "Optimal KNN Positioning Algorithm via Theoretical Accuracy Criterion in WLAN Indoor Environment," IEEE Global Telecommunication Conference, Miami,FL,USA, Dec 2010: 1-5.
[13]. W. Wang and H. Farid, "Exposing digital forgeries in video by detecting duplication," in Proceedings of the 9th workshop on Multimedia security, pp. 35-42, 2007.
[14]. A. V. Subramanyam and S. Emmanuel, "Video forgery detection using HOG features and compression properties," in IEEE International Workshop on Multimedia Signal Processing, pp. 89-94, 2012.