Applied GIS

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

Unsupervised video file container forensics analysis using a novel technique

Mr. D.Sathyamurthy[1]Ms. R.Atchaya[2]Ms. V.Ghouthiya[3]
Assistant professor[1,2,3],
MRK Institute of Technology

***Abstract*—** As technology for editing movies improves, it's simpler than ever to make changes to digital recordings. Verifying the legitimacy of videos is a growing area of study in the realm of information security. The study of video forensics focuses on identifying the characteristics that set authentic videos apart from their fake counterparts. This allows viewers to verify a video's legitimacy before watching it. Copy-move detection and inter-frame tampering detection form a kind of differentiating approach that is increasingly in demand in the field of video forensics. With the rise of malware that allows anybody to publish, download, and exchange anything online (including music, photos, and video), the prevalence of video forgeries on the internet has skyrocketed. Some examples of multimedia software and applications used to alter or edit media files are Video Editor and Adobe Photoshop. Video editing techniques that include inserting or erasing things from the frame are also often used in malicious video forgeries. In this research, we provide an improved method for detecting video forgeries using frame-by-frame feature extraction and matching against the genuine video, a technique known as Scale Invariant Feature Transform (SIFT). First, the image's keypoints are identified and then a SIFT descriptor, a multi-dimensional feature vector, is created for each one. Then, the distance between the describing terms is used to pair the relevant details. While this approach is effective, it is only suitable for detecting copy move assaults. We can offer data on the overall forgery rate and pinpoint the intended target frame. And include image processing into the architecture of the application as a window-based program.

Index Terms— Anti-Video Forgery Techniques: Feature Extraction, Reference Frames, Query Frames, and SIFT Features

INTRODUCTION

Evidence discovered in digital devices and storage mediums is the focus of computer forensics, often known as computer forensic science. To detect, preserve, retrieve, analyze, and communicate facts and views regarding digital information, computer forensics examines digital data in a forensically sound way. Computer forensics is often linked with the investigation of various forms of cybercrime, but it may also be utilized in civil trials. The field is comparable to data recovery in many ways, but it also incorporates specific rules and procedures meant to leave a paper trail in court. The rules and procedures for handling digital evidence are often applied to computer forensics investigation evidence as well. It has been employed in many high-profile cases, and its reliability is increasingly recognized by courts in the United States and Europe. Passive and active recording devices are widely used to collect digital video evidence. A passive recording system is one that doesn't keep any data in its recording device's memory. The term "active recording system" refers to a recording that may save data to its internal memory. A hard disk drive (HDD), solid-state drive (SSD), or volatile (flash) memory is often used to manufacture active recording devices. Digital video recordings may be made in the following formats on video

recorders:

Open source format: An open source format is a file format for storing digital data, defined by a published specification usually maintained by a standards organization, and which can be used and implemented by anyone.

Proprietary format: A proprietary format is a file format of a company, organization, or individual that contains data that is ordered and stored according to a particular encoding-scheme. This scheme is designed by the company or organization to be secret, such that the decoding and interpretation of this stored data is easily accomplished only with particular software or hardware that the company itself has developed. These formats are more common when video evidence is extracted directly from the system that created it, because they are a more secure and higher quality formatting. These proprietary formats also contain digital information like Meta Data and Telemetry Data that can assist a video forensic investigation.

Courtroom ready format: A copy of the video recording that is easily playable in a court of law using a computer, projection system, or large television. This digital format today should be tested on the system that it will be played through prior to presentation in court. Often times this format is deliverable in the form of a flash drive, DVD or Data Disc. Although the playable copy will be encoded in a common video format (MP4, AVI, WMV) it still may require a freeware player like VLC player or DVD playback software to advance frames as well as play or decode smoothly. Forensic video analysis and authentication is the scientific processes performed by a trained video forensic expert in order to determine events that occurred at the time of the video recording. CCTV cameras do not see the same as the human eye. Some of the video recordings we examine in our lab have been altered either with malice or unintentionally using processes that alter the integrity of the evidence. As video forensic experts we help our client attorneys understand any anomalies in the video recording we are asked to analyze and perform several scientific tests to determine the nature of any anomalies. The existence of digital video and digital image editing tools has made it challenging to accurately authenticate multimedia content. The current manipulation technique and the dynamic multimedia technology evolution made it possible even for a novice to easily delete an object from a video sequence, or add an object from another video source, or insert an object developed by graphics software designer. It has become complicated to comprehend and differentiate an authentic video from a tampered one. The basic layout forgery detection is shown in fig 1.

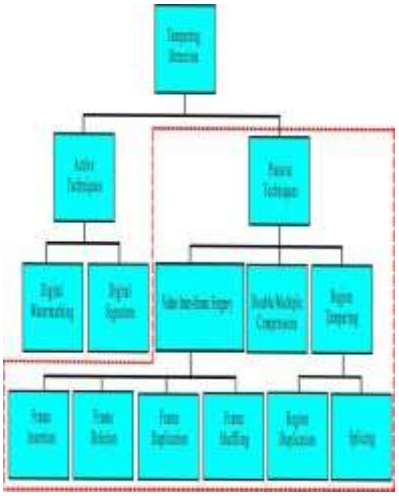


Fig 1: Tampering detection techniques

I. Related Work

A innovative, large-scale Digital Forensics Service Platform (DFSP) capable of identifying illicit material in online films was conceived, created, and deployed by Hao Yin et al. [1]. To analyze the massive amounts of Internet videos in real time, we propose a distributed architecture that makes use of a Content Delivery Network (CDN). In order to schedule jobs in the DFSP effectively, we present a CDN-based Resource-Aware Scheduling (CRAS) method that takes into account resource characteristics including latency and computation load. Integrating a content delivery network's (CDN's) distributed architecture and CRAS algorithm with a massively parallel video detection method, we launch and assess the DFSP system in the wild. The platform's efficiency was confirmed by our testing findings. Existing forensics systems have not yet explored how to determine the legality of widespread Internet films in real time, instead focusing on how to cope with robustness and identification accuracy. Fewer research have been published on the efficiency and scalability for large-scale video content identification, with most

ISSN: 1832-5505
Vol-8 Issue-03 July 2020

efforts instead going toward finding solutions to these issues from the standpoint of video retrieval algorithms.
Stutz, Thomas, et al. [2] Has been investigated thoroughly and is of significant interest owing to its vast application in the context of DRM (digital rights management). This study introduces a revolutionary H.264 CAVLC watermarking approach called replacement watermarking, which enables watermarking to be implemented via easy and effective bit substitutions of the compressed bit-stream. Furthermore, our approach is structure preserving, which means that it accurately maintains the length of the bit stream and even of the smaller units comprising the bit stream. In the context of H.264, the phrase "structure preserving watermarking" refers to watermarking methods that maintain the same length of network-abstraction layer units (NAL units / NALUs) between the watermarked and unwatermarked versions of a file. Blu-Ray watermarking relies on the structural integrity of H.264. The duration preservation is needed since the video needs to fit on a Blu-Ray disk. Production and presentation often use byte-based addressing techniques, such as the meta-data on Blu-Ray discs, therefore it's important that the underlying structure remains intact. Blu-ray players use byte-based addressing (BD-J) to access supplementary internet material that might enrich the display.

Feng Xiaoping et al. [3] tried to figure out how many times a signal was processed and how they were changed. Such data may be used to verify the integrity of a signal or spot any tampering. Multimedia forensics may be done in two major ways: actively and passively. To aid in forensic analysis after the fact, active forensics focuses on changing the multimedia signal before it is broadcast. Active forensics may be shown in the use of digital watermarks. Active forensics is restricted by the fact that watermarks must be included in content creation equipment like cameras, sensors, and microphones. In the absence of such tools, active forensics is rendered useless. In contrast, the signal is not altered in any way before passive forensics is used. Therefore, passive forensics may, in principle, be used in more settings. To identify resampled photographs, we suggest a novel technique.The technique uses the normalized energy density inside windows of varied sizes in the second derivative of the picture in the frequency domain to produce a 19-dimensional feature vector that is then used to train a support vector machine classifier. The BOSS database was used for the experiments, and the outcomes of the experiments are published here. When compared to previous work, the proposed method shows comparable performance for resampling rates more than 1, and better performance for resampling rates less than 1. Both bilinear and cubic interpolations are tested experimentally, with results that are qualitatively comparable. The identification of resampled images corrupted by noise and JPEG compression also has results.

Subramanian et al.[4] devised methods that make it more difficult to tell a genuine from a tampered video by applying digital video editing techniques. The writers make reference to the counterfeit performed in the blockbuster film Speed by replicating the frames to conceal any action. Modifying text by copying and pasting is a simple

convincingly and without any effort on your part. In addition, spotting copy-and-paste fraud may be challenging in practice. As a result, it's not hard to imagine a scenario in which a video was faked using just a copy-and-paste technique. Intrinsic features of recorded material, however, may be utilized to spot such fakes. In this study, we use the media's native characteristics to identify instances of copy-paste manipulation. There are two types of spatial tampering and temporal tampering that may be used to the copy-paste video forgeries. Spatial manipulation involves potentially altering the content of a video by copying and pasting parts of it from one frame to another. The detection of video copy-paste forgeries is complicated by the need to establish strong representations for the video frame blocks, allowing for the identification of copied blocks even after they have been modified. Transforms like FMT have been utilized in features like SIFT that identify picture fraud. The use of normalized correlation noise characteristics or quantization parameters has been used in the detection of video counterfeiting. The robustness of features like SIFT allows them to effectively identify forgeries, although other features like SURF or HoG may also be employed for this purpose.

The use of approaches for analyzing the source of information by Chi-Man Pun et al. [5] means that the trustworthiness of digital pictures is rising up the priority list. More and more scholars have paid attention to the issue of digital image manipulation

in recent years. Copy-move forgery is a popular digital image alteration that involves pasting a copied area or regions into a different location inside the same picture. Image processing techniques including scaling, rotating, blurring, compressing, and adding noise are often used in conjunction with copy and move processes to create convincing forgeries. Some forgery detection techniques that rely on related picture features are inapplicable since the copy and move sections are copied from the same image, sharing the same noise component, color character, and other essential qualities with the rest of the image. Many anti-forgery strategies, including those that specifically target copy-move forgery, have been presented throughout the years. In this study, we offer a unique method for detecting copy-move forgeries by combining adaptive over-segmentation with feature point matching. The suggested approach combines forgery detection techniques that focus on either blocks or key points. To begin, the host picture is adaptively segmented into non-overlapping and irregular blocks using the suggested Adaptive Over-Segmentation method. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to identify the labeled feature points; this technique may roughly indicate the suspected forging locations.

EXISTING METHODOLOGIES

In recent years due to easy availability of video and image editing tools it has become a difficult task to authenticate the multimedia content. Due to the availability of inexpensive and easily-operable digital multimedia devices (such as digital cameras, mobiles, digital recorders, etc.), together with high- quality data processing tools and algorithms, has made signal acquisition and processing accessible to a wide range of users. As a result, a single image or video can be processed and altered many times by different users. This fact has severe implications when the digital content is used to support legal evidences since its originality and integrity cannot be assured. Important details can be hidden or erased from the recorded scene, and the true original source of the multimedia material can be concealed. Moreover, the detection of copyright infringements and the validation of the legal property of multimedia data may be difficult since there is no way to identify the original owner. Digital videos and images having fraudulent content are used for illegal activities. Therefore, integrity of digital content needs to be verified. This can be done by analyzing the properties of the digital media. The existing method divides the test video into frames, and partitions each frame into non-overlapping 12 × 12 sub- blocks. It applies discrete cosine transform (DCT) to each sub-block at each frame and transforms them into the frequency domain. Average DCT value for each sub-block is calculated, and a row vector is obtained from each frame that contains averaged DCT values. The obtained row vectors for each frame are then binarized. The proposed method calculates a correlation matrix from binary row vectors and

creates a correlation image for the current test video. Brighter pixels in the correlation image denote similar frames. The existing framework is shown in fig 2.

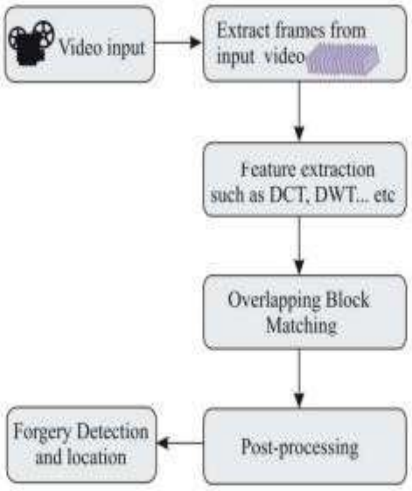
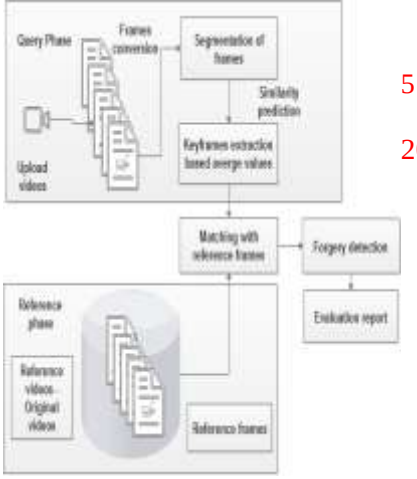


Fig 2: Existing approaches

II. PROPOSED METHODOLOGY

Presently in the digital era, our day to day life is permeated with digital video contents as one of the prominent means for communication. Developments in video technologies such as generation, transmission, storage and retrieval along with applications like Video sharing platforms, Video- conferencing etc. have served the people and society in many ways. In the terms of social, economic and scientific development, the images and videos available on various video sharing and social networking platforms like

YouTube, Face Book, Instagram etc. are of symbolic importance. Besides this, other applications like entertainment industry, video surveillance, legal evidence, political videos, video tutorials, advertisements, etc. signify their unprecedented role in today's context. As a matter of fact, videos can be generated, stored, transmitted and processed in digital format in a easy way, because of extensive use of the Internet and inexpensive and high quality cameras, computers and user-friendly editing tools. Any novice individual can utilize these techniques to make unauthorized modifications to the video content thereby affecting its integrity and authenticity. This possibility arises the need to validate whether the multimedia content available on the internet, obtained as a part of video surveillance system, or received by a broadcaster, is original or not. Thus along with the exemplary behavior of videos comes forward a gloomy side to it which is misusing or inaccurate projection of information through videos. Intentional modification or alteration of the digital video for fabrication is referred to as Digital Video Forgery. Video forgery refers to manipulating a video in such a way that it changes the content perceptually. Video Forgery can be as simple as inserting advertisements during broadcasting of sporting events or as complex as removing people digitally from a video. Video Forgery can be divided into two parts Spatial Forgeries and Temporal Forgeries. When a video sequence is captured, there is typically a great deal of redundancy between the successive frames of video. The MPEG video compression technique exploits this redundancy by predicting certain frames in the video sequence from others, then by encoding the residual difference between the predicted frame and the actual frame. Because the predicted difference can be compressed at a higher rate than a frame in its entirety, this leads to a more efficient compression scheme. Performing compression in this manner has its drawbacks, however, because error



introduced from one frame will propagate to all frames predicted from it. To prevent error propagation, the video sequence is divided into segments, where each segment

is referred to as a group of pictures (gop). Frame prediction is performed within each segment, but never across segments, thus preventing decoding errors in one frame from spreading throughout video sequence. Within each group of pictures, frames are divided into three types: intra-frames (I-frames), predicted-frames (P-frames), and bidirectional-frames (B-frames). Each gap begins with an I-frame, followed by a number of P-frames and B-frames. No prediction is performed when encoding I-frames; therefore each I-frame is encoded and decoded independently. During encoding, each I-frame is compressed through a loss process similar to JPEG compression. P-frames are predicatively encoded through a process known as motion estimation. SIFT features are extracted from gray-level image and tend to be invariant to most of the post processing methods. They are used in a variety of image processing applications ranging from medical to space based application. It is the most widely studied algorithm and also has a variety of modified versions to it.

Fig 3: Proposed framework

VIDEO ACQUISITION:

In this module, we can upload the videos that are considered as query videos. Admin can have original videos which are known as reference videos. We can convert the videos into frames at every
0.5 seconds using video file reader coding. Each frame is considered as single image.

VIDEO FEATURES EXTRACTION:

Feature extraction involves reducing the amount of resources required to describe a large set of data. When performing analysis of complex data one of the major problems stems from the number of variables involved. Feature extraction is a general term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient accuracy. In this module, we can extract the features of each frame such as color, shape of object, background features and so on. These features are extracted for future integrity checking.

SEGMENTATION OF VIDEOS:

Segmentation means grouping of frames based on video features. Video segmentation is a ways of dividing frames into meaningful segments. the context of video capture, segmentation is best applied to captured screen **presentation** that the presenter goes through slide after slide. The program compare and calculate the similarity of each video frames to consider whether there is a change in the scenery or not. If they are a change, we break the video here and finally we will break the video into shots. We assume the first frame of each shot as the key frame and output the key frame to the users.

We follow the basic idea of Color Indexing to compare the similarity of two video frames. In thismodule, key frames are extracted and stored as segmented frames.

VIDEO FRAMES CLASSIFICATION:

After segmentation, we can list out possible frames which are less than the total video frames. In this module, query video segmented frames are matched with reference segmented video frames. Similarity values are calculated based on both frames. These values are calculated based on color, shape and texture values of each frame.

FORGERY PREDICTION:

If the similarity values are not same means, video should be considered as forgery videos. Otherwise, consider as original values. If it is forgery means, predict the forgery frames from query videos.

EXPERIMENTAL RESULTS

The proposed work can be implemented as Video forgery detection framework using C#.NET as front end and SQL SERVER as back end. Based on proposed algorithm we can detect the forgery pixels in uploaded videos. The experimental results are shown in following figures.

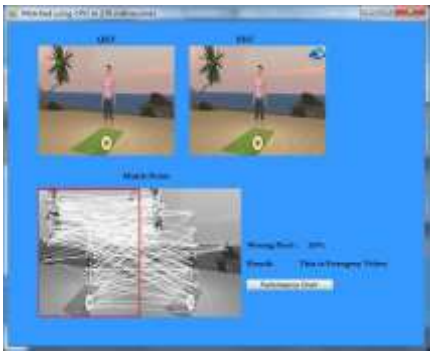


Fig 4: Frames conversion

User can upload the videos and represented as reference frames and query frames. And implement the video file reader to convert the frames at every 0.5 seconds.

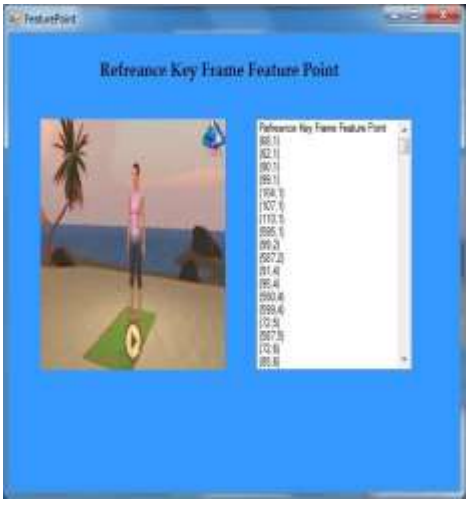


Fig 5: Features extraction in reference frames

In this frame, extract the feature points using SIFT points. Scalar features are extracted and

ISSN: 1832-5505

Vol-8 Issue-03 July 2020

pointed intoframes.

Fig 6: Features Matching (Forgery Video)

This screen describes the features as key points and Match with query and reference frames.

Finally get the wrong pixels with percentage analysis.

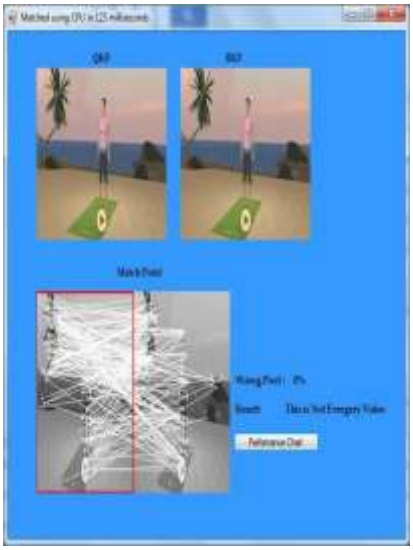


Fig 7: Features Matching (Original Video)

In this screen, display the features matching for original videos and the similarity matching can be implemented with every key point. The screen display the original videos.

Fig 8: Performance chart

The performance of the system can be evaluated in terms of time. The proposed framework analyzes the forgery frames with limited seconds than the existing framework.

CONCLUSION

The discipline of digital video forensics seeks to verify the veracity of movies by reassembling their provenance. Forging a video by replacing a section with another section of the same video (perhaps with certain modifications). Important qualities like noise, color palette, and texture will be consistent with the remainder of the video if the cloned segment is taken from the same source video, making it harder to differentiate and detect. The goal of video copy detection is to create a system for automatically analyzing videos in order to spot differences between the original and any edits.

in the midst of a mountain of video information for reasons including enforcing copyrights, keeping tabs on content, and organizing massive video archives. Digital video forensics is a new area of study that seeks to verify the veracity of films by reassembling details about their production and distribution. Natural, forgery detection, flow mapping, and source identification are four broad classes under which the main difficulties identified by the literature's researchers fall. This means that verifying the legitimacy of movies or data is often a difficult issue to solve. In this thesis, we suggest a number of innovative digital forensic methods for identifying signs of alteration in digital multimedia files. Forensic activities like detecting cut-and-

paste forgeries in JPEG-compressed movies and SIFT are accomplished with the help of segmentation-based forgery detection. Feature extraction via key point identification is important to this SIFT-based method. If a duplicate move attack occurs, this tactic is often utilized to identify the perpetrator using digital recordings (high-tech forgeries). A promising outcome, in conjunction with the departing model, has been uncovered in the suggested effort.

REFERENCES

According to [1] "A Novel Large-Scale Digital Forensics Service Platform for Internet Videos," published in IEEE Transactions on Multimedia, Volume 14, Issue 2, Pages 178-186, 2012, H. Yin, W. Hui, H. Li, C. Lin, and W. Zhu.
Non-blind structure-preserving substitution watermarking of H. 264/CAVLC inter-frames. IEEE Transactions on Multimedia, volume 16, pages 1337-1349, 2014. [2] T. Stütz, F. Autrusseau, and A. Uhl.

[3] "Normalized energy density-based forensic detection of resampled images," X. Feng, I. J. Cox, and G. Doerr, IEEE Transactions on Multimedia, volume 14, pages 536-545, 2012.

According to [4] "Video forgery detection using HOG features and compression properties," written by A. V. Subramanyam and S. Emmanuel and published in 2012's IEEE International Workshop on Multimedia Signal Processing, pages 89-94.

Reference: [5] "Image forgery detection using adaptive over segmentation and feature point matching," Information Forensics and Security, IEEE Transactions on, vol. 10, pp. 1705-1716, 2015.

"Real-time large scale near-duplicate web video retrieval," by L. Shang, L. Yang, F. Wang, K. Chan, and X. Hua, in Proc. Int. Conf. Multimedia, 2016.

"Insight and perspectives for content delivery networks," Commun. ACM, vol. 49, no. 1, pp. 101-106, 2006. [7] G. Pallis and A. Vakali.

"Video-on-Demand Networks: Design Approaches and Future Challenges," [8] F. Thouin and M. Coates.

2007 IEEE Network, volume 21, issue 2, pages 42-48

Server selection in large-scale video-on-demand systems," by N. Carlsson and D. Eager [9]

systems," ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP), volume 6, issue 1, pages 1–1, 2010.

[10] "P2cast: Peer-to-Peer patching for video on demand service," Y. Guo, K. Suh, J. Kurose, and D. Towsley, Multimedia Tools Appl., vol. 33, no. 2, pp. 109-129, 2007.