A Survey on Forensic Video Analysis

Ashwini N[1], Bhavya G[2], Vinutha K[3], Geetha Priya[4]
[1, 2, 3]Asst. Professor, Dept of CSE
[4] Dept of CSE
[1, 2, 3] BMS Institute of Technology and Management

Abstract- *Forensic evidence, audio and video recordings can offer a real-time, eyewitness account of a crime so investigators can watch or hear what transpired. A variety of technologies have their origins in digital forensics investigations. The most popular approach is to endorse or deny a claim in civil or criminal courts. Literature includes the kinds of video analysis in the precise Area. Proposed work focuses on the tampering of forensic data. Spatial manipulation strategies are adapted to modifications made to the frame relying on pixels. The system is successful in detecting even minute changes in a single or multiple frames of the given video.*

I. INTRODUCTION

Unlike other forms of forensic evidence, audio and video recordings can provide a real-time, eyewitness account of a crime so investigators can watch or hear what transpired. For instance, a surveillance video captures a bank robbery in progress, or a hidden camera records an undercover sting operation.

Forensic Video Analysis: Forensic video analysis is the scientific examination, comparison and/or evaluation of video in legal matters. This definition is attributed to American Academy of Forensic Science. It is also the preferred definition by LEVA. LEVA is the most recognized trainer for military and law enforcement agencies seeking to become certified in video forensics. Forensic video analysis has been used in a number of high-profile events, political conflicts and areas of conflict. Video forensics is required to prove that the images and videos for use in courtroom and media are verifiably accurate. Video forensics is especially relevant as media and governments use footage from places of state loss. Most of the footage from within Yemen and Syria has given rise to considerable political and public concern. Teams at the United Nations and governments around the world have used software and technological expertise to ensure that the information is reliable.

Digital Forensics: Digital forensics is a division of forensics that copes with the recovery and analysis of evidence contained in digital devices, mostly linked to computer crime. The concept digital forensics was initially used as a generic term for computer forensics but was expanded to include the investigation of all devices capable of processing digital data. Crime cases include an alleged breach of the law that is enforced by the police and charged by the state, such as murder, robbery and assault against a individual. Civil cases on the other hand deal with protecting the rights and property of individuals but may also be concerned with contractual disputes Forensic Video Analysis between commercial entities where a form of digital forensics referred to as electronic discovery may be involved. Forensics can also work in the private sector, such as internal company investigations or intrusion investigations. The technological aspect of the investigation is divided into many sub-sectors related to the form of digital devices involved; computer forensics, network forensics, forensic data analysis and smartphone forensics. In addition to finding direct evidence of criminal activity, digital forensics may be used to assign evidence to particular suspects, validate alibis or claims, assess motive, locate sources or authenticate records. Investigations are far wider in scope than other fields of forensic research, often requiring complicated timelines or theories.

Storage Data Space: Data is the collection (storing) of data in a storage medium. Examples of storage media include DNA and RNA, handwriting, phonographic recording, magnetic tape, and optical disks. Recording is done by practically any kind of energy. Electronic information storage requires electrical energy to store and retrieve information. Data collection in a physical, machine-readable format is often referred to as digital data. Software data management is one of the main features of a general purpose software. Electronic records can be stored in a much smaller space than paper. Barcodes and Magnetic

II. RELATED WORK ON VIDEO ANALYSIS

After a thorough search and evaluation of the available literature in the given project it has been selected and enhanced in the particular area. The literature review of the documents that support this system has been represented below.

Video content authentication techniques, a comprehensive survey: This paper provides a repository of information on the times of tamper attacks a video can experience and a detailed source of sources for the passive-blind techniques proposed for detection of these attacks. The area of video anti-forensics and counter anti-forensics was also examined. In addition to the study of important disadvantages and practical advantages of each strategy, the shortcomings that have to be addressed in the long-term perspective and some problems needing urgent attention have also been mentioned. Several relevant interconnected research domains, like video up-conversion, phylogeny, and re-capture detection, have also been examined. This work could not only prove useful to the researches and developers working in the field of video forensics domain to find new utilitarian ideas and identifying new research problems, but also inspire new researchers to engage in this very exciting research area of inestimable interest.

Graphcut Textures, Image and Video Synthesis Using Graph Cuts: In this paper the author has demonstrated a new technique for video analysis. The graph-cut method is suitable for computing the seams of patch sectors and for evaluating the position of patches to produce cognitively smooth video. A range of synthesis cases have been shown, including organized and random picture and video textures. We also present extensions that allow the transformation of input patches to allow synthesis variability. They have also presented an application that enables two separate source images to be dynamically combined. This method enhances the cutting edge technology in texture synthesis by having the following advantages: no limitations on the appearance of the field where the seam will Forensic Video Analysis be made, acknowledging the cost of old seams, simple generalization of the production of seam surfaces for film, and an easy form of inserting constraints.

Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System: In this paper, it was argued that it is possible to achieve digital proof relating to using the cloud storage system on the Windows 10 platform. Digital proof can be identified in the databases and log files generated by the programs, the web browser, the memory and the register. This research adds value to the challenges of the cloud, in specific by helping forensics experts map the region that has become a repository of digital evidence. Based on the trial results, the average success rate is 86% and the remainder cannot be measured, the findings depend on the various states, procedures and instruments used, and the study can be conducted easily.

Forensic Analysis of Video File Formats: This paper introduced the first systematic analysis of common video container formats by a forensic point of view. The features found complement the set of tools of forensic experts and to provide useful hints to check the validity of digital video sources. The framework of AVI and MP4 collections is not precisely specified. We have seen major variations both in sequence and in the existence of individual data segments. AVI files also contain detailed or JUNK lists. MP4-like files can use random non-standard units and parameterizations of similar atom entries. Lossless video editing keeps the compression defaults of the original video stream intact, but adds its own unique artifacts into the container file structure. Although the original source system file format idiosyncrasies are usually lost after video editing, all of the evaluated software tools have different file format signatures in our test collection. Forensic Video Analysis

Video Authentication-An Overview: In this paper, the author explains intelligent verification techniques that allow us to create a frame-by-frame relationship by using any statistical features of a frame, like corners or edge points in a frame for a particular video, and to learn if the processed video is tampered or genuine. Using this method with comprehensive survey data and use a nonlinear classifier such as SVM, we can set a kernel in a hyper-dimensional plane which can determine whether or not the video is genuine. Smart techniques are best suited to verifying raw compressed video, as these techniques do not require any computing or key storage. The main disadvantage with smart techniques is that, for even a single form of attack, a large number of repositories of tampered and legitimate video sequences are required to understand. This causes these methods to be a little slower compared to other methods.

III. EXISTING SYSTEM

In the existing this are some of the following observation done and are listed below:

- Traditionally, forensic video analysis is used for crime detection.
- But videos that are supposed to be a part of the investigation are often tampered by criminals. There are many techniques to identify a tampered video.
- Whenever there is a big change in a frame or a number of frames in the video, it can be detected. There are many techniques to detect the compression in a video too.
- The existing systems are lacking of a technique to detect a very tiny change in a single frame or multiple frames.

IV. PROBLEM IDENTIFICATION AND PROPOSED SOLUTION

The problem statement is to design and develop a smart technique to detect a change that is made in a frame of a video even if it is very small. The efficiency of the system should also be high. Hence, a technique that detects small change in a frame of a video should also use fewer resources and result in more efficiency.

The proposed system is a method to analyze a forensic video and check the actualities based on the investigative information and evidence provided. It also focuses on the tampering of forensic data. The proposed system is designed in such a way that it will be able to detect even minute changes in a single or multiple frames of the given video.

V. SYSTEM ARCHITECTURE

System architecture for the depicting methodology of the implementation is shown below:

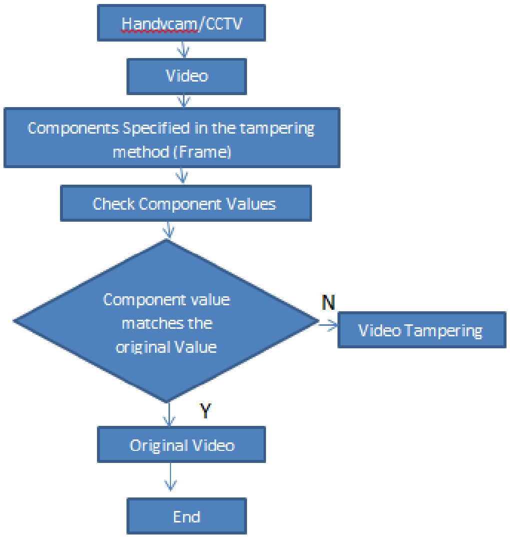

Handycam/CCTV
Video
Components Specified in the tampering method (Frame)
Check Component Values
Component value matches the original Value
N
Video Tampering
Y
Original Video
End

Fig 1: System Architecture of the Implementation

The first step is to find a video for the Close-Circuit Television (CCTV) camera, for example. Then test the value of the frame from the video. After that, unless there is a discrepancy in valuation from the test results, then perhaps the video is tampering. If the value of the variable is still the same, the video is the authentic video. The findings of the study should be understood if there are variations between frames that have encountered interference. The correlations of the general theory were the process of manipulation and the variations of the other experts to confirm the use of methods in this analysis.

VI. IMPLEMENTATION AND RESULTS

The proposed system is a method to analyze a forensic video and check the actualities based on the investigative information and evidence provided. It also focuses on the tampering of forensic data.

Development Stage: It is the phase in which case simulations are made to try to apply Video Cleaner while identifying the video footage is corrupted or not. The aim of the case simulation is to check with Video Cleaner when finding the video recording that will alter or modify the data, such that the video recording looks authentic. Changing the video that differs from its original form is a image and a photo. These adjustments can be marked as deliberate or accidental. Accidental Tampering has the criminal intent of altering information or deleting copyright. In turn, unintended tampering is the product of automated operating procedures, such as brightness enhancement, formatting adjustments, size reduction, etc. In video signals, interference strategies can be defined as spatial and temporal shifts. Spatial manipulation strategies are adapted to modifications made to the frame relying on pixels.

Detection (duplicate the same object in the same scene
Detects (inserts an object from a frame to another frame

Fig 2: Development Stage

Video Simulation Process: The simulation process begins with the preparation of the video as a tool for tampering research. The attacker will delete the proof by altering the video aimed at removing the proof. The figure explains tampering the video simulation process with attack crop, zoom, rotate and grayscale. In the original film, the assault was rendered on a photo tampering by cropping, zooming, rotating, and grayscale. After the video tampering, the local tampering process between the original clip and the video tampering will be evaluated.

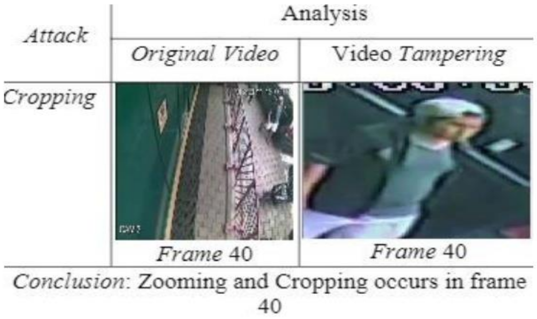
Tampering Video Illustration: The first picture on the left is a tampering method by adding images into multiple frames in the film. In the next picture to the right is a mixing mechanism by adding several frames from each video to other frames in that same video. Many techniques have been developed to detect video interference. Study done on could also detect two forms of interference. The first method is to confirm the presence of a spatial copy of a pass, or it can be duplicated to a similar event in that same scene or scenario using the comparing or lumping Histogram of Gradients (HOG).

Fig 3: Tampering Video Illustration

The stage to prove the video consists of several processes in Figure 10, namely:

1. Proof of CCTV video recordings from the operator / owner of the DVR CCTV is demanded to be captured directly and then loaded into the Tensor Investigative computer.
2. Police investigators Special DIY INAFIS DIYFIS specifically identify the video and scan the details found within.
3. Yogyakarta Regional Police of the Republic of Indonesia Authorities have started to split CCTV video footage into frames.
4. After the frame was set, the DIY Police Investigator began editing the CCTV video recording.
5. Then the Yogyakarta Regional Police of the Republic of Indonesia investigator confirmed the result by video splitting and gathering facts on the scene.

Simulation of CCTV Video Analysis: Video recording shows that the incident of car bleaching started last Sunday on the 11th of March 2018. It is clear from the CCTV video footage showed at 13:06:42 than 2 actors doing the incident 1fellow suspect carboy and tire car seal from the left side of the car, 1 peer as car razor and watched the situation began to car the left-handed car wheel and car trucking. is the front-end AMPED FIVE Ultimate 9010 application used to identify and analyze CCTV video case.



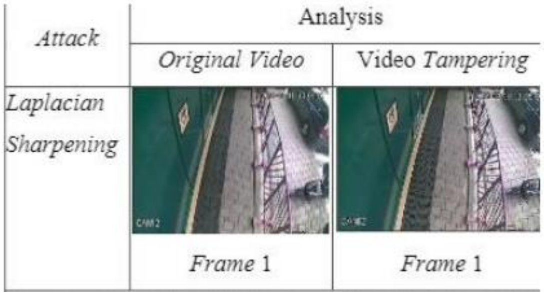
Attack	Analysis	
	Original Video	Video *Tampering*
Cropping	Frame 40	Frame 40

Conclusion: Zooming and Cropping occurs in frame 40

Fig 4: Simulation of CCTV Video Analysis

Tools that exist in the filter in this application include sharpening menu, de-noise, de-blurring etc. In the sharpen menu itself there are 2 (two) features namely Laplacian sharpening and un-sharp masking. Then on the menu de-noise, there are 6 (six) features namely Averaging, Filter, Gaussian Filter, Wiener Filter, Forensic Video Analysis Bilateral Filter, Median Filter and De-blocking. In the de-blurring menu, there are 5 features of Motion De-blurring, Optical De-blurring, Nonlinear De-blurring, Blind DE convolution and Turbulence De-blurring. It shows the main attacker to be can appear in CCTV.

Occurrence of Laplacian Sharpening: Shows that the frame detection scenario on the CCTV video recording in the case of car bundling uses the Laplacian Sharpening to process to sharpen the image of DE blurring results. In the case of car damage and tire car rupture, clarity on CCTV video footage shows the car next to the shop. In frame 1 of the table is Original video in case of car bundling and tire car tire on Laplacian Sharpening feature. In the Tampering Video table shown on the CCTV record evidence, the picture is clarified using the tampering method to provide a scenario in the case shown in frame 1 of the Sharpening Laplacian feature. By doing the tampering method, Yogyakarta Regional Police of the Republic of Indonesia investigators can find the scene or crime scene.



Attack	Analysis	
	Original Video	Video *Tampering*
Laplacian Sharpening	*Frame* 1	*Frame* 1

Fig 5: Occurrence of Laplacian Sharpening

VII. CONCLUSION

The findings show the reality in the case of the car plundering as well as the tire adjustment of the car completely-exactly the same thing and there is an accident. The proof discovered by the DI Yogyakarta Police Investigator has proven to be true. The accuracy of the evaluation in the case of CCTV of car bumping and car tire fitting according to DI Yogyakarta Police investigators who found in the field of INAFIS reported that 70 per cent of the identification of CCTV video footage and the face of the perpetrator or offender or intruder can already be processed by the investigation of the proof.The method to analyses forensic video and check the actualities based on the investigative information and evidence provided. It also focuses on the tampering of forensic data. The system is successful in detecting even minute changes in a single or multiple frames of the given video.

REFERENCES

[1] R. D. Singh and N. Aggarwal, “Video Content Authentication Techniques: A Comprehensive Survey,” Multimed. Syst, 2017.

[2] Amir Putra Justicia, Imam Raidi“Analysis of Forensic Video in Storage Data Using Tampering Method” International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(3): 328-335, 2017.

[3] A. Novianto, “Understanding and Sample Forensic Case Compiled by Graduate Program Faculty of Industrial Engineering Department Master of Informatics Engineering University of Indonesia Islam Yogyakarta,” 2014.

[4] B. Rahardjo, “Overview of Digital Forensics,” J. Sosioteknologi, vol. Edisi 29, no.FSRDITB, pp. 384–387, 2013.

[5] A. Amirullah, I. Riadi, and A. Luthfi, “Forensics Analysis from Cloud Storage Client Application on Proprietary Operating System,” vol. 143, no. 1, pp. 1–7, 2016.

[6] T. Gloe, A. Fischer, and M. Kirchner, “Forensic analysis of video file formats,” Digit.Investig., vol. 11, no. SUPPL. 1, pp. S68–S76, 2014.

[7] B. S. Putra and T. J. Pattiasina, “Study of Data Storage Analysis using Nas-Das-San,” pp. 47–54, 2012.

[8] I. Albanna, Faiz; Riadi, “Forensic Analysis of Frozen Hard Drive Using Static Forensics Method,” vol. 15, no. 1, pp. 173–178, 2017.

[9] A. Setyawan and I. Riadi, “Multimedia Application of Memory Learning Using Adobe Flash,” vol. 1, pp. 181–190, 2013.

[10] A. M. Bagiwa, “Passive Video Forgery Detection Using Frame Correlation Statistical Features,”2017