MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Anti- Forensics: The Tampering of Videos

Fayyad Kazan H[1]*, Hejase HJ[2], Moukadem I[3], Rkein H[4] and Kobeissi K[5]

[1]Information Technology – FBA, Al Maaref University, Lebanon
[2]Senior Researcher and Professor of Business Administration, Al Maaref University, Lebanon
[3]Faculty of Science, Al Maaref University, Lebanon
[4]Faculty of Business Administration(FBA), Al Maaref University, Lebanon
[5]Faculty of Sciences, IUL University, Lebanon

Research Article
Volume 6 Issue 1
Received Date: December 14, 2020
Published Date: January 18, 2021
DOI: 10.23880/ijfsc-16000219

***Corresponding author:** Hasan Fayyad-Kazan, Information Technology – FBA, Al Maaref University, Beirut, Lebanon, Email: hasanfkazan@gmail.com

Abstract

In the context of forensic investigations, the traditional understanding of evidence is changing nowadays where most prosecutors, lawyers and judges heavily rely on multimedia substantiations. However, the evolution of easy-to-use media manipulating tools, made it very easy for almost any (technical) person to alter the content of a digital media (e.g. digital image, audio or video) without leaving any traces that can be detectable by human's basic perceptions. Therefore, the validity of the digital media can no longer be guaranteed which in turn leads to a serious problem regarding digital crime investigation.

As there are tools which can tamper media, there are also ones that can do the reverse: detect the tampering. This paper sheds the light on the available anti-forensics tools. Experiments were done using some of these tools to detect tampered media – more specifically video tampering. Our experiments showed the efficiency of these tools by differentiating between original and altered evidences.

Keywords: Forensics; Evidence; Tampering; Anti-Forensics; Lebanon

Abbreviations: CCTV: Closed Ciruit Television; DVR: Digital Video Recorder; NVR: Network Video Recorder; EDR: Edge Disappearance Rate; MCEA: Motion Compensated Edge Artefacts.

Introduction

In today's era of digitization and computerization, information is mostly conveyed through digital media (video, images, audio). Recent technological developments have exponentially increased the amount of digital data (billions of images and videos) generated every day on the web and mainly on social media. The social and political impact of disseminated media on the web is unquestionable, especially with the contribution of social networks in shaping the current political and social arena. To make online news more attractive and easier to consume for public audiences, most of them are associated with numerous images or videos [1]. They represent a substantial part of the information circulated in our quotidian communications as well, e.g., newspapers and social websites. Information with multimedia content is also disseminated rapidly [1]. Adults in some Arab countries like in Tunisia (80%), Jordan (92%), and Lebanon (79%) almost agreed that even though high-tech made users more knowledgeable, it made them easier to manipulate [2]. As a result, it is increasingly important to ensure the integrity and authenticity of the vast volumes of data before using them in many situations such as courts of law.

The advancements in technology made a huge number of freely software available such as Adobe Photoshop, Pixar and Corel PaintShop, to create fake and tampered data without

being detected by the normal visual perceptions resulting in dangerous consequences. Unfortunately, they are blurring the line between real and faked multimedia content. So nowadays, "Seeing is no longer believing". This potential danger of false evidence imposes providing the authenticity of videos before they are produced as evidence in the court of law. Such operations like thorough video analysis, photo forgery and audio tampering detection lead to fruitful and authentic prosecution results.

The purpose of this paper is to rely on some experiments to show the difference between original and altered videos.

Literature Review

Tamper detection of digital media (images/videos) has been a trend in research area to establish the authenticity of media due to its great societal impact [3] provided in their paper a tamper detection technique for the images used in social media [4] provided a survey of different forging detection techniques with a focus on copy and move approaches [5] presented the analysis of the footprints left when tampering with a video sequence, and propose a detection algorithm that allows a forensic analyst to reveal video forgeries and localize them in the spatio-temporal domain. Their proposed method is completely unsupervised and proves to be robust to compression [6] presented a method to detect video tampering and distinguish it from common video processing operations, such as recompression, noise, and brightness increase, using a practical watermarking scheme for real-time authentication of digital video. Their method was easily configured to adjust transparency, robustness, and capacity of the system according to the specific application at hand [7] proposed a scheme for the reconstruction of the tampered video through watermarking. The watermark payload, which consists of highly compressed versions of key frames of the video and localization information, is embedded in the video using fountain coding. In addition to tampering localization, the proposed scheme can subsequently recover the content of the original video that has undergone malicious attacks [8] discussed a novel approach to detect inter frame and intra frame video forgery using content based signature. Their proposed STTFR algorithm aimed to verify video integrity through the creation of a 128 bit message digest from the input video of variable length that will be unique to that video and acts as a fingerprint [9] provided comparative studies of forgery detection techniques and goes for featuring the difficulties and brings out opportunities in the field of forgery detection [10] presented analysis of forgery detection techniques like inter frame forgery detection & intra frame forgery detection that can be used for video tampering detection. They also presented comparative analysis of newly developed techniques of forgery detection [11]. Proposed inter-frame forgery detection techniques using tamper traces from spatio-temporal and compressed domains.

Background

Of all the disciplines that deal with forensic science, digital forensics has the potential to be one of the most collaborative ones since it touches almost every aspect of our life nowadays. The fact that nearly every area of the current time is supported by electronic devices, like smart phones, tablets and digital cameras..., strongly contributes to the steadily increasing importance of digital evidence in crime investigation [12]. One significant element of this kind of evidence is multimedia content, which just like physical evidence, must be followed to reveal the truth behind every serious event.

Since modern life is unthinkable without multimedia and electronic data, the legal system widely recognizes the pivotal role of video, audio and pictures in the investigations and conviction of the court. Upon realizing this substantiality, recent studies show that up to 80% of the cases are forensically interpreted with the support of digital evidences including multimedia as investigative tools [13].

Eventually there is nothing more cogent to the court and the justice system in their forensic deductions than hearing an audio sent by an intimidator or looking at a burglar face in a video surveillance footage for example. However when analysis is commonly associated with multimedia techniques as forensic evidences, the main focus is on the identification of the authenticity of their content and the information elicited from due to the high possibility of tampering which might lead to injustice in the results.

Video as Forensic Evidence

Since few years, a smart-phone camera has become a common property and the spread of video surveillance cameras has widely increased due to the recognition of their role in preserving public and private security. Because of the availability of the recording equipment, an exponential progression of the use of videos as investigative tools is seen nowadays.

In many cases the only witness to a crime could be a video surveillance camera. This will serve as a key in identifying and finding a criminal or assaulter's face or soft biometrics like height, weight, etc. Was the theft alone or in a multi-person-assisted robbery? What was the model of the car through which the burglar flee? Many more questions could be answered depending on a video record which emphasize on the power of video evidence in analysing an event aiding investigation and initializing the judgment.

Despite its significance, nowadays any type of video could be exposed to tampering due to the easy-to-use and available forgery techniques which makes relying upon it unlawful if the authentication of each evidence is not tested previously to its analysis.

Eventually it is worthy to mention that there are several types of recorders used to create digital video evidences . Some of these are: [14]

- CCTV / DVR: closed-cicuit TV digital video recorder
- CCTV / NVR: closed-circuit TV network video recorder
- MDVR: mobile digital video recorder
- Body camera
- Concealed camera
- Tazer camera
- Police dash-cam

Figure 1 below shows a sample of three types of video recorders: CCTV, DashCam, and Personal phone.

Figure 1: Some types of video recordings.

Video Enhancement and Analysis

According to the circumstance, the type of recordings retrieved is unique in each case as thus its analysis and enhancement is unique as well. Though some recordings appear to be unclear and useless, the collection of every footage is a must for a forensic enhancement technique could clarify unnoticeable details in the video before its processing. Following the collection of the evidence, the model of the recording device, details about the recording system and the current time/date and that of the recorder's display must be noted by the investigator.

Basic Methods of Video Enhancement

The technology of today's video recording has evolved from analog , cassete tape recordings , to digital where information is recorded using data blocks of 0s and 1s. Whether a video evidence is analog or digital, the forensic expert early step after evidence collection must be the creation of a working copy of the video before processing it. This assures the availability of the unaltered form of the original evidence for further comparison with the processed copy.

The handling of a video forensic evidence should be carefully done where the content of the recorded data should never be changed but rather only enhanced. The employment of the video enhancement techniques is important to obtain promising results from the video analysis. Such techniques include:

- Video Stabilization: produce smooth video playback by decreasing the amount of the movement in a video
- Sharpening: clarify the edges of the pictures in the video making them clearer and more distinct
- Masking: protect witness or suspect by covering areas in the video if the record is to be published
- Interlacing: combine two television fields for producing a full frame of a video when working in analog system
- Demultiplexing: isolate each camera when multiple video signals are combined into a single signal in CCTV

Results and Findings

Amped FIVE Software for Video enhancement

In the context of video enhancement, it is very essential to shed the light on one of the most potent video enhancement softwares Amped FIVE. Along with other powerful softwares like Blackstone, this latter is on which most law enforcement surveillance and security applications, military operations, forensic labs and civil litigations mostly depend on due to its convenience, accuracy, simplicity and its capability of producing complete and rigorous outcomes [15].

In a fast, precise and simple way, Amped FIVE provides a complete solution to the video processing and analysis.

The main key element in Amped FIVE design is to maintain the integrity of the original evidence since any manipulated or doctored evidence will be absolutely excluded by the prosecutors, judges and courts.

The concept of Amped FIVE is based on filtering in which every filter takes the video generated by the previous one and the result will pass to their output filter after processing. By this strategy if any value was modified on a previous filter, this will be reflected as a modification of the final result [16]. This filtering concept is very fast and precise to guarantee high effectiveness of this software.

The features and advantages supplied by Amped FIVE are paramount through the video evidence processing and analysis. Some of these options include:

- Motion Blur Correction

Figure 2: Vehicle number before and after deburring [17].

- Background correction

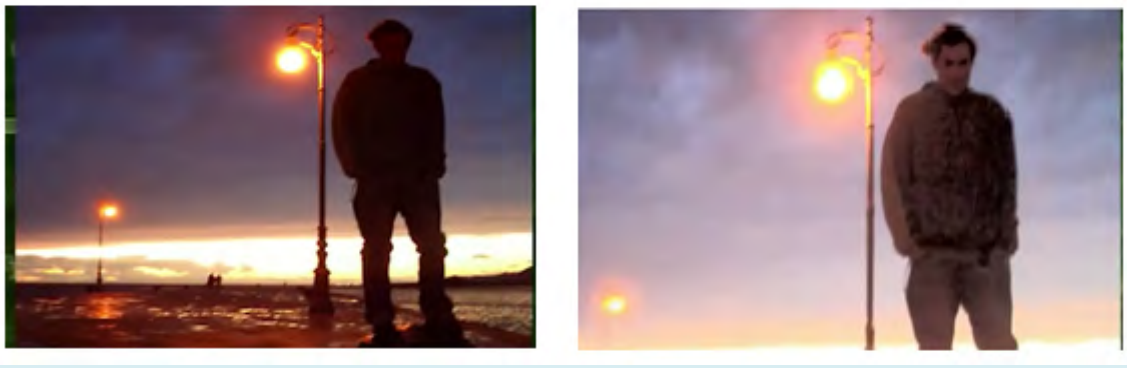

Figure 3: Background view before and after enhancement.

- Optical Debluring

Figure 4: blurred facial and words video frame before and after clarification.

- Poor wheather enhancement

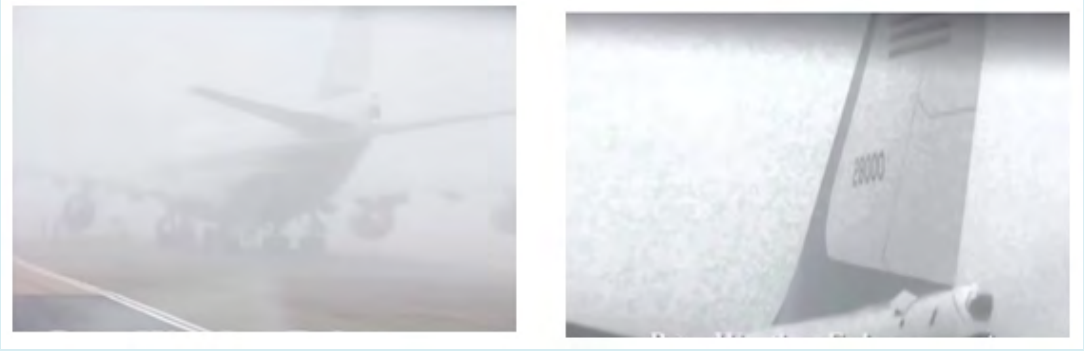

Figure 5: Airplane number before and after clarification.

Average Framing, 3D measurement, Local Stabilization and Latent Fingerprints Enhancements are also supported by Amped FIVE.

Because Amped FIVE is able to support any video format , reduces time and effort due to its fast processing, generates automatic and accurate reports and has high performance in targeting any type of data from latent fingerprints, crime scene digital videos to CCTV recordings, it has become the world's top revolutionary solution for video enhancement and analysis.

Video Tampering

The contents of digital videos and recordings serve as valuable evidences and provide crucial information that form the basis of several consequential decisions in the fields of forensic investigations. Since the initialization of the use of video evidence in the courts, its content had been considered infallible. However, the huge proliferation of the inexpensive and portable video-capture devices like digital cameras and cell phones that most people carry nowadays along with the wide spread of variety of low-cost video editing tools has led to the realization that this is no longer the case [15]. A potential danger is produced by this combination as today anyone has the ability to modify the content of a certain video at ease according to his or her wish. From here the necessity of video authentication was enlarged in order to assure the credibility of the evidence to rely on [13].

Before going into details concerning video authentication in the next section, let's shed the light on video tampering and its types.

Video tampering is the process of furtive manipulation of the content of a video [18]. This easy task is done for the purpose of changing the real meaning conveyed by the imagery in the video by concealing or altering an object or event in the video content. In general the several types of video forgeries are categorized into two: Inter-frame forgery and Intra-frame forgery [15].

Inter-frame Forgery: Tampering that modify the frames' sequence in a video [15]; this sequence can be altered by four different ways that are (Figure 6):

- Frame Insertion: adding new frames to the targeted video from different videos
- Frame Deletion: removing frames from the targeted video
- Frame Duplication: copying a sequence of frames and pasting it at another location within the same video
- Frame Shuffling: changing the order of events by changing the order of frames

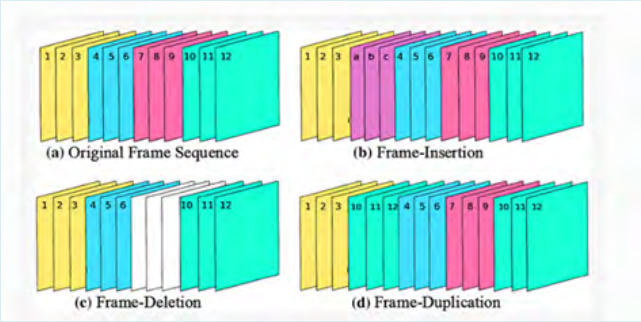

Figure 6: Types of Inter-frame forgery [15].

Intra-frame Forgery**:** Tampering that modify the actual contents of individual frames of the video in 2 ways:

A. Copy/paste or Copy/move Forgery: adding or removing a person or object to or from a scene represented in the video frames (Figure 7). It is called partial manipulation since only a small part of the frame is modified and the rest of the frame regions remains unaltered [15].

Figure 7: Deletion of video frame objects [15].

While adding an object to the scene could be simple, removing an object from the video frame does not sound so. How will the region left behind the removed part from the scene be covered so that the frame appears as a complete untouched one? This is solved by Impainting technique. This technique helps restoring the missing part and tainted region left after object deletion in the most visually plausible manner [15].

One important type within the copy/paste forgery is the Green Screening or Blue Screen Compositing. This allows changing the background in the targeted video and merging any other view or scene behind the foreground objects, as shown in Figure 8.

Figure 8: Background Alterations [15].

B. Upscale Crop Forgery: cropping specific frames of a video which allow the elimination of evidence present in a crime scene for example. To fill the gap created, enlargement of the affected frames is followed to maintain resolution consistency of the whole video.

Figure 9: Cropping objects from video frames [15].

These are all examples of how malicious video tampering is and how the created plausible video forgeries could be inconspicuous to a human eye.

Video Re-Enactment: Face2Face System

Tampering a video content by cropping a frame to hide a suspect, changing the background to alter time and location or removing an object to conceal evidence could sound familiar to a lot of people somehow. Many of the video-editing softwares like Adobe Premier, Photoshop, Light works and Cinelerra lead to results that most people expect and find simple. But what about manipulating a video in real time to alter the facial expressions and the saying of a target person?! This idea was not considered believable at first.

The existence of new kinds of face tracking softwares has taken the days when we could trust what we see in a video to an official end. The up growth of video re-enactment or face tracking algorithms like that of Face2Face led to astonishing outcomes. This latter tends to animate facial and vocal expressions of the target actor in a video by a source actor synthesizing a photo-realistic manipulated output.

Figure 10: Video Re-enactment Input and Output [19].

Face2face can be applied to any video type or format for example a YouTube video [19]. After selecting the targeted person speaking in a video, one should use a standard webcam to capture video of someone (the source actor) whose facial expressions to be transferred to the targeted individual. An efficient and fast re-enactment will be carried out by processing both videos by Face2Face system. The re-enactment output video is rendered in the most believable manner so that no one could ever think that there might be a possibility of manipulation in the video watched.

While some people find it funny, the idea has a scary and illegal side. Imagine that someone can synthesize a whole video of you making you say words you didn't and transferring the source actor's facial expressions such as lips movements and eyebrows raises to your face. You, the video subject, will turn into the actor's puppet via a flawless face masking system [20]. This concept is dangerous and malicious if taken deeply into consideration. When such a perfectly manipulated video act as an evidence, it can mislead many investigations and judgments, convict many innocent ones and proliferate bias and injustice.

Video Authentication

A video evidence is expected to provide a truthful depiction of any event under investigation. For this reason interpreting any video evidence and relying on its content in the courts, video authentication is a must. The evaluation of the authenticity and integrity of the video has become attainable since the development of video tampering detection techniques that aim at finding traces left after any forgery creation. These techniques are classified into active and passive [21], as shown below:

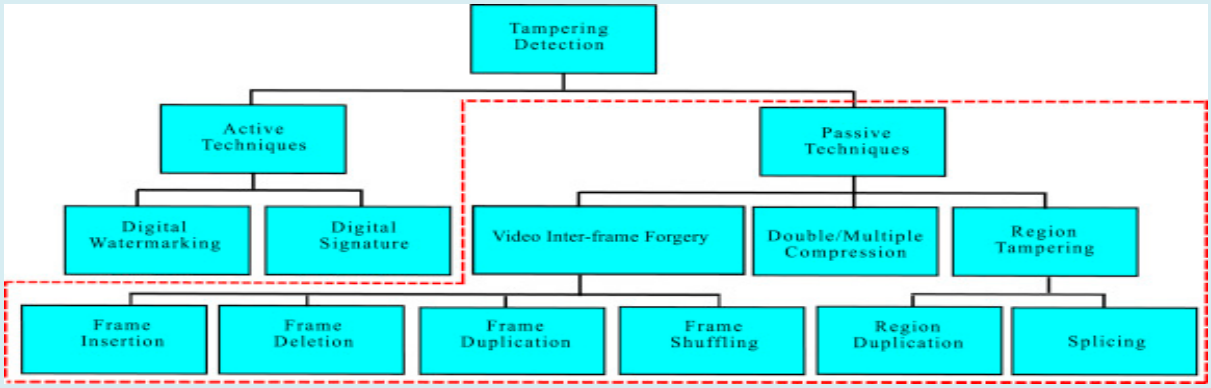

Figure 11: Types of Video Tampering Detection Methods [21].

Active Tampering Detection Technique: Active techniques are based on watermarking and digital signature. Watermarking represents embedding content-based specific codes or digital producer identification labels unique for each multimedia file to verify integrity [15]. Digital signatures represent the digital identity that can also be used to sign a file in which any modification in the content will change this signature as well. These methods provide key information to detect any video manipulation. However some video capturing devices lack the ability of embedding a watermark or digital signature into the video recording. In these cases active techniques will fail to expose tampering traces. Video authentication in such situations leans on passive detection techniques.

Passive Tampering Detection Technique: Passive techniques or what called blind tampering detection techniques are independent of watermarks and digital signatures [21]. They check the authenticity of the video by detecting the footprints left by the video editing operations in the video content. Such footprints help in predicting noise, frame intensity values, motion residues, abnormalities in optical flow and many other complex calculations that these algorithms rely on to detect tampering [21]. No further details concerning these calculations will be discussed since these contain complicated information only comprehended by IT experts. It is good to mention that if a perpetrator is aware of these fingerprints and uses anti-forensic tools to hide or reduce them, this process itself will create another footprint to be detected. In fact passive techniques are classified into three:

1) Detection of double compression: This type is based on the idea that the compressed video must be decompressed before tampering it. After modifying the content the forged video will be restored in compressed format. Hence the resultant altered has undergone double compression which leaves footprints as artefacts that can be detected by blind tamper detection techniques [21].
2) Region tampering detection: This type is applicable in case of copy/ paste and region/frame duplication tampering. It is based on algorithms that identify the exact location of tampering in the video [21].
3) Video inter-frame forgery detection: This type is used for detecting inter-frame tampering like deletion, insertion and duplication. It consists of many algorithms that are specific for each kind. One of them is MCEA (Motion Compensated Edge Artefacts) technique that detects frame deletion tampering by producing digital spikes in the locations where frames were deleted (tampered) [21].

VideoCleaner for Video Enhancement and Authentication

VideoCleaner [22] is a powerful video enhancement and tampering detection software that uncover the truth in a world of distorted realities [22]. It is one of the most efficient video authentication softwares upon which law enforcement rely on worldwide. VideoCleaner facilitates the analysis and enhancement of the video evidence prior of checking its integrity and authenticity. This is done through its effective features such as increasing details clarity, removing electrical noise, correcting the viewing perspective, repairing recordings, improving the brightness of poorly lit scenes and many others that make every small detail in the video content obvious.

Figure 12: VideoCleaner Outcomes [22].

Beside the potent features of VideoCleaner to enhance the analysis by uncovering any hidden details in the content of the video , its recent version has a new 'Forensic Section' that can detect tampering in the video evidence. For example in the figures below, VideoCleaner processsed the frame captured in a video to detect any presence of tampering . As shown in the last picture , the forensic tools of VideoCleaner has detected the presence of tampering in the specified locations due to pixels difference with respect to the original untouched regions in the relative frame.

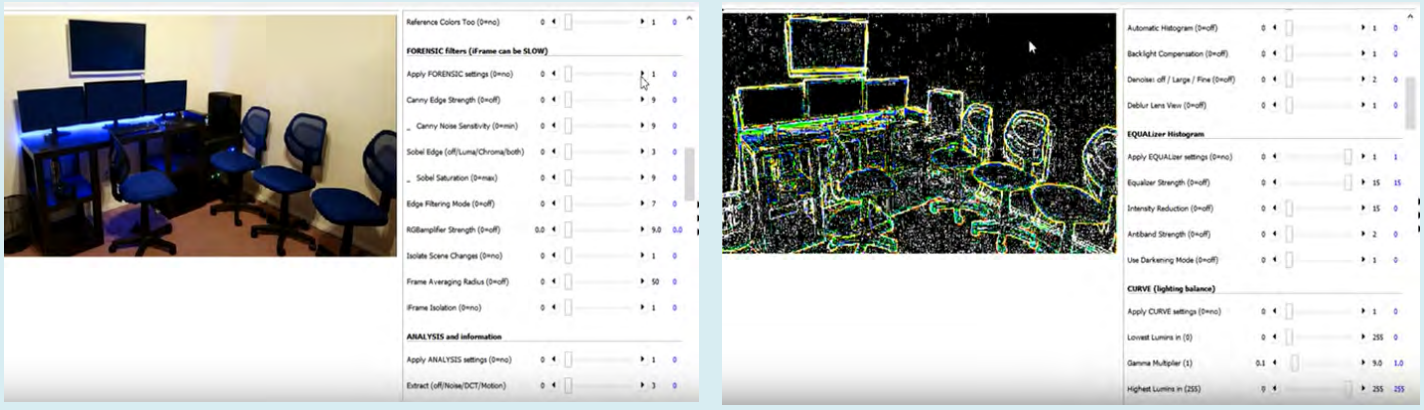

Figure 13: Spotting video tampering traces via VideoCleaner Algorithm.

Today VideoCleaner, along with several others tools for video enhancement and authentication, delivers a clear and credible video evidence to rely on during forensic investigations. Many research studies are looking forwards to provide more vigorous and precise tools to optimize and check the authenticity of the video evidences.

Eventually there is a growing prominence of using videos in the forensic investigations for their paramount role in assisting the courts to make their judgments. This importance of the video evidence compels checking its authenticity and makes it an imperative due to the wide range of tampering techniques available nowadays.

CCTV / Video Surveillance

One of the most powerful video evidence on which many investigators across the globe use in their investigations of crimes and critical events is the recording of the camera surveillance system. Many countries aoround the world are employing CCTV surveillance camera systems in their public and private spaces for recognizing its importance as a tool to secure their streets, airports, businesses, shopping centers, car parks and houses, capture a crime as it unfolds and prevent crimes from happening by discouraging criminals that they will be spotted .

Video surveillance systems or what is called CCTV (closed ciruit television) is a system that relies on a strategic placement of cameras for the aim of monitoring , watching and recording a particular location, event or person for the purpose of security and governing activity.

There a several ways in which CCTV footages act as vauable evidences for court trials , help in police operations through crime investigations and deter crime commission. CCTV roles include :

- Identification of clues , suspects , witnesses and vehicles linked to the event under investigation
- Assisting the police to examine the behavior of the suspects before , during and after a certain incident
- Precisely detecting the date and time of a specific crime or event
- Monitoring an unoccupied home or business to determine the suspect identity if any robbery took place and discompose the burglar while commitiing the crime which could prevent its occurence
- Determining the points of entry and exit utilized in a crime scene
- Having the ability to help in saving the life of abducted person by providing vital source of information to track him down

These facilities and many others provided by a surveillance camera system are what make its footages valuable pieces of evidences for law enforcement , capture crimes and add a layer of security for the lives of private and public sectors.

CCTV tampering

The primary objective of employing surveillance cameras to extract information to track and identify individuals and their activities and detect crimes , will be misfired in case the recording is tampered or the camera is hacked and distorted. Concerning this issue, tampering a CCTV recording is the impact of extrinsic or intrinsic factors [23].

Extrinsic camera tamper attacks are categorized to 3 types [23], including:

- Defocused camera event: altering the focal length of the camera that leads to blurring of the content of the captured video
- Covered camera event:occluding the camera lens partially or totally by external objects
- Moved camera event: changing the camera viewing angle by external forces

All of the three types will be help the perpetrator by inhibiting his face identification. On the otherhand, intrinsic manipulation of the video recording is also applied by permenantly deleting the recorded footage or altering and distorting the video content via antiforensisc techniques.

In this way suspects are able to hide their tracks, alter the data/time of a certain event and even permanently remove the whole footage of an incident in order to mislead and foil the investigation. The question is how to overcome this issue:

CCTV Tampering Prevention and Detection

One solution to reduce the possibility of extrinsic physical tampering in a surveillance camera is activating Tamper Detection setting within the IP camera. This setting will allow sending alerts to the corresponding owner when the camera is tampered with. It is available from several leading IP camera manufacturers including Vivotek, Optica and Axis [15].

If anyone is trying to knock the camera down or any other action has been detected to partially or totally block the camera view, Tamper Detection will notify you and the alert will let you know to log into the video management system to see what happened [24]. This option helps detect individuals' malfunctions and peculiar acts and hinders the occurrence of a complete crime by permitting to quickly recall the police officers on the response of the alert sent from the camera distorted in the area.

While this solution, along with many methods for preventing camera hacks like data encryption and firmware updates, seems helpful and simple, it is not always the case. Regarding intrinsic manipulation where the content of video recording is deleted or altered, other more potent techniques are needed. A proposed method for CCTV video content integrity verification is Unified Tamper Detection Algorithm [23]. This algorithm is based on detection of tamper events by measuring the rate of edge pixels disappearance in the current frame compared to the edge pixels in the background frame resulting in a rate termed EDR (edge disappearance rate) [23]. Based on complex operations and further calculations

depending on this concept, any deletion or alteration of an object or individual in the video frame will be spotted.

Figure 14: Detecting tampered bus video frame using Unified Tamper Detection Algorithm [23].

In this picture the edge characteristics of the foreground object (the bus) differ from those of the occluded region (where the bus was excluded in the tampered frame) [23]. This will be reflected as an abrupt change in the number of pixels in the current frame which is manipulated. Extraction of the foreground objects could be done with the help of complex algorithms like background-subtraction-based video analytics algorithms [23].

Conclusion

The past decade has previously seen unimagined advances in the field of digital forensics due to the wide proliferation of multimedia and its trending tools. By the time being investigators' work limits are no longer restricted by the traditional physical evidences they used to only rely on. The potent role that multimedia tools like video, audio and photos play as forensic evidences drove the court for approving their admissibility and emphasizing on their significance in convincing them to make their decisions and judgments.

Although video, audio and photos are paramount evidences that assist the investigators, any unnoticeable incident of tampering will definitely mislead the whole investigation. The possibility of manipulating any multimedia file has increased with the evolution of technological softwares and algorithms specialized for tampering and alteration. On the other hand various advanced softwares are developed to check the authenticity of any multimedia evidence and ensure its integrity and originality.

References

1. Bourouis S (2020) Recent Advances in Digital Multimedia Tampering Detection for Forensics Analysis. Symmetry 12(11): 1-26.

2. Smith A (2019) Publics in Emerging Economies Worry Social Media Sow Division, Even as They Offer New Chances for Political Engagement. Pew Research Center.

3. Maji P, Pal M, Ray R, Shil R (2020) Image Tampering Issues in Social Media with Proper Detection. Noida, India, IEEE.

4. Qureshi MA, Deriche M (2014) A review on copy move image forgery detection techniques. Barcelona, Spain, IEEE.

5. Bestagini P, Milani S, Tagliasacchi M, Tubaro S (2013) Local tampering detection in video sequences. Pula, Italy, IEEE.

6. Fallahpour M, Shirmohammadi S, Semsarzadeh M, Zhao J (2014) Tampering Detection in Compressed Digital Video Using Watermarking. IEEE Transactions on Instrumentation and Measurement 63(5): 1057-1072.

7. Amanipour V, Ghaemmaghami S (2018) Video-Tampering Detection and Content Reconstruction via Self-Embedding. IEEE Transactions on Instrumentation and Measurement 67(3): 505-515.

8. Sowmya KN, Chennamma H, Rangarajan L (2018) Video authentication using spatio temporal relationship for tampering detection. Journal of Information Security and Applications 41: 159-169.

9. Kaur S, Kushwaha AKS (2018) A Comparative study of various Video Tampering detection methods. Jalandhar, India, IEEE.

10. Kumar V, Singh A, kansal V, Gaur M (2020) A Comprehensive Analysis on Video Forgery Detection Techniques. Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

11. Sitara K, Mehtre BM (2018) Detection of inter-frame forgeries in digital videos. Forensic Science International 289: 186-206.

12. Poisel R, Tjoa S (2011) Forensics Investigations of Multimedia Data: A Review of the State-of-the-Art. Sixth International Conference on IT Security Incident

Management and IT Forensics.

13. Ho AT, Li S (2015) Handbook of Digital Forensics of Multimedia Data and Devices. Wiley.

14. (2020) What is Video Forensics?. Video Forensic Expert.

15. Signh RD, Aggarwal N (2017) Video content authentication techniques: a comprehensive survey. Multimedia Systems 24: 211-240.

16. SRL A (2021) Forensic Image and Video Processing. Amped Software.

17. Anusha GK, Rashmi M, Shobha CK (2019) A Survey on Technique Used for Deblurring Licence Plate of Fast Moving Vehicles Using Sparse Representation. International Journal of Computer Science and Mobile Computing 8(5): 95-99.

18. Joseph S, Palanikumar S (2020) Detection and Localization of Image and Video Tampering. International Journal of Innovative Technology and Exploring Engineering (IJITEE) 9(4): 1951-1956.

19. Thies J (2016) Face2Face: Real-time Face Capture and Reenactment of RGB Videos. s.l., Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp: 2387-2395.

20. Thies J (2018) Real-time expression transfer for facial reenactment. Patent Application No. 15/256,710.

21. Sitara K, Mehtre BM (2016) Digital video tampering detection: An overview of passive techniques. Digital Investigation 18: 8-22.

22. (2020) VideoCleaner FREE forensic video enhancement software. Video Cleaner.

23. Lee Gb, Lee Mj, Lim J (2015) Unified Camera Tamper Detection Based on Edge and Object Information. Sensors 15(5): 10315-10331.

24. (2020) Tamper Detection on IP surveillance cameras. Video Surveillance.