Digital Video Forgery, Detection and Authentication Techniques

Jaswinder Singh

Abstract:-We are living in the era of multimedia technology. Digital video occupies an imperative role in our daily life. With the use of omnipresent multimedia technology, we can create process, transmit and store digital information in many forms such as an image, audio and video. Digital video is convenient tool in forensic investigation, medical treatment, education, entertainment and other disparate fields. Videos are recorded by the people with their smart phones, camcorders, digital cameras and CCTV cameras. We have seen the rapid growth and development in the use of surveillance cameras. Videos recorded using these electronic and smart gadgets mostly contain crucial proof of most of the events. Inasmuch, the most affected to inter frame forgery which can be freely done by replication, insertion, removal and deletion of frames. However, the advancement and usage of inexpensive and effortless video editor software there has been tremendous growth in the consequences and risks of usage such editing techniques. Therefore, forgery is a technique of getting altered, fake and duplicate videos by joining, altering new video. Hence, the genuineness of such digital videos questionable and requires to be verified. In this paper review various video forgery detection methods those are applied to detect whether the video is original or duplicate, real or fake and digital video authentication techniques.

Keywords:- Cameras, Digital Video, Internet, Multimedia Technology

I. INTRODUCTION

Internet has made world a global village today. The Internet is widely used by masses for watching movies. Movie is also known as digital video. Digital videos are easily downloaded with the help of an Internet. These digital videos are captured with the use of digital cameras, camcorders, CCTV cameras, drone cameras or by smart phones. Digital videos are shared by the people on the social messenger as well as social networking websites such as Instagram, Facebook, Youtube and Whatsapp, Telegram, line, Wechat et cetera. Technology provides us with various Applications and tools for generating and transmission video, compress video and video conferencing. Furthermore, another applications such as legal evidence, video surveillance, political videos, video tutorial, entertainment industry, advertisements et cetera occupies their imperative role in today's circumstances. In reality, videos are generated, processed stored and transmitted in digital format in a fast and easy way inasmuch of ample use of Internet and cheap and high quality, high definition cameras. Any newcomer individual can use these techniques to produce unauthorised modifications to the video therefore changing its integrity and authenticity. Deliberately alteration and modification of the digital video is known as Digital Video Forgery.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author

Dr.Jaswinder Singh*, Designation-Asst.Prof.,Department- Computer ScienceName of the Institute- Govt.College Hoshiarpur,Punjab Pin -Code-146001 IndiaE-Mail id –sahota12@yahoo.com

II. METHODOLOGY

In this paper Descriptive Analytic method is used. The study is on the basis of secondary sources like, Articles, Journals, Expert opinion, Books, University News, websites, Thesis, et cetera.

III. VIDEO FORGERY

The crime of falsely and deceitfully or dishonestly creating, making or altering a document, an object is known as forgery. A technique of making altered or fake videos by combining, altering or making new video or tempering the videos by modifying the content or changing the content of the video called video forgery. The purpose of the counterfeiter is to create tampered or fake video by original or real video. Original video is the main source to make tampered video [1]. Tampered videos are used to present in the court as evidence to mislead the court's process. Authenticity must be examined before presenting video in the court as evidence. The digital content can be easily tampered and changed in many ways without leaving any hint or clue. The integrity of video cannot be taken for granted for long period of time. Moreover, this is becoming greater displeasure of the authenticity of these digital videos [2].

IV.AREAS AFFECTED BY DIGITAL VIDEO TAMPERING

Digital videos are used in various applications in different spheres such as legal and law enforcement, video surveillance, social networking, video tutorials, advertisements and entertainment et cetera. These applications play pivotal role in today's life. However its reverberation depends on the circumstances or conditions and the area as well as field where it is used. Different areas influenced by video tampering are:

A. ***Defamation*: -** Video tampering is used to defame the famous personalities and celebrities in movies, politics and related to other fields and hide the actuality then these videos are shared and posted on social websites and social messengers as well [1].

B. ***Forensic Investigations*: -** Forensic investigation means evaluation and scientific analysis of digital video in legal affairs. Digital evidence can be gathered from different locations like banks, parks, malls, stores, restaurants which even help the police in different cases.

Therefore, forensic investigations require assuring their originality.

C. ***Video Surveillance*: -** Videos are captured using the surveillance system available in the Airports, Railway Stations, Shopping malls, Bus stands and other places would be easily changed removing and duplicating some objects and frames from the digital videos. It would also be possible to add some objects, events and other material into the video. In this matter it is hard to judge that the digital video used as proof recorded by the surveillance camera is original or fake.

D. ***Law Enforcement*:-** Digital Videos and pictures are very powerful evidences in legal courts and general opinion. It is assertive to assure the genuineness of digital video and that the video proof has not gone any negligence. Using the tampering techniques culprits use the fake video proofs in the court and exempt from penalty.

V. TAMPERING ATTACK ON VIDEO

Tampering can be done by different domains related with the video sequence. Digital video forgery can be categorised in the following ways:

A. ***Spatial tampering***:-Spatial tampering is known as intra- frame tampering defines as to change the frame, cropping and replacement, adding and removing the content and object of the digital video. Spatial tampering can be performed on visual content of the frame along with the X-Y axis of the digital video. Spatial tampering is performed by operating the pixel bits in frame in the video sequence. Because, spatially tampering is done at block level, pixel level, scene or shot level.

B. ***Temporal Tampering***:-Temporal tampering is also known as inter-frame tampering. Changes performed in the time domain that is re-ordering the sequence of frame, adding extra frame, dropping and replacing frames. The attacks are mainly suffering the time sequence visual data caught by recording gizmos of the digital video.

C. ***Spatio-Temporal Tempering***:- When Spatial tampering and temporal tampering are joined with each other then it is called Spatial-Temporal Tampering. The graphic and sequence of frames are changed in the video. Spatio-Temporal Tempering changes the concatenated sequence of frames with the visual contents present in the frames of the video [2].

VI.GRADE OF TAMPERING ATTACK

A. ***Scene Level Tampering***: - Both type of tempering Spatial and Temporal can be performed at the scene level. Not the scene is altered or tampered but the scene of the digital video is tampered. Delete s scene or copying this to another place.

B. ***Pixel Level Tampering***:- Pixel level attacks are done at spatial tampering. The Content of the video frame is altered at pixel level. The video reliability system must be powerful enough to differentiate the normal video processing operations are done at the pixel level [1].

C. ***Block Level Tampering***:- The content of the video frames are handled as blocks in which the tampering attacks are performed in Block Level. Block refers to a specific portion of the video's frame can be modified, altered, cropped, replaced in Block level Tampering.

D. ***Frame Level Tampering*:-** Alteration is performed on video's frames in Frame Level Tampering. The attacker can add the frame, delete the frame, replicate the frame and reshuffle the sequence of frame from a video to modify or change the content of the video. It can be performed using temporal level.

E. **Shot Level Tampering**:- In shot level tampering shot is added as well as deleted in the video. It can be done at Temporal and Spatial both kind of tampering. A specific shot can be altered or changed from the video [2].

VII. VIDEO TAMPERING DETECTION

Video Tampering Detection is an importantly rising issue in image processing that treats as a restorative to deliberately misuse of data such as video and different digital altering tools. The aim of video tampering detection is to set up the authenticity of a video and to reveal the possible modifications that the video might have gone through. Moreover, Tampering, undesired post processing operations and forgeries normally are constant and leave behind some digital footmarks. Video Tampering detection techniques take these footmarks in order to identify between the original or forged video. When video is forged many of its basic properties alter and to identify these alterations what is called video forgery detection techniques. There are two fundamental mechanisms to video forgery detection [3].

A. ***Active Approach***: - Active forgery detection embeds techniques that is Digital watermarking and Digital Signatures. These techniques are helpful to authentic content ownership and copyright offence or violations. The basic application of Water Marking and Signatures is copyright protection it is used for Forgery Detection, Error concealment, Fingerprint and so on. The major demerit of this approach is that pre-embedding of Digital Signatures and Watermarking reduce and degrade the quality of the Digital video [3], [4].

B. ***Passive Approach***: - This approach does not require any type of fresh information about the video contents nor the constraint of specialized hardware. Though this approach is also known as Passive-Blind Approach. The premise performed by this approach is that videos have some inherent features and properties which are persistent in original or real videos. Passive approach is widely used approach in video forensic domain because of its substantial advantages over active approach [3], [4].

VIII. VIDEO AUTHENTICATION TECHNIQUES

A. ***Digital Signature***: - The authenticity of many legal documents is performed by the presence and absence of handwritten signature. Digital signature is the best technique for authenticity in different areas. Digital signature is an attachment with the specific portion of Digital information which depicts the content and identification of the owner. Digital signature was developed by Hellman and Diffie in 1976. The Digital Signature will rely on secret data which is known by signer it cannot be altered as the content of visual data matches the data comprise in the digital signature.

Moreover, Key is removed from the original video by the sender then the video is encoded by a private key that give signature. Public key is used to decode the signature to authenticate the acquired video by the receiver. Signature can be stored separately in user specified field. Last but not least Digital signature provides Integrity, Authenticity, and Non-repudiation to Digital document [5], [6].

B. ***Watermarking***: - In Watermarking technique, visual data used as authentication enclosed in multimedia data. Different water marking techniques are declared to prevent malicious modification and illegal copying. The water marking mechanisms work on compressed as well as uncompressed information. Embedded watermark is required in copyright-related applications to protect it from different malicious attacks. The watermarking mechanisms are worked in spatial or frequency domain using different transforms such as DWT, DCT and Fourier et cetera [5], [6].

IX.RESULTS

In this paper of study exposes video forgery or tampering is done by using various methods. So there must be number of ways to detect video tampering. There is no separate or unique detection method can be applied on every condition. It depends on video quality, video formats, video forgery techniques, computational restrictions et cetera. In this different authentication methods such as Digital signature and Water marking are discussed.

X. CONCLUSION

To put it in a nutshell, the problem of video forgery is escalating day by day. It requires to be contradicted to avoid its continual impact. There is finite necessity to organise more effective ways to arrange clear distinction between altered and original Digital video. It is essential to understand the requirements and needs discussed above in video tampering detection. Video forensic is a significant research issue in signal processing. Different Authentication techniques such as Digital signature based and Water marking based provided by many researchers. It is mandatory that information provide must be safe to the various kinds of manipulations to some amount. Last but not least, these techniques are not inadequate to the Digital video but also can be implemented on Images.

REFERENCES

1. Rohini Sawant, Manoj Sabnis "A Review of Video Forgery and Its Detection". IOSR Journal of Computer Engineering. Volume 20, Issue 2, Ver. III .Mar. - Apr. 2018
2. Aldrina Christian, Ravi Sheth "Digital Video Forgery Detection and Authentication Technique - A Review" 2016 IJSRST. Volume 2.Issue 6.November 2016
3. Staffy kingra,Naveen Aggarwal,Raahat Devender Singh.(2016) Video Inter-frame Forgery Detection Approach for Surveillance and Mobile Recorded Videos. International Journal of Electrical and Computer Engineering. Volume.7, No.2, 2017
4. Staffy kingra,Naveen Aggarwal,Raahat Devender Singh. "Video Inter – Frame Forgery Detection: A Survey". Indian Journal of Science and Technology**.** Volume 9(44),2016
5. Randeep Kaur,Er.Jasdeep Kaur "Video Forgery Detection Using Hybrid Techniques" IJARCCE Volume 5,Issue 12,December 2016.
6. Mehdi Fallahpour, ShervinShirmohammadi, Mehdi Semsarzadeh, Jiying Zhao." Tampering Detection in Compressed Digital Video Using Watermarking"IEEE transactions and measurement-May 2014.

AUTHOR PROFILE

My first name is **Jaswinder**, my middle name is **Singh** and sahota is my surname. I have passed my higher secondary and Senior Secondary from Punjab School Education Board, Mohali, in the year 1996 and 1998 respectively. I completed my three year bachelor degree from Panjab University Chandigarh , After it, I completed my M.SC.(IT) and M.C.A from Punjab Technical University. Under OPJS University, I completed my Doctorate (Ph.D). At present, I work with an appellation as an Assistant Professor at Govt. College Hoshiarpur and having 10 years of teaching experience in the subject of computer science. E-Mail ID -sahota12@yahoo.com