Challenges in Surveillance Video Forgery Detection

Sowmya K.N[1], Dr H.R Chennamma[2]

Abstract— In the modern world / current scenario technological advancements in the area of photography has made pave for digital cameras by replacing classical analog cameras which are increasingly used to record events in day to day life. Law or security enforcement agencies are increasingly relying on digital photographs or videos for corroborating evidence against crime scene scenario. Verifying authenticity and integrity of such digital evidence which was gathered from crime scene place an important role Various forensic tools help in examining the digital evidence to identify whether it has been forged or not.

Low cost and easy availability of CCTV's has made many household people to consider it for security along with the corporate world. Surveillance cameras are found hanging in public places to prevent crime and for gathering evidence. Authentication of the digital video footages procured from city surveillance system (CSS),digital video recorders(DVR's) is a challenging task since most of these CCTV's are installed over time and technical specifications of these differ from each other. Various factors like the codec used by these CCTV's, their camera resolution, the distance involved in capturing etc pose new challenges to the investigators every day. In earlier days the video footage data obtained were stored locally at the place of recording. For the real time analysis now they are stored centrally in the repositories or cloud which requires secure transmission media.

Index Terms— Video forgery detection, Digital forensics, Camcorder forensic identification, Video Tampering

1 Introduction

IN forensic analysis police is an incident responder. Forensic evidence which is collected through seizure memo by punch witness is an important proof for providing justice. They need to be well trained to collect collect and manage digital evidence from scene of crime. The evidence collected from the scene has to undergo further analysis in labs without affecting its originality. Normally an image of the evidence is made and further forensic analysis is made on the copy obtained.

Video forgery detection can be active or passive depending on the approach used [1]. In active video forgery detection, watermark or digital signature retrieval is done to verify its integrity. In passive forensics, visor techniques need to be followed to detect intentional tampering [2]. Tampering can be in a small region of the video frame by cloning or in series of frame through splicing etc. Unified approach to detect Spatial, temporal and spatio temporal tampering is the need of the day.

Assistant Professor, Dept of ISE, JSS Academy of Technical Education, Bangalore, Visvesvaraya Technological University , Karnataka, India. kn_sowmya@rediffmail.com,ph:9945505336
Assistant Professor, Dept of MCA, Sri Jayachamarajendra College of Engg., Mysuru, Visvesvaraya Technological University, Karnataka, India. anuamruthesh@gmail.com, ph:9480057455

2 Factors affecting Surveillance Video forgery detection:

The modern day ombudsman - CCTV's are mounted on video camera system in fixed or dynamic mode with certain degree of rotation. It helps to identify and prevent crime by monitoring varied resources such as people, assets and patrol. Though it cannot be installed at all places it helps to provide linking evidence at times for proving crime. Codecs and containers used for storing the visuals play an important role here. Resolution adopted by the camera has high significance with repsect to quality. Inherent characteristics of the video acquisition device help to determine whether the given video is tampered or not. All these aspects are discussed below:

.

2.1 Codec Identification:

The common problem encountered by law enforcement agencies is the proper identification of encoding method adopted in the recordings obtained in real time/prime time. Most of the DVR vendors who sell their products at low price in grey market do not specify the complete technical details in documentation provided to identify the codec used by the container. Codec is the encoding

approach adopted to store the raw visual recordings in a compressed format. Container identified by the file type/extension holds or supports multiple codecs. If the obtained video container file extension or video format is known then it does not guarantee that the video will run in any media player. Video file formats help to identify the arrangement and structure of the file contents. File extension do not determine the quality of the video footage but the encoding approach adopted inside them determine the quality of the video. Generally raw video obtained is down sampled and encoded before sent through IP for storage. Encoding approach adopted by the DVR vendors vary for the same codec. Same camera may be used by multiple applications and they may use different encoding options for recording before transmission. Ex: mobile phone cameras. The common way to detect codec is through footprint analysis which would have been introduced by non invertible operations [3], [4]. In case of IP based CCTV's which are expensive when compared to analog CCTVs instant feed of visuals can be obtained through internet from any place. Today since all the members in a family are working and hardly anyone or elderly people stay at home it has helped to obtain instant information of homes from offices through mobile phones or laptops. Network video recorders can be used to store data in case of centralized IP cameras and decentralized IP cameras can directly store data on cloud through network attached storage (NAS). Security of data thus obtained and during transmission is a huge concern here.

.2.2 CCTV Camera Resolution:

Camera resolution, particularly in conventional CCTV's is measured with respect to its inherent quality in terms of TV lines (TVL) in terms of standard analog definitions. If more number of TVLs is available then more details can be obtained from the rendered video/image. The image resolution that the CCTV camera can capture depends on image sensors based on CCD/CMOS architecture. Normally CCTV cameras and DVRs need to maintain same resolution specification to maintain quality. At times DVRs can also have higher resolution too which is less available in nature. TVLs refer to alternating light and dark lines vertical in nature that can be captured or displayed by the camera and monitor. Conventional DVRs provide resolution, compression capability with QCIF (176 X 144 –PAL, 176 X 120 - NTSC), CIF (352 X 288 – PAL, 352 X 240 – NTSC), 4CIF(704 X 576 – PAL,704 X 480 – NTSC), D1 (704X 576 – PAL, 704 X 480 – NTSC) resolution formats etc by using appropriate codec. Today we are moving from traditional CCTVs to HD system where camera resolution is spoken in terms of pixels rather than TVLs. But it is a long way to adopt uniformly in all sectors. Higher the resolution more the bandwidth required to transmit streaming videos obtained from camera. Currently we find QCIF resolution used for remote viewing from a mobile device and higher resolutions in city surveillance systems by video codec such as H.264 etc [5],[6].

Electrical network frequency (ENF) supplied by the power grid in an area have an impact on imaging sensors used in cameras. At time of forgery detection identifying the change in ENF values from the recording is a challenging task [7]. Security systems record the visuals at regular resolution. Intentional tampering for malicious act like cropping requires up-scale forgery of video to erase crime evidence.

2.3 Distance Artifact:

An untampered video has its own characteristic features influenced by the ambience where it is recorded and also due to the imaging device used. Whenever there is a forgery the natural scenes of the video obtained are altered with respect to statistical correlations found in a original video. Also the consistent qualities of the used acquisition device found in the original video will be missing in the forged video. Initially the type of forgery is unknown and identification of such video forgery detection is a challenging task.. Camera based techniques adopted for video forgery detection relies on the inherent characteristics of the camera. The camera response function (CRF) which differs for each model acts as an excellent clue to detect forgery. Chromatic aberrations in optical imaging systems, sensor pattern noise deviations support forgery detection [8][9].

Optical range is determined based on lens used and details captured. Details vary with respect to context in security systems. In a traffic management surveillance system details may refer to number plate of vehicles, people recognition etc. Details may also refer with respect to objects such as gold ornaments in a jewellery shop. Details depend upon the security needs. CCTV cameras are available with fixed lens and vari-focal lens. Fixed lens camera have a single angle of view where as a vari-focal lens based CCTV camera can be adjusted to balance the area to be covered along with the details to be captured. With the help of current angle of view the relevant details in focus can be captured in the later. Increase in the focal length help us to get finer details of object in focus even though the viewing angle gets reduced. Normally vari-focal length cameras are found in Banks, ATMs, checkposts etc. The total distance involved between the

CCTV cameras where mounted to the display screen has its impact on the signal captured. The inference of electrical signals, noise increases with distance. Identifying differential patterns obtained when forged other than the distortions introduced by the camera lens helps to detect forgery.

If there is sufficient darkness then the IR CCTV cameras help night vision by capturing the video footages with the help of LEDs which are positioned around the outer edges of the lens. The number of LEDs decides the distance of illumination. If there is an intentional forgery in IR camera footage then the constant direction of the light source is affected in a forged video footage which acts as an evidence for video tampering detection.

2.4 Cost:

Cost incurred in proving digital evidence not only depends on time and man power but also depends on resources used in authenticating the procured digital evidence. Today most of the digital evidence is procured from DVR's of third party sources owned and controlled by them in order to meet their specific requirements and it is going to increase in coming days. When the proprietary DVR vendors do not specify explicitly the encoding approach used, the cost and time incurred is sure to increase. At time, the maintenance of the surveillance units are so bad after installation that the video footages procured from them becomes waste or tedious to analyze affecting cost. Everytime the CCTV evidence is procured the police need not send it to labs for further analysis if they are provided all the available DVR players locally unless foul play is suspected of the video evidence procured.

3 Conclusion

Video surveillance is a package comprising trivial hardware, software in an indoor/outdoor environment. It helps to increase safety of the subject in context and help to prevent and record crime. With the increase in its adaptation vulnerabilities associated with it is in rise. The procured video footages are tampered before acquisition intentionally to mask crime or after acquisition to protect culprit. Video forgery detection does not have a universal law to follow. Challenges vary with respect to demography, region, regulations and rules to be abided by law enforcement agencies in proving crime through digital evidence. Safety and security of the visuals obtained through CCTVs require a systematic approach. The universal fact that a criminal cannot escape without leaving any digital footprints for performing forgery motivates the opposite team. We need to be sensitive particularly when such video footages are abusive and affect moral or ethical standards in the society. The type of video procured, who, when, where, why etc all need to be answered in an organized way. Standard policies, procedures need to be advised, framed and followed.

Acknowledgment

The authors wish to thank JSS Mahavidyapeeta for their constant support and encouragement.

References

[1] Hyun, Dai-Kyung, Min-Jeong Lee, Seung-Jin Ryu, Hae-Yeoun Lee, and Heung-Kyu Lee. "Forgery detection for surveillance video." In *The Era of Interactive Media*, pp. 25-36. Springer New York, 2013.

[2] Wahab, Ainuddin Wahid Abdul, Mustapha Aminu Bagiwa, Mohd Yamani Idna Idris, Suleman Khan, Zaidi Razak, and Muhammad Rezal Kamel Ariffin. "Passive video forgery detection techniques: a survey." In *Information assurance and security (IAS), 2014 10th International Conference on*, pp. 29-34. IEEE, 2014.

[3] Chen, Yingwei, Kiran Challapali, and Mahesh Balakrishnan. "Extracting coding parameters from pre-coded MPEG-2 video." In *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*, vol. 2, pp. 360-364. IEEE, 1998.

[4] Bestagini, Paolo, Ahmed Allam, Simone Milani, Marco Tagliasacchi, and Stefano Tubaro. "Video codec identification." In *Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on*, pp. 2257-2260. IEEE, 2012.

[5] Alles, Erwin J., Zeno JMH Geradts, and Cor J. Veenman. "Source camera identification for heavily jpeg compressed low resolution still images." *Journal of forensic sciences* 54, no. 3 (2009): 628-638.

[6] Rocha, Anderson, Walter Scheirer, Terrance Boult, and Siome Goldenstein. "Vision of the unseen: Current trends and challenges in digital image and video forensics." *ACM Computing Surveys (CSUR)* 43, no. 4 (2011): 26.

[7] Grigoras, Catalin. "Applications of ENF criterion in forensic audio, video, computer and telecommunication analysis." *Forensic science international* 167, no. 2 (2007): 136-145.

[8] Hsu, Chih-Chung, Tzu-Yi Hung, Chia-Wen Lin, and Chiou-Ting Hsu. "Video forgery detection using correlation of noise residue." In *Multimedia Signal Processing, 2008 IEEE 10th Workshop on*, pp. 170-174. IEEE, 2008

[9] Ravi, H., Subramanyam, A.V., Gupta, G. and Kumar, B.A., 2014, October. Compression noise based video forgery detection. In *Image Processing (ICIP), 2014 IEEE International Conference on* (pp. 5352-5356). IEEE.