



ISSN 2394-3777 (Print)

ISSN 2394-3785 (Online)

Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 3, Special Issue 5, February 2016 in association with

HEERA COLLEGE OF ENGINEERING AND TECHNOLOGY, THIRUVANANTHAPURAM

Organizes

NATIONAL CONFERENCE ON ENGINEERING FOR LIFE (NCEL – 2016)

(12th -13th February 2016)

Surveillance Video Authentication and Enhancement

Guided by

Mrs. Ashmi.G.V

Cyber Forensics and Information Security

ER & DCI institute of Technology,Trivandrum

By,Neethu Prakash

Cyber Forensics and Information Security ER & DCI institute of
Technology,Trivandrum

Abstract: Now a day's video and audio evidence are admissible as evidence in court of law. But in numerable cases; the video evidences that are collected from various surveillance systems are of low quality. Further processes on this video may either get blurred or distorted. This paper introduces a novel technique for detecting the tampered frames and enhancement of video acquired under challenging conditions lighting conditions such as haze, low light, fog etc. The main aim is to improve the visual appearance of the video. Along with the video enhancement this paper also introduces techniques to automatically detecting the input impairments from the video evidence, object detection and license plate detection. Histogram equalization technique is used to detect the input impairment, so that we get an idea about whether the distortion in the input video is due to any artificial activity or any natural conditions. This video enhancement helps to analyze background information that is essential to understand object behavior without requiring expensive human visual inspection.

1.INTRODUCTION

As per the increase in various surveillance systems such as CCTV, body wearing surveillance equipment's used by law enforcement forces; there is an exponential increase in the crimes related to these surveillance systems. The crimes may include altering or distorting various recorded images and videos, adding unwanted videos along with the original video, deleting the evidence from the videos etc. The main factor behind these crimes is, it is easy to alter or doctor the image and video evidence by using relevant and efficient techniques. An image or video evidence will be distorted due to other reasons such as atmospheric and lightning conditions which may include haze, mist, fog, rain, cloud cover, low light, bright light etc.

While capturing videos become much easier,

video defects, such as blocking, blur, noises, and contrast distortions, are often introduced by many uncontrollable factors such as unprofessional video recording behaviors, information loss in video transmissions, undesirable environmental lighting, device defects, and so forth. As a result, there is an

increasing demand for the technique video enhancement, which aims at improving videos' visual qualities, while endeavoring to repress different kinds of artifacts. There are two most common defects: noises and contrast distortions. While some existing software have already provided noise removal and contrast enhancement functions, it is likely that most of them introduce artifacts and could not produce desirable results for a broad



variety of videos. Until now, video enhancement still remains a challenging research problem in filtering noises as well as enhancing contrast.

II. VIDEO EVIDENCE

Video Evidence is any sort of video used as permissible evidence in court of law. It can be recorded in video home system (VHS) or in digital format through a security surveillance camera or other devices. As there has been an increase in the use of both types of evidence, due to their validity in the court, it has led to a biased debate on its appropriate use.

Most often, Video footage from a CCTV camera is taken as an evidence for a crime in a public or a private place. As the technology is shifting towards digitalization, the use of digital surveillance cameras as evidence, during court trials is getting prominence.

With the rise in the availability of video devices, people who found themselves unintentionally at the scene of a crime can capture video evidence by means of mobile phones and digital cameras and sometimes this video evidence can act a valid proof in the court of law.

While considering video evidence, it has to undergo a strict handling procedure in order to be admissible in the court of law. The name of the video evidence handler is registered and then the video is stored in a climate controlled place, in order to ensure that it is not available for modification in any way. If this strict handling procedure is not followed and if the video containing the evidence is produced in the court, it will be treated as inadmissible evidence.

A. Video tampering:

A large scope of revealing and low price of digital video cameras along with the sharing of video websites, the digital videos are playing a suitable role in our daily life. Since digital videos can be easily distorted, their authenticity cannot be taken as trustworthy. Christo Ananth et al. [5] discussed about Reconstruction of Objects with VSN. By this object

reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state-of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of-the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results. In today's digital era in which all type of the communication and compression techniques has been done with the help of the multimedia data such as image and video. Through the multimedia editing tools one can easily change the content of data which lead to lose the authenticity of the information. It is fact that tampering with a digital video is seemed to be more time consuming as well as the challenging task than tampering with a single image. Due to the availability of the video editing tools it become easier to tamper the videos

The tampering has been categorise in two ways firstly Temporal Tampering: under this different changes have been done in to the matter regarding the information including every pixels as well as frames. So number of the operation has to be performed to distort the various videos. This is done by adding number of frames in between the two consecutive frames as well as removing the number of frames between them. In the case of spatial tampering different changes have been done on every pixels of the particular frame of videos and images which stored the data values of that frame. So number of the operation as to be performed in order distorted the videos. And that is by doing the adding of the object and removing any particular object from the frame.

III. PHASES OF VIDEO AUTHENTICATION AND

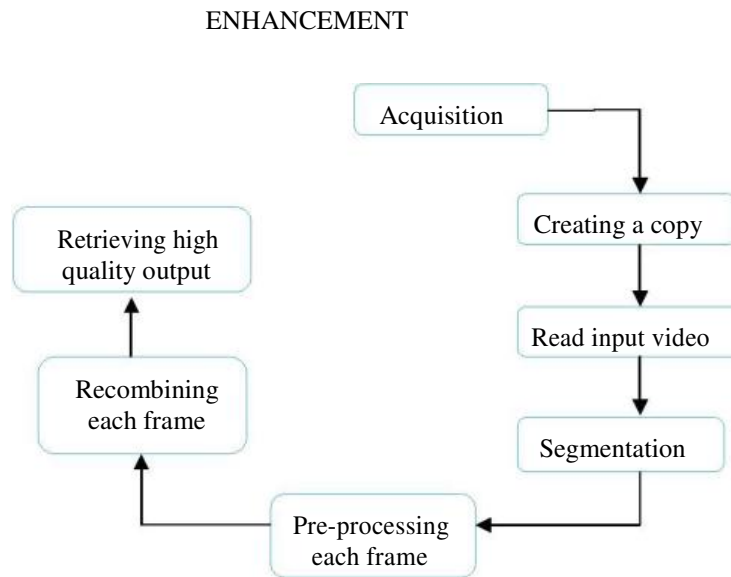


Figure 1.phases

1. Acquisition of the input video from the cctv equipment:

Sometimes it is necessary to recover the video evidence onsite when the original is available. This process assists the video forensic expert through examining the equipment that created the video recording. Then examine the video evidence for signs of physical tampering, scratches, or dis-assembly.

2. Create an image of it:

We can't work with the original evidence due to loss of integrity of the video evidence. Before starting the video analysis the image of the original image will be created. When we use the original evidence for analysis purpose various features of it may change.

3. Read the input video:

The video can be loaded using few software applications based on the platform that we are used.

Digital properties of video evidence such

as, exif or metadata and hexadecimal information, where examined in this phase, it is crucial to determine if manipulation is present.

4. Pre-processing each frame:

Re-Create the events as they occurred using the same technology or digital recorder that created the video evidence. Various pre-processing techniques such as de-blurring, brighten, sharpen etc. are used to improve the quality of input video.

5. Recombining all the frames:

In this phase the enhanced frames will be recombined to get a clear output video.

6. Retrieving high quality video:

This is the final phase; we can retrieve a high quality video during this phase. Document the video authentication process, providing notes taken, and state all forensic findings about the authenticity of the video evidence.

IV.PROPOSED SYSTEM

The new techniques introduced in this paper are as follows: Tampering detection, input impairment detection, Automatic license plate detection, pre-processing techniques to enhance the input video etc. The main aim is to ensure authenticity of the input video along with the enhancement techniques to improve the quality. Security surveillance systems often produce poor-quality video, and this may be problematic in gathering forensic evidence.

This paper presents a novel technique to detect video tampering and video processing operations, such as frame averaging, sharpen, and brightness increase, de-blurring, de-interlacing, scaling speed reduction etc. While this method can be applied to any modern video codec, including the recently released high-efficiency video coding standard. The automatic input impairment detection technique is used to distinguish the natural conditions and artificial activities that lead to impairment of the



input video. The third technique Automatic license plate detection technique is used to automatically locate and enhance the license plate characters in a vehicle. So this system can able to detect the tampered frames in all kinds of surveillance videos such as outdoor videos and indoor videos and also able to improve the quality using various pre-processing techniques.

A. Tampering Detection

Video forgery primarily falls into two methods based on their approaches; active approaches and passive-blind approaches. The first approach (active approach) is primarily focused on the invisible data and requires pre-embedding of information like watermark, fingerprint into images or digital signatures, and to identify them through integrity detection of the pre-embedded information. On the other hand, the latter approach is more appropriate for some occasions like video, photo image or audio.

Specifically, passive approaches can be divided into three general types' namely splicing, source identification and copy-move forgery. Such approaches are used for the detection of digital video and double compression video tampering like MPEG or H.246. This is clear from the several works dedicated to digital video tampering detection. These methods are effective in the detection of traditional forgery operations and it is often beneficial to determine the digital video authenticity with the help of video object detection, video double compression, and video frame of region duplication, frame-based tampering and image double JPEG compression.

B. Input impairment Detection

This technique is used to automatically detecting the reason behind the impairment in the input video sequence. In the case of surveillance videos, some may be captured using outdoor surveillance equipment's and some other are recorded using indoor surveillance equipment's. So the two

possibilities of distortions in these videos are due to natural conditions or artificial activities. The natural conditions include haze, fog, cloud cover, rain, low light, bright light etc. The artificial activities may include intentional activities to distort the video for example, the person one who tries to blur the surveillance videos by using a torch light, or someone tries to veil the focus of the surveillance systems. This technique aims to distinguish between the natural conditions and artificial activities which may cause distortion or blur to the captured videos from the surveillance equipment's.

C. License plate Recognition and Enhancement

License plate is a unique identification for every single vehicle. Hence, it has been used in various applications such as for security monitoring, access parking systems, private area identification and etc. Due to the benefit of using license plate as personal identification, a lot of research has been done to recognize the plate number automatically.

Various technique of License Plate Recognition (LPR) is developed based on different techniques, applications and countries. In general, the characters for vehicles plate number are arranged in two structures, either the characters are placed in a single row or in two rows.

The LPR consists of two main processes; firstly, identify license plate location and secondly recognize the license plate number. In the first process, the exact location of the license plate is defined, so that only the selected area will be analyzed in the second process. It also helps in minimizing the processing time taken in the next process. Failure to identify the location of plate number will result complexity in identifying the characters of plate numbers and the worst scenario, the system is unable to recognize the character at all. It means, to get an exact location of plate number is a crucial process of LPR. Normally, location of license plate is determined based on the features of license plate such as license plate format, shape, symmetry, colour, texture, interval between



characters, and spatial frequency. In recognition phase, the character of the license plate is identified. Before the process of alphanumeric character identification, each character in the selected area is separated. After the separation process has been done, the character will be identified. There are several techniques have been used for the character recognition.

V.CONCLUSION

This proposed system can able to detect the temporal tampering techniques and enhance the input video to improve the quality, also this system can able to automatically detect the input impairment and the LPR is used to locate and enhance the characters in the license plate. From the first technique we can able to measures the processing image pixels to produce a frame-by-frame motion energy time for the video which further help in detecting the temporally tampered video frames, so that different tampering attacks in the temporal domain along with the location of the tampered frame. Thus these techniques are able to judge authenticity of the video and from the second technique we can able to compute the local information through the average object area and entropy of the video frames which further use as the input for SVM classifier in order to distinguish the reason for the input impairment in the given video. The hazy video and video captured in various challenging lighting conditions can able to enhance using this proposed system. This system also provides user friendly techniques for efficiently enhance a low quality input video. The user may need only less knowledge about the various image or video processing techniques to efficiently enhance the low quality input video.

REFERENCES

- [1].Urvashi Sharma,Tripti Sharma,Trisha Jain
"Efficient object detection with its enhancement",International Conference on Computing, Communication and Automation (ICCCA2015),2015.
- [2.]Gil-beom Lee, Myeong-jin Lee, and Jongtae Lim

"Unified Camera Tamper Detection Based on Edge and Object Information", 2015.

[3.]Ankita Gupta, Shilpi Gupta, Anu Mehra,"Video Authentication in Digital Forensic" International conference on futuristic trend in computational analysis and knowledge management,2015.

[4.]Ishan. A. Patil,,Mr. Vijendra. P. Meshram2, Mr. Ishan. S. Chintawar, Ms. Snehal. B. Meshram4."

Enhancement of imagery in poor visibility conditions" International Journal of Advanced Research in Computer Science and Software Engineering,2014.

[5.] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiq Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[6.]Zarna Parmar, Saurabh Upadhyay "A Review on Video/Image Authentication and Tamper Detection Techniques",2013.

[7.]S.S. Bedi1, Rati Khandelwal "Various Image Enhancement Techniques- A Critical Review" International Journal of Computer Science & Engineering Survey,2013.

[8.]Manglesh Khandelwal, Shweta Saxena ,Priya Bharti"An Efficient Algorithm for Image Enhancement" EURASIP Journal on Advances in Signal Processing,2012.

[9.]Xuan Dong, Jiangtao Wen, Senior Member, IEEE, Weixin Li, Yi Pang, "Intra-and-Inter-Constraint-based Video Enhancement based on Piecewise Tone Mapping",2012.