IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10214

Detection of Copy-Paste Forgery in CCTV Footages

Sana Shamsudheen[1], Reesha P.U[2]

MSc Scholar, Computer Science, St Joseph's College (Autonomous) Irinjalakuda, Thrissur, India[1]

Assistant Professor, Computer Science, St Joseph's College (Autonomous) Irinjalakuda, Thrissur, India[2]

Abstract: Video forgery detection aims at checking the authenticity of videos by recovering information about their history. Copy-paste forgery is done by replacing a region from a video with another region from the same video. By copying a part from the same video , its important properties, such as noise, colour palette and texture, will be fit with the rest of the video and thus will be more difficult to distinguish and detect these parts. In this paper DWT (Discrete Wavelet Transform) is used to compress the frame and optical flow technique is used to detect the flow of the moving objects and the forgery object. But the SIFT (Smart Information Flow Technology) is used to detect the key features of the original frame and the forgery frame. OpenCV is used for image processing.

Keywords: Copy Paste forgery Detection in videos, Optical flow, ROI masking, DWT, SIFT.

I. INTRODUCTION

With the wide attainability of low cost and user friendly digital video cameras and the availabilities of video sharing websites such as Instagram ,YouTube digital videos are playing very supreme role in current context. Due to this forgery detection of videos is an important subject in current situation .Nowadays digital videos undergoes many illegal alterations, due to that the authenticity couldn't be taken for trustworthy. Authentication of digital video is also known as digital video forensic and which is a process of proving and identifying that the video taken have no tampered content and is original .at the same time forgery detection of a video isn't that much easier, but with the ease of advanced, increasingly advanced digital video editing tools are making it easier to tamper a video, so because of this identification of tampered video is so much vital .because originality and authenticity of video data is very crucial. For example in forensic investigation, video surveillance, law enforcement and content ownership. When it comes to court of law, it is very crucial to establish trustworthiness of any kind of video when it used as evidence. And by the emergence of sophisticated video editing technology which is rapidly growing in today's situation, anyone can easily alter the video by removing an object from video sequence by simply removing some of frames, insert an object from a different video source or a portion of the video will be replaced with another part of the same video. So a video frame could be tempered in a specific way to slander a n individual. And also a criminal could be free easily, because a video shows about crime has been altered. Because most artifice techniques are highly available for general public, so video recording is emerging as a serious challenge. For identification of originality of video contents and to detect malicious forgeries and to prevent various types of tempering, various types of detection techniques are used on video data. These techniques could detect the types and the locations of malicious forgeries. But the case is there are wide range of powerful digital video editing tools which allow maximum access, manipulations and reuse of videos. Digital video offer many attributes for forgery detection algorithms to take advantage of, specifically the colour and brightness of individual pixels as well as the format and resolution. These properties provide opportunity for the analysis and comparison between the fundamentals of digital forgeries in an effort to develop a better algorithm for detecting forgery in a video .This paper propose some methods to find copy paste forgeries that occurs in CCTV footages.

II. COPY-PASTE FORGERY DETECTION IN VIDEOS

This section sheds light on the notable contributions made in the field of copy-paste forgery detection in CCTV footages, so as to provide an overview of the current state of affairs in this research domain. All the copy-paste detection techniques proposed in the literature can generally be divided into two categories: the first techniques is that optical flow ,which is used for calculating the motion of image intensities; which may be ascribed to the motion of objects in the scene. Hence the forgery in the video will be detected and the second category constitutes ROI (Region of Interest) masking, which can be used as "mask" to remove pixels from the image which means setting their intensity to zero. Alternatively, we can choose to set the pixel intensities to some other non-zero value .The mask tool can remove pixels that are outside the selected ROI and remove pixels that are inside the ROI. We also use DWT (Discrete Wavelet Transform) to compress frames that obtained from the given input video. And SIFT (Scale Invariant Feature Transform) which is a feature

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10214

detection algorithm in computer vision to detect and describe the local features in from the compressed frames .We get the forgery frame as the output.

III. TECHNIQUES USED FORGERY DETECTION

There are mainly four techniques used for the detection of copy-paste forgery in CCTV footages:

A. Optical flow

Optical flow is the technique used for calculating the apparent velocities of objects in a frame that are extracted from the videos. This method is used to measure the velocities of objects in the video by estimating optical flow between video frames. Generally, moving objects that are closer to the camera will display more evident motion than distant objects that are moving at the same velocity. This technique is mostly used in computer vision for quantifying and characterizing the motion of objects in a digital video, often for tracking systems Optical flow is an important concept that is used in one form or another in most video processing algorithms.

Optical flow works on diverse assumptions:

Now we check the pixel intensities of two consecutive frames because the neighbouring pixels have similar motion.

Take a pixel I(x,y,t) in first frame. It movements with the aid of using distance (dx,dy) in subsequent frame taken after dt time. So on the grounds that the ones pixels are the identical and intensities does not change, we are able to say,

$I(x,y,t)=I(x+dx,y+dy,t+dt)$

After that take Taylor series approximation of right-hand side, remove the common terms, and then divide it with dt to get the subsequent equation:

$fxu + fyv + ft = 0$

Where:

$fx = \partial f \partial x ; fy = \partial f \partial y$

$u = dxdt ; v = dydt$

Above equation is referred to as Optical Flow equation. Here, we are able to discover fx and fy, they're image gradients .The gradient along time is ft. But (u,v) is unknown. We can't deal this one equation with unknown variables. So various techniques are supplied to clear up this problem and certainly considered one among them is Lucas-Kanade.

B. ROI masking

The Region of Interest (ROI), which is a part of image that we want to filter. The toolbox of ROI contains set of ROI objects and using these objects we can create various shapes like rectangle, circle, ellipse, polygons and other hand drawn shapes. After its creation using the properties of these ROI objects we can customize its functioning and appearance. And also ROI objects provide events and object functions, using these we can enforce interactive behaviour .For example, using events the application can execute custom code whenever the ROI changes its position. The toolbox consists of parallel set of features for ROI creation. For Example, we can create square ROI, with the aid of using the **images.roi.Recatangle** or using its corresponding convenience function **drawrectangle**.

C. Discrete Wavelet Transform(DWT)

Discrete Wavelet Transform(DWT) , which is used for compression and de-noising of images and signals .In the case of functional analysis and numerical analysis .DWT is used to discretely sample the wavelets. The main benefit it has over Fourier transforms is temporal resolution which will bag both location information and frequency with different wavelet transforms.

D. Scale Invariant Feature Transform(SIFT)

The scale-invariant feature transform (SIFT), which is a feature detection algorithm in computer vision. This algorithm is used to detect and describe local features in images. This feature detection algorithm was published in 1999 by David Lowe.

The SIFT algorithm have been used which is able to detect the copy-move forgery done in an image and also, evaluate the parameters of the transformation used. It detects the group of points belonging to cloned areas. First the all the features

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10214

are extracted from the image and checks whether these features are matched to the original image. Then forged regions are detected after the clusters and formed using hierarchical clustering.

SIFT key points of objects are first extracted from a set of reference image and it will be stored in a database. After comparing each feature from the new image to this database an object is recognized in new image and also find candidate matching features based on Euclidean distance of their feature vectors. From the full set of matches, subsets of key points that agree on the object and its location, orientation, and scale in the new image are identified to filter out good matches. The determination of consistent clusters is performed rapidly by using an efficient hash table implementation of the generalized Hough transform.

IV. ALGORITHM

Step 1: Read a video as input.

Step 2: Apply the frame separation to separate the frames in the given video with the help of: nFrames = videoObj.NumberOfFrames, vidWidth= videoObj.Width, vidHeight = videoObj.Height, T_frames=nFrames-1.

Step 3: Write the frames into a folder.

Step 4: The Gaussian noise are removed by applying fsfilter.

Step 5: The replication and noise are reduced by applying imfilter.

Step 6: The forgery frames are detected by applying optical flow technique.

Step 7: The forgery frames are detected by applying ROI mask.

Step 8: The forgery video frames are compressed by applying DWT.

Step 9: The feature points in forgery frames are checked by applying SIFT technique.

Step 10: Get the forgery frames as output.

V. PROPOSED WORK

This paper discuss about the techniques used to detect the copy paste forgery of CCTV footages with the help of Key point features and the optical flow algorithm and ROI masking. First of all Gaussian noises are removed using some filters, then frames will be extracted from the given input video as shown in Fig.1.Then using ROI masking remove pixels means which means setting their intensity to zero as shown Fig.2. Alternatively, we can choose to set the pixel intensities to some other non-zero value. The mask tool can remove pixels that are outside the selected ROI and remove pixels that are inside the ROI .The optical flow algorithm is modified with the help of DWT(Discrete Wavelet Transform) and the SIFT(Scale-Invariant Feature Transform). The frames are compressed using DWT and optical flow is used to detect the flow of the moving objects and the forgery object. But the SIFT technique is used to detect the key features of the original frames and the forgery frames after compressing those frames by applying DWT .After applying all these techniques we obtain the forgery frames as shown in Fig.3 and the time at which the forgery occurred as output.

Fig.1 Extracted frames from input video

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10214

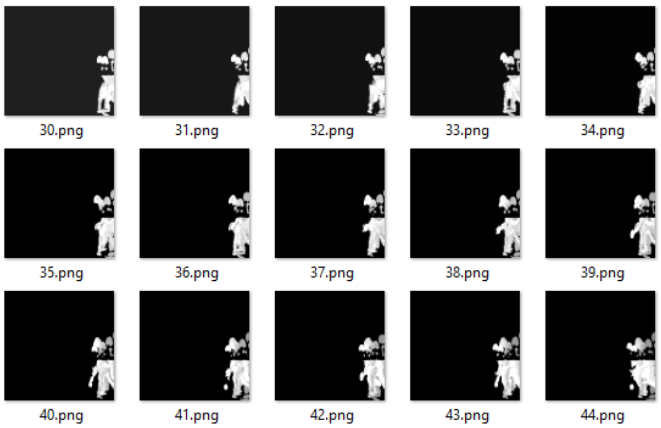

Fig.2 Applying ROI masking

Fig. 3 Output after forgery detection

VI. FUTURE SCOPE

In future we can detect the removed and copy paste part in a video with the help of frames and masking .To detect these different techniques can be applied like DCT, correlation and filters. It can also extend on the real time crime department videos. So that the criminal will be easily identified .It can also be extended with the help of other techniques so that the better results may be produced.

VII. CONCLUSION

This paper deals with the various techniques used in order to tackle the copy paste forgery within the CCTV footages. The digital video tampering in which the contents of videos is modified or changed to make it doctored or fake video. Optical flow and ROI (Region of Interest) masking are the two important techniques used to detect copy paste forgery in CCTV videos in this paper. We have to take out the frames from the given input video before applying the techniques to detect forgery and then we apply ROI mask to separate the foreground and background images from each frames. This method is used to measure the velocities of objects in the video by estimating optical flow between video frames. After calculating the velocity differences between each consecutive frames forgery frames will be detected .Then compress these forgery frames using DWT and use SIFT (Scale Invariant Feature Transform) which is a feature detection algorithm in computer vision to detect and describe the local features in from the compressed frames .Finally we get forgery frames as output.

But these methods do not provide accurate result. In future we can detect the removed and copy paste part in a video with the help of frames and masking .To detect these different techniques can be applied like DCT, correlation and filters. It can also extend on the real time crime department videos. So that the criminal will be easily identified .It can also be extended with the help of other techniques so that the better results may be produced .In order to tackle the other issues in video forgery detection mechanisms are researched over.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 2, February 2021

DOI 10.17148/IJARCCE.2021.10214

REFERENCES

[1]. Video Forgery detection using Hybrid techniques | Computer Science Project Topics
[2]. (PDF) Detection and Localization of Copy-Paste Forgeries in Digital Videos (researchgate.net)
[3]. Copy Create Video Forgery Detection Techniques Using Frame Correlation Difference by Referring SVM Classifier (ijcert.org)
[4]. (PDF) Review of Techniques for Detecting Video Forgeries | IJCSMC Journal - Academia.edu
[5]. Optical Flow - MATLAB & Simulink (mathworks.com)
[6]. ROI-Based Processing - MATLAB & Simulink (mathworks.com)
[7]. Discrete wavelet transform - Wikipedia
[8]. Discrete Wavelet Transform (DWT) — PyWavelets Documentation
[9]. An Image Forgery Detection using SIFT-PCA (ijert.org)
[10]. Scale-invariant feature transform - Wikipedia