Available at: www.sabauni.net/ojs

S.J.I.T.N
Saba Journal of
Information Technology
and Networking

Article

FRAME DUPLICATION FORGERY DETECTION USING PHYSICAL RANDOM OBJECTS

*Tawfiq S. M. Barhoom *, Ahmed J. I. Elaff*
Information Technology Faculty, Islamic University of Gaza

Article info

Article history:

Accepted Jan, 2016

Keywords:

Digital Tampering

Digital Forensics

Image Forgery

Frame Duplication

Abstract

Due to the revolution of image editing video tools, it is easy to tamper with any video by altering, combining or creating new video contents. A common way of manipulation is to duplicate frames to hide objects. We proposed a new reverse algorithm to discover the duplication of the frames to stop theft by stopping the ip-cam in specific places.

* Corresponding author: Tawfiq S. M. Barhoom
E-mail address: tbarhoom@iugaza.edu.ps

Introduction

In the last few years, many social media sites were published to enable users around the world to share their knowledge, life events and their diaries. This makes a huge amount of data that is replicated to be used for defamation. One of the types of media is videos and the tampering with them, which makes the privacy of the internet and its contents less confident.

However, the problem lays on the tampering process before sharing these resources. These videos have turned to be harassment to some people. Another problem is tied to the network resources that are being hacked and edited before publishing.

The video forgery or tampering has two types: Active and passive [1,2,3], the active allows the user to make watermark [4,5]or signature to the videos before publishing and when it is being tampered with, we check the watermark or signature for any editing or changing. This type is rarely used because we can't know if the video really needs to do that or not, and in the online recording system that decreases the performance of the recording frames speed. Another approach is a passive one which means to check the video by several techniques with several purposes such as reversed algorithm. We can detect the changes by a sensor device pattern [6, 7] or reverse post-production techniques such as white balancing. When the DETECTOR finds any changes in the video content the DETECTOR detects that it has been tampered with. The other ones are duplication on regions and frames to hide an object or change its position or make the duplication increase the object number which is used in wars to increase the objects of rockets or military equipment.

In recent years, due to the improvement of network technologies and devices, IP-cam is a device that is connected to the networks to watch the places we want to with low-costs and expenses.

One of the problems of this device is related to connecting it to the network all day. So if any attacker hacks this LAN, this device will be driven by the attacker and will be turned off. The attacker can show any video regardless if the IP-cam is tied to the system or not. One of the attacks is to change the checking system of the video with duplication of frames to hide the thief's personality. And with a corporation with the thief he can steal or ignore the cam recording process.

In this paper we proposed a new method called DETECTOR. The DETECTOR has been added between the video and the system alarm to detect the duplication by using a random animation object. We can compare the frames to ensure that they are no duplicated regions in the specific area in efficient way.

Our methodology includes multiple steps to make this process more efficient such as using Grayscale to speed up the image processing in our online system.

In this paper we will also discuss the process with details, results and evaluation with all measurements taken for the online camera and offline videos.

RELATED WORK

VIDEO INPAINTING FORGERY DETECTION TECHNIQUES

"Inpainting is the process of reconstructing lost or deteriorated parts of images and videos. For instance, in the case of a valuable painting, this task would be carried out by a skilled image restoration artist."[8]

Here inpainting is used to remove objects by filling the gap with adjacent pixel colors as shown in Fig. 1. The difference here is our purpose and usage. Here it was used to hide objects but in our research, we used it to detect frame group duplications to ensure that the video has not been edited.

Fig. 1: The top figure shows a character is that hidden in the lower picture by inpainting

EXPOSING DIGITAL FORGERIES IN VIDEOS BY DETECTING DUPLICATION

It's a paper that talks about how to detect region and frame duplication. Regarding the frame duplication, we can see this example by looking at Fig.2.The figure shows a series of videos captured by the cam of a man who is moving through the camera in the top series but at the bottom the frames are duplicated to hide this person. Compression techniques were used to convert the frames to JPEG instead of PNG ones to make the comparison faster.[11]

Fig. 2: The top figure shows a sequence that show a person and in the bottom one the person is hidden by duplication

Here the tampering (hiding objects) was discovered by checking the repeated frames that were duplicated to hide an object. In our research we do the reverse. We want to check the duplication of our physical object. When the duplication is found with the motion we can detect the duplication where it needs less image processing and faster because we only check the region that the physical object lies on and not whole frame.

ADOBE PREMIERE PRO CC

Adobe Premiere is a program used for video editing and montage for multiple videos. One of the features of the new version called CC, is used to check duplication series in editing processes and not in the full rendered and extracted ones. So it used to check the video duplication in the editing process which is called active forgery and that type is not useful for criminal investigation.

Fig. 3 shows the duplication detecting done to check the colour series. If it's similar that means it is duplicated.[12]

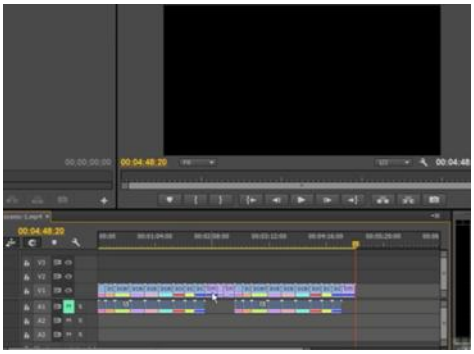

Fig. 3: Duplication detected by watching the similar colours means that this frame is duplicated

System Architecture

In this section we have defined the system components and where the DETECTOR is actually located. The component of the system is an IP-camera for recording the video which is connected by a hosting hardware system to store the recording video through the camera. When there is any problem, the hosting system monitoring software starts the alarm system to close the doors and make a loud sound to inform the police. Our DETECTOR lies between the system that records frames (which can be hacked and store the forgery video) and the alarm system as shown in Fig.4.to check the frames; as we will discuss in the next section. Then if there is a forgery of duplication, the alarm system starts working

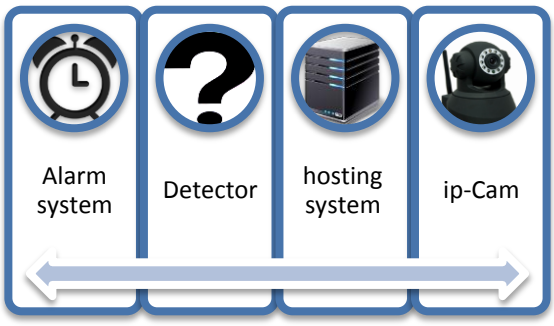

Fig. 4: The components of the system and where the DETECTOR lies

Methodology and Implementation

This paper's experimental implementation is programmed on HTML5. This is a powerful language to handle the pixels and change their colour system, such as grayscale. Not needing to add plug-ins, and good for making image processing online because it handles the video as the image to make processing on it.

The DETECTOR has been tested on different multiple offline videos and online webcams to make a sense of the minimum resolution needed, and the frame rate to make the process faster and efficient.

Before making any process, a random animated object which is animated randomly without animation repetition period will move in specific region in any corner in the camera boundaries it can be a digital clock including the date to ensure that no repeating in the days periods or something else, so the detection will be in this region to ensure that it's not repeated. Our methodology is based on seven steps, as shown in Fig. 5.

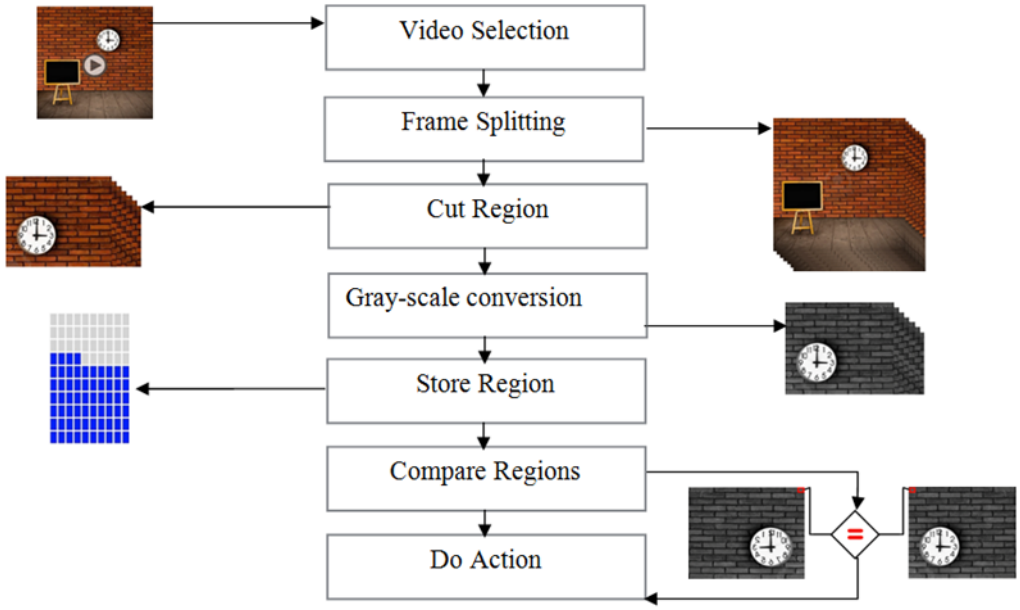

Fig. 5: methodology processes

You can follow these steps to detect the frame duplication forgery:

- ***Video Selection:***

Our experiment is based on taking a number of offline videos to detect if they were tampered with or not. We used a multiple of videos with deferent properties such as different dimensions, multiple colours and different frame rates. And the next step is to apply it by an online IP camera

- ***Split to frames:***

• Because the pixel processing cannot be performed on all the video, we are concerned by the duplication on frames. So we must split the video taken to frames. We didn't mean to take all the video to achieve the performance, but we checked the duplication for multiple random series of frames.

- ***Cut the region:***

Cut the region that contains the physical object to make the process more efficient unless you take all the frames together which we needn't, the process becomes faster.

- ***Grayscale Conversion:***

Convert the taken regions to grayscale unless the RGB makes the process faster.

- ***Store the region:***

Store the regions in the array and sort as the frame sequence in the video.

- ***Compare regions:***

By taking the stored regions and compare their pixels, after a specific amount of time we can detect the duplication.

- ***Do Action:***

Here we detect if there is a duplication region or not. However, if there is duplication, we can do any

action such as turn the alarm on or calling the owner's number.

Experiment Measurements

In this paper, the DETECTOR has been tested for 3 videos where each video is a 2 minutes long. The first one contains one duplication frame every second. The second video has 20 duplication frames distributed randomly. And the last one has no duplication frames. Every video has a 400x600 dimension with a 24 fps frame rate. We tested these 3 videos on the DETECTOR and the error percentage was zero. But the challenge was the time which the DETECTOR has consumed and which was 20 to 40 second for 2 minutes, it depends on the pixel density and the resolution number of the video.

Before the pre-processing grayscale conversion technique, the DETECTOR took approximately 3 times more than now, and if we look to the region comparison, it reduced more time and which can be computed from the following equation:

$$T(Region) = \frac{\text{region } width \times \text{region } height}{original\ width \times original\ height} \times \rho \times 100\%$$

T(Region): the time the DETECTOR does consume for regions.

ρ : the pixel density percent. If the pixels are focused on this region, it will make a variance.

The DETECTOR has been developed in HTML5 JS language which is powerful in color correction to make grayscale, cropping the regions and pixel comparison moreover than it can be used for online cameras as we talked about in the introduction.

Conclusion

In this paper, we have proposed a digital video forgery detection scheme using a random animation object that moves in the camera boundaries. We proposed a 3rd party system between the watching systems and the alarm one to detect the camera stopping or what we called frame duplication. We are using an HTML5 for it is powerful for handling the video as an image and looping on its pixels to make the changes to grayscale. Cutting the regions and comparing the pixels DETECTOR is fast and efficient because it checks regions on grayscale with powerful language.

References

[1] Deshpande, P., & Kanikar, P. (2012). Pixel based digital image forgery detection techniques. IJERA, 2(3), 539-43.

[2] Chittapur, G. B., Murali, S., Prabhakara, H. S., & Anami, B. S. (2014). Exposing Digital Forgery in video by mean frame comparison techniques. InEmerging Research in Electronics, Computer Science and Technology (pp. 557-562). Springer India.

[3] Johnson, M. K., & Farid, H. (2006, September). Exposing digital forgeries through chromatic aberration. In Proceedings of the 8th workshop on Multimedia and security (pp. 48-55). ACM.

[4] Hsieh, C. T., & Wu, Y. K. (2006). Geometric invariant semi-fragile image watermarking us-

ing real symmetric matrix. WSEAS Transaction on Signal Processing, 2(5), 612-618.

[5] Lin, P. L., Hsieh, C. K., & Huang, P. W. (2005). A hierarchical digital watermarking method for image tampers detection and recovery. Pattern recognition, 38(12), 2519-2529.

[6] Khanna, N., Mikkilineni, A. K., Chiu, G. T., Allebach, J. P., & Delp, E. J. (2007, February). Scanner identification using sensor pattern noise. In Electronic Imaging 2007 (pp. 65051K-65051K). International Society for Optics and Photonics.

[7] Chen, M., Fridrich, J., Goljan, M., & Lukáš, J. (2008). Determining image origin and integrity using sensor noise. Information Forensics and Security, IEEE Transactions on, 3(1), 74-90.

[8] Das, S., Darsan, G., Shreyas, L., & Devan, D. (2012). Blind detection method for video inpainting forgery. International Journal of Computer Applications,60(11).

[9] Bayram, S., Avcıbaş, İ., Sankur, B., & Memon, N. (2006). Image manipulation detection. Journal of Electronic Imaging, 15(4), 041102-041102.

[10] Patwardhan, K. A., Sapiro, G., & Bertalmio, M. (2005, September). Video inpainting of occluding and occluded objects. In Image Processing, 2005. ICIP 2005. IEEE International Conference on (Vol. 2, pp. II-69). IEEE.

[11] Wang, W., & Farid, H. (2007, September). Exposing digital forgeries in video by detecting duplication. In Proceedings of the 9th workshop on Multimedia & security (pp. 35-42). ACM.

[12] Detect Duplication Frames Automatically | Adobe Premiere Pro CC [Online]. Last access : 11-2-2015 , Available : https://helpx.adobe.com/premiere-pro/how-to/premierepro-duplicate-frame-detection-cc.html