Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 1 Issue 1, August – 2021, Pages: 24-27

Watermarking for Video Inter-Frame Tamper Detection

P. Keerthana[1], E. Nikita[2]

Received: 6 August 2021 / Accepted: 29 August 2021

Abstract:

Technology advances at the same rate as human beings. Technology comes with both pros and cons. As difficult as it may be to create a video, modifying it is a piece of cake. Today's culture has easy access to video editing tools, making it possible to make changes to video footage. Video fraud cannot be detected by the sagacity of a person. Tampering is the act of making unauthorised changes or additions to video content by tampering with the video's source code or other code. As a result of their frequent use as evidence, digital videos are indispensable in the courtroom. This method uses Particle Imaging Velocimetry (PIV) to locate areas in the video that have been tampered with. Video manipulation may be detected in a variety of ways using this technique.

Keywords— Inter-frame forgery, forencies, PIVdetection

1. Introduction

Video tampering is the act of viscerally altering the content of a video. All it takes to tamper with a video is to add or remove an item or a person from it. There are two kinds of tampering: spatial and temporal. Tampering may be prevented using digital video forensics, which were created to do just that. It helps in figuring out whether a video is real or fake. Intra-frame and inter-frame video manipulation are two methods of video tampering. To tamper with one frame, use inter-frame tampering; to tamper with a video frame, use intra-frame tampering.

Classification of Video-Tampering Attacks

The video may be manipulated in a number of ways, mostly in terms of space and time.

The video content's visual information is tampered with using a Spatial Tampering Attack. Transform, remove, trim, or replace video material as needed. Pixels and blocks are the two ways to accomplish it.

Attack 2: Video tampering: In this attack, the video frame sequence is altered. In the temporal province, you may add, duplicate, remove, or rearrange the frame as needed.

Forgeries may be categorised in a number of ways.

• Inter-frame

• Intra-frame

1). Forgeries that take place between frames

Forgeries that occur between frames are referred to as inter-frame forgeries. Types include: inserting and removing frames, shuffle and replicating frames. Here are some definitions for some often used concepts.

frame insert: a particular frame is interpolated in between the video frames of the sequence.

Frame Removal: Video footage is forged by deleting a certain frame.

Shuffling of the frames is all that's happening in the video, and it's called frame shuffling.

Frame Replication: A frame replica is a video that uses frames from the original to create new frames.

2) Forgeries committed inside a single frame of reference

A video consists of a sequence of still pictures or video frames. It's possible that fakes will be found throughout the video.

Forgeries at the pixel level are those that take place in a different frame from the original.

Object level forgeries, such as frame insertion or removal, are types of forgeries that occur at the object level.

Overture for Video Tamper Detection with a Detailed Precise

Video Tampering Detection has two preliminaries:

There are two approaches: active and passive.

Approaching the Situation Actively

Digital apogee and digital signatures are effective methods for detecting intentional manipulation in content ownership and consortium offences. The apogee and signatures help to establish who someone is. Due to the many faults in the active method, a signature or watermarking is required during the recovery stage.

Individual reporting is incorporated into the recovery step at the time of transmission. So much for the active method, which calls for using specialised equipment like custom-built cameras. Compression and noise are the sources of some of the durability issues with watermarks and signatures.

P. Keerthana[1]

B. Passive Approach

The passive approach to digital security is analysed as a step forward. As opposed to the aggressive approach, the passive approach takes a more conservative approach. No prior knowledge of video counterfeiting is needed for this technique to function. It may be applied with any technology. Methodologists call it the Passive-Dark Approach. Using this overture, it's suggested that the actual videos will have some kind of video implied tract. A video's fictional content has been inflated. These analyse a video clip for a wide range of various subjects by taking a segment of it. A passive video tamper detection method is needed to get around the active strategy's drawbacks. In comparison to the active dignitary strategy, the passive method has proved to be better. Eyewitness information is used and no further samples of knowledge or hardware are required. Fake video data is the only thing it uses; it has an unique demeanour that makes it ineligible for use with real video data.

2. Areas Affected by Video Forgery

Nowadays, films are used for a wide range of purposes including entertainment, video surveillance, legal education, and advertising. No matter how much of a backlash there is, the coincidence and the location where it is utilised are what determine how effective it is.

Video forgery has opened up a new market:

Surveillance Video as an Example:

Videos from camera systems are readily available in public places including airports, train stations, and retail malls. Copying, duplicating, or removing particular sections or frames from a video clip may enhance other public places. It's feasible to record a certain spatial event or people at a particular location at a given time. It's impossible to ensure that the security camera's recording of the recycled footage, which serves as confirmation of the original, is correct in this situation.

In-Depth Examinations

The assessment and analysis of video in contractual material as a barometer for goals is carried out. In video falsification, a fake affirmation or criteria is inserted to hide an incompatible event, item, or idea. A wide range of places, including shops, restaurants, malls, banks, and parks, have video evidence available to the authorities, and this evidence may be helpful in a number of circumstances. In order to maintain their confidence, they use a method known as disputative analysis.

C. Authorities of the law

Images and films are sufficient proof in contractual courts and common beliefs. It's critical to check if the videos you're seeing are genuine. The video confirmation was not abused in any way. Using this method, gangster mae gets a fake video confirmation and avoids going to jail.

D. Defamation

In movies and campaigns, a visual shock is repeated to dishonour an identity or conceal facts via video trickery. In our everyday lives, services like Sapp and Facebook allocate community posting, which is why this happens.

3. Related Work

In order to identify video tampering, several research are expanding their focus on video forgeries. Zhang et al. [4] found a way to identify video forgery by looking at the ghost shadow artefact left behind after painting a moving object has been erased. Because it is unable to determine where a specific object is forged, this technique is more suited for the identification of copies in paintings rather than inter-frame forgeries. According to Connote et al [5,] a video clip's ballistic movement may be used to identify a counterfeit. The sole constraint is that the moving object must have projection. Cho and his comrades A technique of frame-to-frame optical movement was described in [6]'s frame insertion and removal. A technique developed by Bruce D. Lucas and Takeo Kanade, known as the Lucas-Kanade method, forms the basis of the Lucas-Kanade approach [7]. Wang et al. [8] carried out a similar study on optical movement and assessment aberration detection for inter-frame forgery detection. Wang et al. [9] developed an SVM classifier to identify inter-frame fraud using the Consistency of Correlation Coefficient of Gray Values (CCCoGV) isolated from other video frames. In [6,] Wang and colleagues [10] utilised an SVM classifier on an optical movement hinge to discover faked classification. The SVM classifier needed to be instructed on the statistical distribution count of the regiment optical values. Based on the classification of the SVM, the video forgery detection carried out by Upadhyay et al. The real difference between the inter-frames was recovered and converted to binary representation before distilling the statistical local information. For video inter-frame manipulation detection, Zheng et al. [12] presented the Block-wise Brightness Variance Descriptor (BBVD) as a strong method with high sensitivity and low computation time. This method relies on pixel grey value block subtraction to work. There is no effect on the original video if you use one of these techniques to insert a forged frame. This is applicable in the real world. The

bulk of methods are only 90% reliable and are mainly used to identify inserted frames..

4. Proposed Plan

Recognizing video that has been altered is possible with the use of the displacement field. Cross correlation is used in this instance to analyse the interframes one by one. To perform this operation, open the Fast Fourier Transform window on your computer.

$$Pc(u,v)=F\text{-}1((F(I(x,y,t))F(I(x,y,t+1)^*) \quad (1)$$
$$Argmax(u,v)Re(Pc(u,v)) \quad (2)$$

Where I(x,y,t) & I(x,y,t+1) are the query windows at (x,y) position in t & t+1 frame .The displacement field intensity is expressed as

$$DFIh(t)=\sum \sum|u(x,y,t)| \quad (3)$$
$$DFIv(t)=\sum \sum|u(x,y,t)| \quad (4)$$

Frame with low DFI value are excluded. Three frames are get sampled as a single frame with maximum DFI. It introduces some abnormalities in the DFI.

$$Pfh(t)=(MDFIh(t+1) + MDFIh(t-1)/MDFIh(t+1) *MDFIh(t- 1))*MDFI(t) \quad (5)$$

$$Pfv(t)=(MDFIv(t+1) + MDFIv(t-1)/MDFIv(t+1) *MDFIv(t- 1))*MDFI(t) \quad (6)$$

Distinct peaks in the characteristic identify tampering. The video is one of a kind if it doesn't have a peak. One peak in at least one sequence indicates that a frame was deleted. Two peaks in the sequences indicate that the frames have been duplicated. Frames are classified as either I-Frame, P-Frame, or B-Frame. In I-Frame, the frame is compressed without referring to the previous frame in any way. The B-Frame stores the data from the preceding frame. In P-Frame, changes may be made to the previous frame. In a collection of pictures, each frame is called a Grouping. An I-Frame and many P- and B-Frames make up the design. The resilience of the DPF is calculated in the prediction frame. Before calculating the tampered location, it counts the number of Blocks in the current, previous, and future frames.

5. Experimental Results

Fig. 1. Example of importing video

Fig. 2. Example of frame conversion

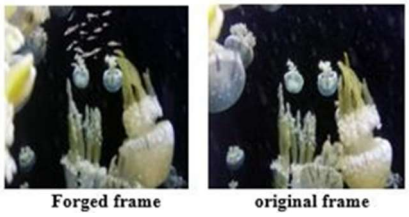

Fig. 3. Examples of forged and original frame

6. Conclusion

We went over how to accomplish Particle Imaging Velocitimetry in this approach. Forged frames, such as frame insertion, removal, shuffling, and duplication, are briefly covered in this approach. Nowadays, it is a really effective strategy.

REFERENCES

[1] Ainuddin Wahid Abdul Wahab, M. A. (2014). Passive Video Forgery Detection Techniques: A Survey. 2014 10th International Conference on Information Assurance and Security. IEEE.

[2] Staffy Kingra, N. A., "Video Inter-Frame Forgery Detection: A Survey," Indian Journal of Science and Technology, Vol. 9, 2016.

[3] Forensics. ACM Digital Library Ashish Kumar Kushwaha, A. P. (2015). Video Forensic Framework for Video.

[4] J. Zhang, Y. Su and M. Zhang, “Exposing digital video forgery by ghost shadow artifact,” in Proc. of the First ACM workshop on Multimedia in forensics, 2009.
[5] V. Conotter, J. O’Brien and H. Farid, “Exposing digital forgeries in ballisticmotion,” in IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 283-296, 2011.
[6] J. Chao, X. Jiang and T. Sun, “A novel video inter-frame forgery model detection scheme based on optical flow consistency,” in Y. Q. Shi, H. J. Kim, F. Perez-Gonzalez (eds) The International Workshop on Digital Forensics and Watermarking, Lecture Notes in Computer Science, vol 7809, Springer, Berlin, Heidelberg 2012.
[7] B. D. Lucas and T. Kanade, “An iterative image registration technique with an application to stereo vision,” in Proc. of the Imaging Understanding Workshop, pp. 121-130, 1981.
[8] W. Wang, X, Jiang, S. Wang, M. Wan and T. Sun, “Identifying video forgery process using optical flow,” Springer Berlin Heidelberg, pp.244- 257, 2013.
[9] Q. Wang, Z. Li, Z, Zhang and Q, Ma, “Video Inter-Frame Forgery Identification Based on Consistency of Correlation Coefficients of Gray Values,” Journal of Computer and Communications, vol 2, pp.51-57, 2014.
[10] Q. Wang, Z. Li, Z. Zhang and Q. Ma, “Video Inter-Frame Forgery Identification Based on Optical Flow Consistency,” Sensor & Transducers, vol. 166, no. 3, pp. 229-234, 2014.
[11] S. Upadhyay and S. K. Singh, “Learning Based Video Authentication using Statistical Local Information,” International Conference on Image Information Processing, 2011.
[12] L. Zheng, T. Sun, Y. Q. Shi, “Inter-frame video forgery detection based on block-wise brightness variance descriptor,” Springer International Publishing, pp. 18-30, 2014.
[13] Y. Wu, X. Jiang, T. Sun and W. Wang, "Exposing video interframe forgery based on velocity field consistency," 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, 2014, pp. 2674-2678.
[14] I. Grant, "Particle image velocimetry: a review," Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science 211, no. 1, pp. 55-76, 1997.
[15] B. Iglewicz, D. C. Hoaglin, “How to Detect and Handle Outliers,” Milwaukee (Wisconsin): ASQC Quality Press, vol. 16, 1993.
[16] D. Vazquez-Padin et al., "Detection of video double encoding with GOP size estimation," 2012 IEEE International Workshop on Information Forensics and Security (WIFS), Tenerife, 2012, pp. 151-156.
[17] A. Gironi, M. Fontani, T. Bianchi, A. Piva and M. Barni, "A video forensic technique for detecting frame deletion and insertion," 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, 2014, pp. 6226-6230.
[18] Sowmya K. N, H. R. Chennamma, “A Survey On Video Forgery Detection,” in International Journal of Computer Engineering and Applications, Volume IX, Issue II, 2015.
[19] Misbah U. Mulla, Prabhu R. Bevinamarad, “Review of Techniques for the Detection of Passive Video Forgeries,” in International Journal of Scientific Research in Computer Science, Engineering and Information technology, vol. 2, no. 3, 2017.
[20] Chee Cheun Huang, Ying Zhang, Vrizlynn L. L. Thing, ‘Inter-frame Video Forgery Detection Based on Multi-Level Subtraction Approach for Realistic Video Forensic Applications’, IEEE 2nd International Conference on Signal and Image Processing, 2017.
[21] Rohini Sawant and Manoj Sabnis, “A Review of Video Forgery and Its Detection,” in Journal of Computer Engineering (IOSR-JCE), vol. 20, no. 2, Ver. III, March/April 2018.