International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

Tampering Detection in Video Inter-Frame using Watermarking

P. Keerthana[1], E. Nikita[2], R. Lakkshmi[3], R. Suguna Devi[4]
[1,2,3]*B.E. Student, Department of ECE, Anand Institute of Higher Technology, Chennai, India*
[4]*Assistant Professor, Department of ECE, Anand Institute of Higher Technology, Chennai, India*

***Abstract*: Nowadays technology is growing along with us. Technology overtures both pros and cons. creating a video is not an easier one but editing the video is more compatible by using many editing software. In existing world altering the video content is made easier due to easy accessibility of video editing software. Video forgeries are not visibly identified by a human sagacity. Tampering involves pottering the content of the video in order to make an unapproved modification / content. Digital videos plays a virile role in judiciary department as they are consider as an evidence for most of the cases In this technique we use Particle Imaging Velocitimetry (PIV) to find where the video has been fiddled. This method is very efficient to provide which type of tampering has occurred in the video**

***Keywords*: Inter-frame forgery, forencies, PIVdetection**

1. Introduction

Manipulating the video by changing the content viscerally refers to video tampering. Tampering the video is as easy as inserting or deleting the object or a human in the video. Tampering can be done in two provinces spatial and temporal. In order to solve the problem of tampering and maintain the originality of the video digital video forensics have been evolved. It helps to detect the whether the video is a veritable one or not. Tampering of video can be done in two ways inter frame and intra-frame tampering. Doing tampering within an individual frame is referred as inter-frame tampering whereas in intra-frame, tampering can be done sequence wise in the frame of the video.

A. Classification of Video Tampering Attacks

Tampering the video can be done in various ways mainly on spatial and temporal province.

1) Spatial Tampering attack: Here the visual information of the video content is altered. It can be morphing, deleting, cropping or replacing the video content. It can be performed in two levels pixel level and block level.
2) Tampering attack: Here the sequence of the frame gets altered in the video. It can be done by adding the frame, duplicating the frame, removal of frame or by shuffling the frame in the temporal province.

B. Types of Forgeries

Videos are commonly classified as:

- Inter-frame
- Intra-frame

1) Inter-frame forgeries

Forgeries that are happening in the entire frame are said to be inter-frame forgeries. They are further classified as frame insertion, frame-removal, frame shuffling, and frame replication. Let us see the brief outlook of these terms.

Frame Insertion: In the sequence of video frames, a particular frame is added in between the video content.

Frame Removal: In the given video content, forgeries are done by removing the particular frame.

Frame Shuffling: The video content which is provided is given with misalignment of the frames that is nothing but shuffling of the frames.

Frame Replication: Video containing the replicated frames of the original video frames are said to be replica of frames.

2) Intra-frame forgeries

A video is a sequence of images or frames. In the video, forgeries can happen in the full frame.

Pixel level forgeries: Forgeries that are happened in the separate frame at pixel level.

Object level forgeries: Forgeries that are happened in the separate frame like frame insertion or frame removal.

2. A Detailed Precis for Video Tampering Detection overture

There are two preliminary overture for Video Tampering Detection:

- Active Approach
- Passive Approach

A. Active Approach

Active tampering detection techniques are digital apogee and digital signatures are useful accuracy content proprietorship and consortium offense. The apogee and signatures is used for identity. There are many imperfections in the active approach so it desires to embed a signature or watermarking at the recovery stage.

The reporting of an individual person is embedded in the recovery stage at the sending time. This terminates the utilization of active approach is the use of original hardware like specially rigged cameras. There are some problems on the durability on watermarks and signature is the cause such as compression and noise.

B. Passive Approach

Passive approach is investigated as a progress in digital safeguard. The passive approach works in the opposition of the active approach. This approach works without the constraint of the particular hardware it does not desire any eyewitness information about video forgery. This approach is called as Passive-Dark Approach.

The expectation made by this overture get some video implicit tract in original videos. The spurious of a video is decorated are modified. These countenance excerpt from a video and evaluate them for various distinct ideas. To conquered the inability in the active approach the need of passive approach for video tampering detection is made. Passive approach confirms to be improved than the active dignitary. It works on the eyewitness knowledge without the use of additional knowledge sample and hardware concern. It absolutely confides on the usable forged video data and peculiar countenance left out the right of original video data.

3. Areas affected by video forgery

The convention of videos in various utilization like entertainment industry, video surveillance, legal and law tutorials, advertising imprint its unparalleled role in today's life. Notwithstanding its backlash depends on the coincidence and the space location it is service.

Distinct space stirred by video forgery is:

A. Video Surveillance

Videos are accessible from the surveillance system instant at the Airports, Railway Stations, Shopping Malls. Other communal Space would be efficiently modified copying, duplicating or removing convinced article or frames within the video progression It would be achievable to embed into the video, convinced space affair or people instant at peculiar space and cameras at peculiar time. In this case, it is challenging to assure the video recycled as confirmation original one is absolutely reported by the surveillance camera.

B. Forensic Investigations

The measure of objectives scrutiny and appraisal of video in contractual material. The falsification of video is to hide an incompatible affair or article or idea to be embed specious confirmation or criterion. Video confirmation can be possessed from distinct areas such as stores, restaurants, malls, banks, parks whatever may be benefits the police in distinct cases. Thus disputative analysis use of assure their boldness.

C. Law Enforcement

Images and videos handle as appropriate confirmation in contractual courts and familiar ideas. It is critical to assure the authority of videos. The video confirmation has not borne any dereliction. Using this technique gangster make benefits of spurious video confirmation are hesitant in the courts and spared their suffering.

D. Defamation

Video falsification in movies and campaigning has an conspicuous shock recycled to disgrace an identity or obscure fact. This is because of convention of allocation of communal publishing such as what Sapp, face book performance a brunt in our daily lives.

4. Related work

In the video forgery detection, there are various studies are increasing in order to find the video tampering. Zhang et. al [4], found a method to find video forgery by analysing ghost shadow artefact created when a particular moving object is removed from the in painting process. It is more applicable to copy in painting detection but not to inter-frame forgery detection why because this method cannot find where the particular object is forged. Connote et al [5] explicated a method for forgery detection hinge on ballistic movement of video sequence. Restriction for this particular method is that we should have projection in the object that is moving. Chao et. al. [6] described a method of frame to frame optical movement in frame insertion and frame removal. The optical movement extraction is depending on the method proposed by Bruce D. Lucas and Takeo Kanade and is generally assigned to as the Lucas-Kanade method [7]. Wang et.al. [8] done a same inquisition on inter-frame forgery detection through optical movement and aberration detecting of evaluation. Wang el at [9]. implemented the Consistency of Correlation Coefficient of Gray Values (CCCoGV) which were separated from other video frame training a Support Vector Machine (SVM) classifier to find inter-frame forgery. Wang et. al. [10] used on optical movement hinge in[6] to find forged classification based on SVM classifier. The aspect to build to teach the SVM classifier was hinge on statistical distribution count of the regiment optical values. Upadhyay et. al. [11] transacted a temporal and spatial video forgery detection hinge on SVM classification. Actual difference between the inter-frame has been retrieved and converted to binary format before distillation the statistical local information. Zheng et al. [12] proffered a potent algorithm design namely Block-wise Brightness Variance Descriptor (BBVD) to find video inter-frame tampering with accurate and minima reckoning time. This technique is hinge on block based subtraction of pixel gray values. The restriction in these methods of forger frame insertion is not relevant to the original video. This is applicable to the realistic world. Most of the techniques provided are only with accuracy of 90% and is only for detecting inserted frame.

BBVD algorithm will be useful for good accuracy.

5. Proposed plan

Tampered video can be detected using displacement field. Here the inter-frames are compared in a sequence wise using cross correlation. It is done by Fast Fourier transform window.

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

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

$$DFI_h(t)=\sum \sum|u(x,y,t)| \quad (3)$$
$$DFI_v(t)=\sum \sum|u(x,y,t)| \quad (4)$$

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.

$$Pf_h(t)=(MDFI_h(t+1) + MDFI_h(t-1)/MDFI_h(t+1) *MDFI_h(t-1))*MDFI(t) \quad (5)$$

$$Pf_v(t)=(MDFI_v(t+1) + MDFI_v(t-1)/MDFI_v(t+1) *MDFI_v(t-1))*MDFI(t) \quad (6)$$

Discrete peaks in the feature identify the tampering type. (1) If there is no peak then video is an original one. (2) One peak in at least any one sequences indicates the deletion of frame. (3) Two peak in the sequences indicates the frame duplication. Frame of are of three types namely I-Frame, P-Frame, B-Frame. In I-Frame the frame is compressed without referring the other frame. B-Frame contains the data that is altered from the preceding frame. In P-Frame changes can be done in previous frame. A sequence of frame forms a Group of Pictures. It contains I-Frame with many P-Frame & B-Frames. The robustness of DPF in prediction frame is estimated. It determines the count of Block in the present, previous & next frames & finally identifies the tampered location.

6. Experimental results

Fig. 1. Example of importing video

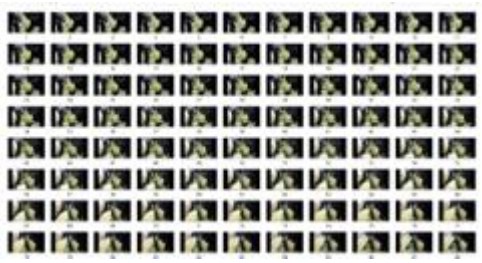

Fig. 2. Example of frame conversion

Fig. 3. Examples of forged and original frame

7. Conclusion

In this particular method, we discussed how to perform Particle Imaging Velocitimetry. In this technique, forged frames like frame insertion, removal, shuffling, duplicating is explained briefly. It is very efficient method nowadays.

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.