International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Review of Techniques for the Detection of Passive Video Forgeries

Misbah U. Mulla, Prabhu R. Bevinamarad

M.Tech, Department of Computer Science and Engineering, B.L.D.E.A'S Dr.P.G.Halakatti College of Engineering and Technology, Vijayapur, Karnataka, India

ABSTRACT

Due to the availability of various types of digital cameras and video technology giving rise to multimedia data for communication purpose. Digital videos play an important role in court rooms, in news, defense and for security purpose to ensure their authenticity and integrity is a important task and also a challenge. On the other hand due to advancement of technology and availability of various editing software tools has made the digital video tampering possible allowing it to modify, edit and alter easily, the digital forensics demands effective research in this field to find different techniques to detect the video forgeries. The various techniques are proposed by the researchers for video tampering detection. But passive techniques are based on detecting the forgeries without the need of pre embedded information .This review paper focuses on various passive techniques which are used to detect forgeries in videos.

Keywords: Video Forgeries, Passive Techniques.

I. INTRODUCTION

In Today's world the use of digital videos is increasing rapidly and are considered as important means of information exchange and due to availability of various editing software tools which are easy to use ,in expensive and portable.They enable the user to easily alter, modify and edit any part of digital video.This illegitimate behaviour raises a concern towards the authenticity of the videos and demands the digital forensics to carry out effective research in this field.Digital forensics deals with identification of various kinds of tamperings in videos.

In this paper,we are giving firstly the classification of video tampering attacks ,in the second section the classification of the video forgery detection is discussed and finally there is a survey on different passive approaches for detecting video forgeries.

A. Classification of Video Tampering Attacks

The videos are tampered in various ways, the video tampering attack is classified into spatial tampering,temporal tampering and spatio-temporal tampering.

1.Spatial Tampering attack: In this the modifications are performed on the contents of the frame which alters the visual information in videos.The various operations performed during the spatial tampering attack are morphing, cropping ,adding or removing the content from the video ,replacement and so on.Spatial tampering can be done at two levels pixel level and block level both leads to the alteration of video frames[1].

2.Temporal Tampering attack: In this the modifications are done on set or sequence of frames ,this tampering effects the visual information's timing sequence.In this type of attack addition of frames, removal of frames, shuffling of frames and reordering of frames is done through temporal tampering.The temporal tampering attack can be done at frame level,scene level and shot level[1].

3.Spatio-Temporal Tampering attack:It is a combination of both spatial tampering and temporal

tampering in this type of attack modifications are done on both the visual information as well as frame sequences in the same video,the combination of inter frame tampering and intra frame tampering falls under this category.This type of tampering is basically carried out at scene level[1].

Figure 1 depicts the classification of video tampering attack

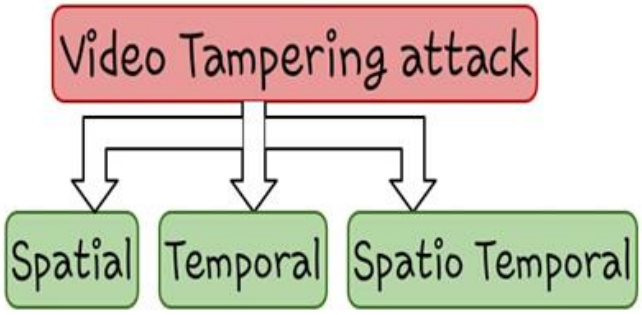

Figure 1. Classification of video tampering attacks

B. Classification of Video Forgery Detection Approaches

Video forgery detection is broadly classified into two types

a.Active approach
b.Passive approach

Active approach makes use of the information from videos as reference such as,digital watermark, digital signature or hash value.The active approach is further classified as full reference and reduced reference based upon the reference information.In full reference the actual video and the forged video both are available to identify tamperings in digital video.If the reference information exists as digital signature or digital watermarking to find out tamperings than such approach falls under reduced reference.

In passive approach the forgeries are detected based on certain assumptions and algorithms in which no preembedded or reference information available the only available data is the contained information of suspected video and from this the tamperings should be identified[2],so it is classified as No reference.

The Figure 2 depicts the classification and categorization of digital video forgeries detection**.**

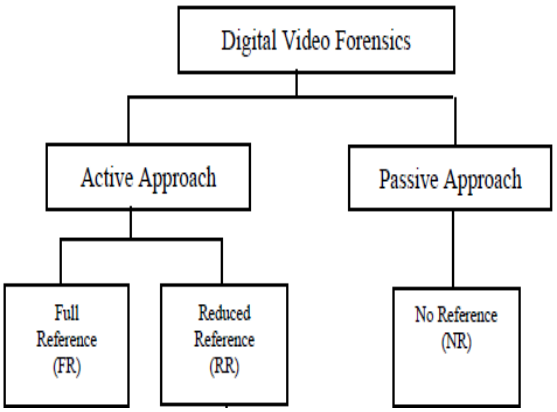

Figure 2. Classification of Digital video forgeries detection.

II.LITERATURE SURVEY

The literature survey has been done to study in detail and to analyse the passive video forgery detection techniques,some of the important passive techniques applied for detecting video forgeries has been discussed in this review paper.

In[3] the authors have introduced a passive approach based video forgery detection technique its main aim is to detect and to localize temporally the inpainting forgeries in digital videos using optical flow inconsistencies,the algorithm has two main steps,in the first step the video is checked whether it is authentic or inpainted,in the further step the temporal localization is carried out, the working of the method is the optical flow is calculated for each video sequence that leads to the generation of optical flow matrices for every sequence of frame later when the optical flow of the specific region of source frame is compared with the frames which are inpainted than that will not show any motion in their corresponding source frame this will prove that in the video the objects which are moving have been removed using inpainting.Hence ,this technique efficiently detect and temporally localize the tamperings in videos caused by copy-paste inpainting and also the experimental results shows that it has good performance when compared to previous techniques.

In[4] the authors have introduced a video forgery detection method based on compressive sensing which is used to detect the deletion of moving object in videos and changing the tampered area with the information available around that object. In this the moving foreground is separated from background and gives the traces of forgeries left in forged video.The results obtained from experiments gave efficiency and robustness in terms of performance but the limitation of

this method is that it takes long detection time for finding out forgeries in videos.

In [5] the authors have presented a copy-move forgery detection in videos based on cellular automata and local binary patterns. The copy move forgery in videos is done by copying few frames and then pasting those frames at a different position but sequence remains the same.In this method first the feature set is defined for each and every frame which usually gives texture and other related properties of every frame. Each frame is further divided into small blocks which are overlapped, than cellular automata is used find rules for every block the rules shows the change in the intensity of the blocks than finally the histograms of the blocks are taken as features to detect the presence of frames which are duplicated. This method gave accurate detections when tested with various cases, but the issue is that sometimes the frames are mistakenly identified as not copied. This method is also able to find duplicated frames from the video which have similarities.

In[6] the authors have proposed a technique for detecting frame duplication in videos using similarity analysis. This method consist of two stages,In the first stage the features of each frame are obtained via SVD (Singular Value Decomposition).Next, the Euclidean distance is calculated between features of each frame and the reference frame. After dividing the video sequence into overlapping sub-sequences, the similarities between the sub-sequences are calculated, and then those video sequences with high similarity are identified as candidate duplications. In the second stage, the candidate duplications are confirmed through random block matching,random block matching is used to confirm these candidate duplications, this method provided good detection accuracy and efficiency in performance.

In[7] the authors have presented video forgeries detection technique based on the pixel estimation,which detects double quantization arising from the tampered video double compression. The method uses principles of estimation theory to detect double quantization. Each pixel of a given frame is estimated from the spatially collocated pixels of all the other frames in a Group of Picture (GOP). The error between the true and estimated value is subjected to a threshold to identify the double compressed frame or frames in a GOP. In this from frame each and every pixel is estimated in a Group of Picture (GOP),the difference between the actual pixel and estimated pixel value is computed and compared against the threshold to identify the tampered frames in the video.This technique gave efficient results.

In[8] the authors have worked on inter frame forgery detection based on Lucas Kanade optical flow consistency, based upon the fact that the inter frame forgery that may be frame addition or frame deletion will effects the optical flow consistency.The first step is generation of optical flow for the given video,than based upon the optical flow the frame deletion or insertion tamperings are detected separately according to their procedures.The forgery is detected and their tampering model is identified according to the type of tampering based upon whether frame deletion or insertion forgery, if no such tamperings are found in the video than such videos are termed and considered as normal .Experiment results have shown that for frame insertion forgery detection the precision rate is 98% recall rates is 95% but the detection rates for frame deletion detection are lower when compared with the frame insertion tampering detection.

In[9] the authors have worked on passive method for detection of video forgeries using markov models to the motions in videos.The motion in videos can be found using prediction error frame,motion vectors and motion information ,finally the markov model is applied on the obtained motion outcomes and finally Support Vector Machine(SVM) is used for pattern recognition and classification .

In[10] the authors have presented a novel technique for detection of temporal and spatial copy paste forgery in digital videos based upon the compression properties and Histogram of Oriented Gradients(HOG) features, for spatial forgery detection to set the cell size the image thresholding mechanism is applied, than the HOG features are generated for each block that further leads to generation of individual block descriptors and matching is carried out ,In temporal forgery detection based upon the compression properties frames are taken than the HOG features are extracted for each block and block descriptors are generated and compared with the block descriptors of spatial blocks and checked whether they match or not.The experimental results shows that this method gave good

results in detection of temporal tamperings in videos and also have better performance when compared to other copy paste forgery detection techniques.

In[11] the authors have introduced a blind video tampering detection based on the source features fusion.The forgeries are detected from various frames it starts with the extraction of quantization residue and noise features in inter and intra frame blocks and than these are transformed to the cross-modal subspace next the correlation properties are extracted from this and checked whether the tamperings exist or not. Retouching ,double compression and re-sampling operations usually alter the correlation properties of the pixel sub blocks between the frames and as well as within the frames which indicates the difference between the forged or unforged video,the accuracy rate of this method is 92% for the mul timodal residue features fusion which are transformed to cross modal subspace.

In[12] the authors have worked on the technique for the detection of video forgeries by detecting Motion-Compensated Edge Artifact,it is based on the fact that frame deletion from MPEG video sequences effects the temporal correlation by decreasing it and further leads to larger motion compensated error ,the deletion of frame effects the Motion compensated edge artifact (MCEA) value which is calculated by using defined method and procedure, the vibrancy of before and after frame deletion is measured as impact factor ,and the impact factor varies significantly if several frames are deleted from the video sequence and based upon this the video is marked as tampered or authentic.But the limitation of this method is that the impact factor does not work for the videos with low motions.

In[13] the authors have worked on the detection of tamperings in videos based on noise characteristics.In this method the photon shot noise from the video is considered for detecting the tamperings,from the observed intensity the variance is computed and the variance is closely related to its means than by relating the mean and variance the Noise level Function is formulated which is the clue for detecting forgeries in digital videos by using temporal averaging the noise characteristic for each pixel is calculated and leads to the authenticity for every pixel and provides accuracy.

In[14] the authors have presented a method for detecting forgeries in videos by using correlation of noise residues.In this method first the original frame is substracted from its noise free version the result obtained is the noise residue for each frame ,wavelet denoising filter is used for finding the noise free version .In the next step each frame is divided into non overalapping blocks of size N×N,from two consecutive frames the correlation noise residue is calculated and in last step the forged blocks are identified by analysing and going through the block level correlation properties.The GMM model and bayesian classifier are used for classification purpose ,The experimental results shows that this method provides accurate and good detection results.

In [15] the authors have introduced a forgery detection methods for deinterlaced and interlaced videos ,for deinterlaced videos the correlations are measured which are generated by the camera or by deinterlacing algorithm and by using this it can be shown that if the video is tampered than it effects and disturbs the correlation, For interlaced videos the motion of fields of the frame and its neighbouring frame is computed using the defined method and procedure and it should be same and equal ,these motions are measured and if tamperings are present in video than it effects and changes this relationship ,based upon this the video can be marked as forged,if motions remain same than the video is marked as not tampered and is normal.

In[16] the authors have presented video cut detection technique using frequency domain correlation.In this method by using spatial decomposition the video frame is divide into 32x32 size of blocks ,normalized correlation in frequency domain is carried out between the blocks and the overall correlation coefficient for every individual frame is found based on accepting the similar blocks and by not accepting the dissimilar blocks.Three different methods are used to compare the performance those are likelihood ratio, color histogram comparison and displaced frame differencing.This method does not consumes more time and when compared this method gave good results by providing reliability.

III.CONCLUSION

The digital video forensics is one of the most important and growing research field in recent years.There are various techniques available for the detection of video forgeries based upon passive approach and few of them are discussed above.Every technique has its own advantages and limitations as some methods can detect simple modifications in digital videos instead of the complex heterogeneity resulting from multimedia or detecting the tamperings in the hidden content of digital video. On the other hand few methods can detect complex forgeries but they have few constraints and limitations such as detection of only spatial tampering or conventional temporal copy paste tampering but not complex temporal copy paste tamperings from the videos, and also some of the techniques are time consuming and are not cost effective.so,there is a need to develop video forgery detection techniques which are economically feasible, fast and robust.Also there is a demand from many areas such as judicial forensics,information security etc to develop robust and standard techniques for detection of wide variety of tamperings in digital videos to overcome the challenges related to passive video forgery detection.

REFERENCES

[1]. Sowmya K.N and H.R. Chennamma, "A Survey on Video Forgery Detection",in International Journal of Computer Engineering and Applications, Volume IX, pp. 17-27 , February 2015.

[2]. Shashank Sharma and Sunita V Dhavale,"A Review of Passive Forensic Techniques for Detection of Copy-Move Attacks on Digital Videos",in IEEE 3rd International Conference on Advanced Computing and Communication Systems (ICACCS),2016.

[3]. Shobhita Saxena,A.V.Subramanyam and Hareesh Ravi, "Video Inpainting Detection and Localization Using Inconsistencies in Optical Flow",in 2016 IEEE Region 10 Conference (TENCON) — Proceedings of the International Conference, pp .1361-1365,2016.

[4]. Lichao Su ,Tianqiang Huang and Jianmei Yang, "A video forgery detection algorithm based on compressive sensing" , Springer Science and Business Media New York ,pp. 6641-6656 , 2014.

[5]. Dijana Tralic, Sonja Grgic and Branka Zovko-Cihlar, "Video Frame Copy-Move Forgery Detection Based on Cellular Automata and Local Binary Patterns", in IEEE X International Symposium on Telecommunications (BIHTEL), October 2014.

[6]. Jianmei Yang ,Tianqiang Huang and Lichao Su "Using similarity analysis to detect frame duplication forgery in videos", Springer Science and Business Media New York ,pp. 1793-1811,2014.

[7]. A.V. Subramanyam and Sabu Emmanuel, "Pixel Estimation Based Video Forgery Detection",in IEEE 2013 ICASSP ,pp.3038-3042,2013.

[8]. Juan Chao ,Xinghao Jiang and Tanfeng Sun, "A Novel Video Inter-frame Forgery Model Detection Scheme Based on Optical Flow Consistency",Springer-Verlag Berlin Heidelberg , pp. 267–281, 2013.

[9]. Kesav Kancherla and Srinivas Mukkamala, "Novel Blind Video Forgery Detection Using Markov Models on Motion Residue", Springer-Verlag Berlin Heidelberg, pp. 308–315, 2012.

[10]. A.V. Subramanyam and Sabu Emmanuel, "Video forgery detection using hogfeatures and compression properties" ,in IEEE International Conference on Multimedia signal processing. pp.89 - 94 , 2012.

[11]. Julian Goodwin and Girija Chetty, "Blind Video Tamper Detection Based on Fusion of Source Features",in IEEE International Conference on Digital Image Computing: Techniques and Applications,pp. 608-613,2011.

[12]. Yuting Su, Jing Zhang and Jie Liu, "Exposing Digital Video Forgery by Detecting Motion-compensated Edge Artifact", in IEEE International Conference on Computational Intelligence and Software Engineering(CiSE), 2009.

[13]. Michihiro Kobayashi, Takahiro Okabe, and Yoichi Sato, "Detecting Video Forgeries Based on Noise Characteristics",Springer-Verlag Berlin Heidelberg , pp. 306–317, 2009.

[14]. Chih-Chung Hsu , Tzu-Yi Hung, Chia-Wen Lin, Chiou-Ting Hsu,"Video Forgery Detection Using Correlation of Noise Residue", in IEEE 10th workshop on multimedia signal processing , pp .170-174,2008.

[15]. Weihong Wang and Hany Farid, "Exposing Digital Forgeries in Interlaced and Deinterlaced Video", IEEE Transactions on Information Forensics and Security, Vol. 2, NO. 3, pp .438-449 ,September 2007.

[16]. S. V. Porter ,M. Mirmehdi and B. T. Thomas, "Video Cut Detection using Frequency Domain Correlation",in 15th International Conference on Pattern Recognition, pp .409-412, 2000.