International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 12: December 2015, pp 60 - 62 www.aetsjournal.com ISSN (Online) : 2394-6237

A Novel Approach For Inter Frame Copy Move Forgery Detection

Shamna Parveen.S, Dr.D.Palanikkumar

Abstract— With sophisticated video editing software, it is becoming rapidly easy to forge a digital video without any visual evidence. One of the most common video forgery process on video is to remove some frames and then insert into another manner. one of the common type of video forgery is copy move forgery. It can be performed in two levels inter frame and intra frame level. In this paper, we propose a new method for detecting interframe copy move operation by using mean coefficients of correlation value between the adjacent frames. This method is a good than existing method in terms of accuracy, call rate, and precision.

Keywords— video forgery, inter frame forgery, intra frame forgery, digital forensics, analog forensics.

I. INTRODUCTION

Nowadays verification of a digital data has become more complex. This is because of easy availability ,low priced and simply operatable digital devices like mobile phones, digital camera etc. together with the flourishing of high-quality data processing tools and algorithms, has made signal acquisition and processing accessible to a wide range of users. As a result, a single image or video could have been processed and altered many times by different users. all type of modification made by the single video cannot be called as fake video. But the modification made for some intentional value of specific user to cozen another person or society.

A. Digital Forensics

Digital forensics[2] is a branch of forensic science.

The main aim is to find the diffects and forgery present in a digita content.

According to [2] Forensics science emerged in the last decade in response to the escalation of crimes committed by the use of electronic devices as an instrument used to commit a crime or as a repository of evidences related to a crime. [2] During2001,a first definition for digital forensics science was given in the first Digital Forensic Workshop.

B. Branches of Digital Forensics

Digital forensics science is classified into several sub-branches[1]: computer forensics, network forensics, database forensics, mobile device forensics and recently multimedia forensics

Shamna parveen.s, PG Scholar, Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore, Tamilnadu, India (Email:shamnaparvin@gmail.com)

Dr..D.Palanikkumar, Professor/ Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbatore,Tamilnadu,India,(Email:palanikkumard@gmail.com)

.i) Computer Forensics: In computer forensics, forensic investigators want to extract noviciate facts from the computer data. The investigators typically follow a definitive type of protocols. First step is to physically extracting the features in computer in order to make sure it cannot be accidentally contaminated, investigators make a digital copy of the hard drive and all investigation is done on the digital copy. a variety of techniques and proprietary are used for forensic applications to examine the hard drive copy. The operations include searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files.

ii) Network Forensics: In Network forensics, the investigator analyses the network events continusly in order to find security issues. a network forensic analyse the database and transaction for identifying evidence of a fraudulent activities

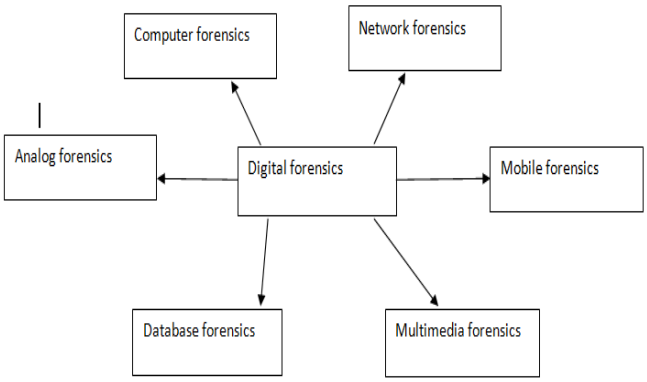

Figure 1: Forensics

iii) Mobile Forensics: in Mobile device forensics, investigate on various mobile devices internal memory and communication ability.

iv) Database Forensics: Database forensics deals with database for investigate any fraudulent transaction within database is carried out.

v) Multimedia Forensics: In multimedia forensics, the main aim of investigator is to digital representations of parts of reality, such as images, videos or audio files captured from a digital devices.

The multimedia forensics is able to demonstrate that such digital evidence.that can be used as trial because of its reliability and authenticity or otherwise demonstrate the contrary[2].

C. Copy Move Video Forgery

One of the most common image manipulations is copy and move forgery, where portions of the image is used to conceal a person or

object in the scene of the same image. Since textured areas have same properties like colour, dynamic range, noise variation. it will be imperceptible for human eye investigating for incompatibilities of image properties. The fashion and advertising industries are frequent users of copy-move. This technique is also commonly called as cloning. By copying regions of the original image and pasting into other areas of the same image.actors/actresses can be made to look perfect by removing wrinkles, and unwanted features.

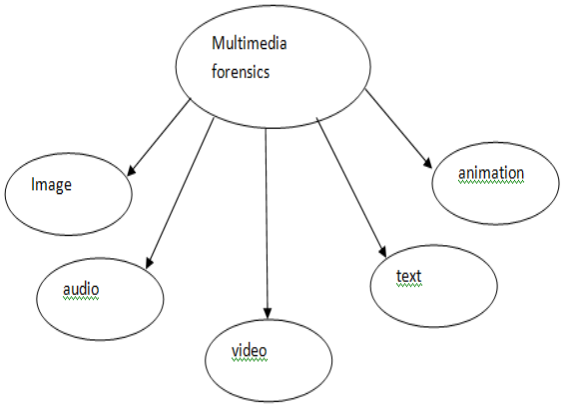

Figure 2:branches of multimedia forensics.

Intraframe forgery can be done at block or pixel level. In both cases objects of video frames are altered. Block is a specific area on the frame and pixel is smallest portion in the video sequences.

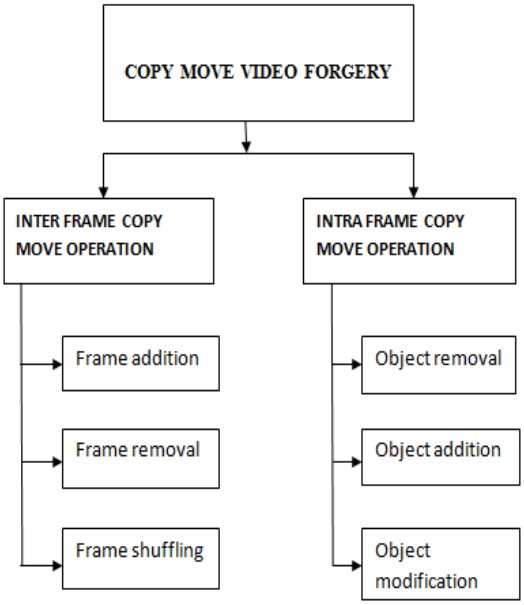

Figure 3: Different Levels Of Copy Move Video Forgery.

Operations performed intraframe forgery can be cropping & replacement, morphing, modifying, content addition and removal. Interframe forgery is performed on adjacent frames. Such attacks are mainly affecting time information in video. Common attacks are: addition of frame, removal of frame, reordering of frame, and shuffling. spatiointerframe forgery is a association of interframe and intraframe tampering. Frame sequences and video objects are altered in the same video. It is done at frame level. Intra frame tampering and inter frame tampering combination is appear in here.

II. EXISTING WORK

There are different existing methods are available for finding interframe forgery. Qi Wang, Zhaohong Li[4] proposed video inter-frame forgery identification based on the grey value of different frame block. In original video the grey value of each frame is constant but in fake video it will be changed. In this paper to identify the inter frame forgery, first step is ti extract the features in each frame then normalization and quantization process was applied to find the consistent correlation gray values. Then SVM is used to test the consistency value.

In a new inter frame copy move forgery detection algorithm based on video sub-sequence finger prints [5]. DCT coefficients of different frame are calculated to extract the matched pairs. This method shows better and and simple metric for the similarity measurements. This algorithm achieves a good tradeoff between computational complexity and detection capability. Another approach, which is the main interest of this paper, Paolo Bestagini and Simone Milani[6] proposed a detection algorithm that allows localize to detect video forgeries and better localization. The main idea behind this method is to reveal fake area in the three dimensional space by using cross correlation value of 3x3 block.. The algorithm detects the fake area by examining the footprint residual value computed from the adjacent frames, and robust against different compression. In the second case, the forgery is detected by analyzing the correlation value.

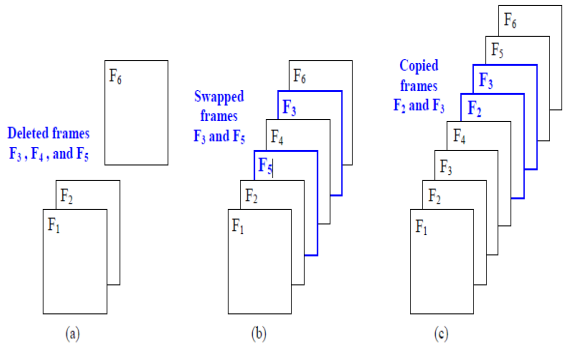

Figure 3: (a) deleted frame,(b)swapped frame and (c)copy move forgery.

In velocity field consistency approach[8] is used to detect both inter frame deletion and duplication. in this paper, a partial image velocity metric(PIV) is used to find the displacement between the any two adjacent frame in video. To

avoid low velocity value due to the camera error maximum sample technique is applied .three consecutive frame is selected for maximum sampling. but localization of fake area is not accurate.

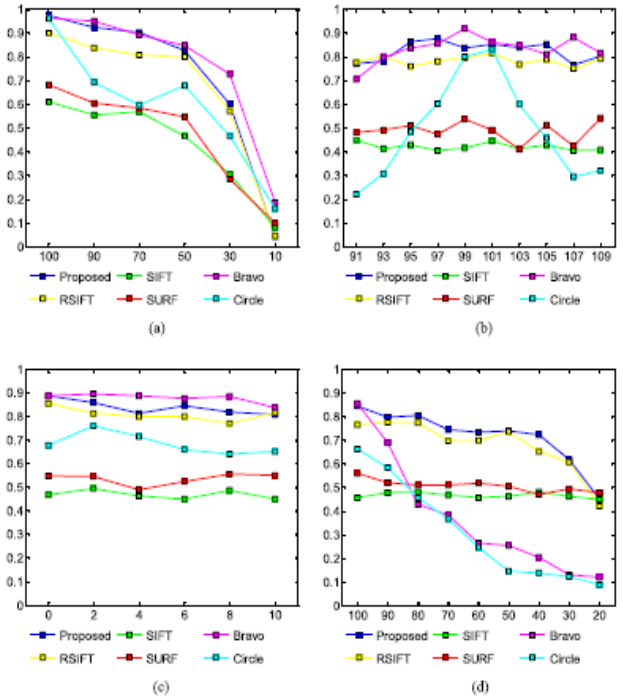

Figure 4: Precision results at the pixel level (a) Down sampling; (b) Scaling;(c) Rotation; and (d) JPEG Compression[7]..

III. Proposed Work

The value of Frame count will be high if a video is manipulated by copying and paste the video frames in to some other location in the video. Inter frame forgery, these copied frames may be appears in some other order of a video . at the video level,the all frames of a video sequence can be copied and pasted into another video such that the copy of a source video is created.

The proposed inter frame forgery detection technique can achieve better and accurate copy move video forgery detection and localization. The proposed method first transforms a video into different frames. Each frame segmentation algorithm is applied based on the quality. If the video quality is low then the intial segmentation size must be taken as large.If the video quality is high then the initial segmentation size must be taken as small. After selecting the size the segmentation algorithm is applied. Mostly for segmentation the SLIC (Simple Linear Iterative Clustering Approach) is used to create frame blocks. The second step is to extract the feature from each frame block. The Scale-Invariant Feature Transform (SIFT) [7] was applied to the host images to extract feature points, which were then matched to one another.

When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In recent papers [7] the speeded up robust features (surf) were applied to extract features instead of SIFT. However, although these methods can locate the matched key points, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate

Finally, for each from block feature is compared with adjacent pairs of frame .to locate the forgery region mean correlation coefficient value of each pair of adjacent frame block is calculated. Value should not exceed than value one. If the value is greater than one than corresponding block is copy move forged block. This method can produce better detection result than the existing system.

IV. Conclusion

Thus in the new video forgery detection method is applied for inter frame copy move forgery detection. This method use a mean correlation calculation to detect the interframe copy move forgery. In the existing technique, the detection accuracy is very low and time complexity is large. The new inter frame copy move forgery detection technique may achieve better accuracy than existing system. But the time complexity is same as existing technique.

The future work must be focused on the complete video forgery detection by combining all type of forgery.

References

[1] https://en.wikipedia.org/wiki/Digital_forensics
[2] *"Introduction To Digital Forensics"Eforensics Magazine Vol 03,No 11,Issue 11/2014november Issn 2300-1986.*
[3] "A Survey On Video Forgery Detection" Sowmya K.N. 1, H.R. Chennamma International Journal of Computer Engineering and Applications, Volume IX, Issue II, February.
[4] Qi Wang, Zhaohong Li, Zhenzhen Zhang, Qinglong Ma, "Video Inter-Frame Forgery Identification Based on Consistency of Correlation Coefficients of Gray Values" Journal of Computer and Communications, 2014, 2, 51-57 Published Online March 2014.
[5] Sreelekshmi Das and Gopu Darsan "Blind Detection Method for Video In painting Forgery" International Journal of Computer Applications (0975 – 8887) Volume 60– No.11, December 2012
[6] Paolo Bestagini, Simone Milani "Local tampering detection in video sequences" MMSP'13, Sept. 30 - Oct. 2, 2013, Pula (Sardinia), Italy.978-1-4799-0125-8/13/$31.00 °c 2013 IEEE.
[7] Chi-Man Pun , Xiao-Chen Yuan and Xiu-Li Bi "Image Forgery Detection Using Adaptive over segmentation And Feature Point Matching" IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, August 2015.
[8] Yuxing Wu And Xinghao Jiang "Exposing Video Inter-Frame Forgery Based On Velocity Field Consistency" 2014 Ieee International Conference On Acoustic, Speech And Signal Processing (Icassp)