A Survey on Forensic video Analysis

Prof. Chandrakanth Biradar[#1], Dr. Shubangi D.C [#2],
[#1]*Department of Computer Science*
PDA College of Engineering Kalaburagi
[#2]*Department of Computer Science and Engg*
V.T.U ,RO, Centre for PG Studies , Kalaburagi

***Abstract*— Video tampering is a process of malicious alteration of video content, so as to conceal an object, an event or change the meaning conveyed by the imagery in the video. Video tampering detection aims to find the traces of tampering and thereby evaluate the authenticity and integrity of the video file. Nowadays, videos are core part of live entertainment in television and movies, and they are breathing of real entertainment world. People believe movies and video snaps in everywhere of digital media. Digital Photo images are everywhere: on the covers of magazines, in newspapers, in courtrooms, and all over the Internet. We are exposed to them throughout the day and most of the time, we trust what we see. Trusting unbelievable video may create sensation over the news and gossip media world. The identified telecasted and forecasted video's truthfulness is challenging in multimedia.**

With the innovations and development in sophisticated video editing technology and the wide spread use of video information and services in our society, it is becoming increasingly significant to assure the trustworthiness of video information. In surveillance, forensics, medical and various other fields, video contents must be protected against attempt of manipulation. Such malicious alterations could affect the decisions made based on these videos. A lot of techniques are proposed by various researchers in the literature that assure the authenticity of video information. These techniques can be classified into active and passive (blind) techniques.

This paper present a survey on passive video tampering detection methods. Passive video tampering detection methods are classified into the following three categories based on the type of forgery they address: Detection of double or multiple compressed videos, Region tampering detection and Video inter-frame forgery detection. Here we are also making a survey of some of the recent passive methods for video tampering detection in the literature proposed so far and critically reviewing them by listing the strengths and weaknesses of each of them.

***Keywords*—–Digital video, Surveillance, Forensics, Video Tampering, Video Authentication**

1. INTRODUCTION

Digital videos are being used every day for security purposes in many fields, and they are visually impressing and convincing than still images. Videos are widely used in lawsuits. But the biggest threat to the video is the availability of easy to edit video editing tools to anyone. In many cases the meaning of the video is distorted by inserting, removing or duplicating group of frames. Such type of malicious attack on videos is called tampering. While it is certainly true that tampering with a digital video is more time consuming and challenging than tampering with a single image, increasingly sophisticated digital video editing software's are making it easier to tamper with videos.

Of course not every video forgery is equally consequential; the tampering with footage of a pop star may matter less than the alteration of footage of a crime in progress. But the alterability of video undermines our common sense assumptions about its accuracy and reliability as a representation of reality.

In some applications the authenticity of video data is of paramount interest such as in video surveillance, forensic investigations, law enforcement and content ownership. For example, in court of law, it is important to establish the trustworthiness of any video that is used as evidence. In the case of surveillance videos such as the ones captured by the surveillance cameras situated at railway stations or airports to monitor the activities, it would be fairly simple to remove a certain activity, people or even an event by simply removing a handful of frames. On the other hand it would also be feasible to insert, into this video, certain objects and people, taken from different cameras and in different time. A video clip can be doctored in a specific way to deframe an individual. On the other hand criminals get free from being punished because the video (used as evidence), showing their crime cannot be proved conclusively in the court of law. In the case of surveillance systems, it is difficult to assure that the digital video produced as evidence, is the same as it was actually shot by camera. In another scenario, a news maker cannot prove that the video played by a news channel is authentic. These are the instances where modifications cannot be tolerated.

Digital watermarking has been firstly proposed as a valuable mean to cope with these problems, by imperceptibly embedding a message into documents. Such message can later be detected and/or retrieved and used to disclose possible copy-rights violations or manipulations. This technology is said to be active, since it requires known information to be embedded onto the content at the time of recording (or a person to embed it at the time of sending) to make a forensic analysis possible. This may represent a limitation to digital watermarking techniques, requiring a special equipped hardware or a post processing of the content. In a scenario, where digital watermarks or signatures are not available, passive (or blind) approaches have to be applied to protect and verify the integrity of multimedia contents. The basic idea of passive forensics techniques is that the alteration of a digital media, if performed properly, may not leave visual trace of its occurrence, but it alters the underlying statistics of the content. An accurate analysis can be carried out, without any prior knowledge about the content and alterations can be taken as evidence of forgery or help in tracing back the history of the content.Video forgery process can be roughly divided into two classes: intra-frame and inter-frame. Intra frame forgery is done frame wise whereas inter frame involves attack to a sequence of frames. The process of identifying video forgery spans in three different phases such as source identification, detecting video doctoring and compression analysis which is depicted in Fig.1. Source identification includes methods for identifying the camera which is used to take a particular video. In this phase a video is declared as authentic if the camera identified by this method match with the one that is provided as evidence. The identification of whether the video is tempered by inserting, deleting or duplicating frames comes under video doctoring analysis. Compression analysis check whether the video is double compressed. Double compression can be regarded as an evidence for tampering since a genuine video undergoes only single compression.

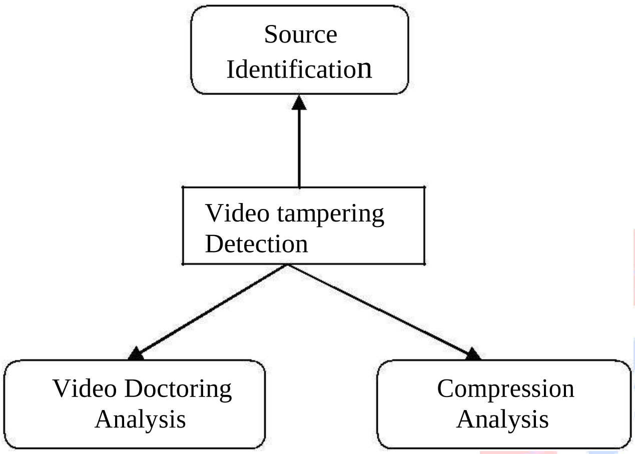

Fig. 1 Forgery Detection Phases

2. LITERATURE REVIEW

A video forgery detection technique by exploiting the correlation of noise residue is proposed in [1]. In this method, block level correlation values of noise residual are extracted as a feature for classification and the distribution of correlation of temporal noise residue is modeled as a Gaussian mixture model.

The authors adopt a bottom up approach as shown in Fig.2 for the forgery detection based on block level temporal noise correlation. The various steps in the process are,

Noise residue of each video frame is extracted by taking the difference between the original frame and its noise free version.

Each video frame is partitioned into non-overlapping blocks with size NxN. Calculate the noise residue between the same spatially indexed blocks of two consecutive frames

Tampering can be located by using the statistical properties of noise correlations.

Coarse classification can be obtained by simple thresholding.

Based on this classification a GMM model is applied to characterize the noise correlation between tampered and non-. The GMM model para meters are estimated using the EM algorithm and the optimum threshold is derived using maximum-likelihood estimation and Bayesian classifier.

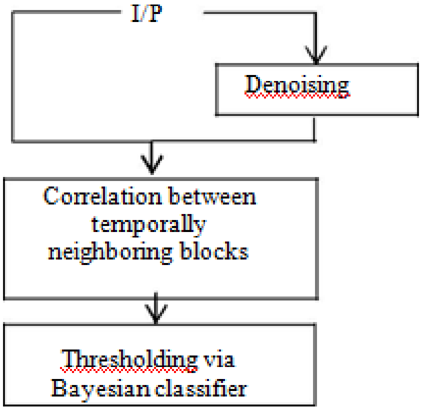
I/P
Denoising
Correlation between temporally neighboring blocks
Thresholding via Bayesian classifier

Fig.2 Flow chart of Noise Correlation method

The major drawback of this method is that it is not reliable for low-quality video such as low-bandwidth internet streaming videos and also the correlation feature is not stable for applications with dynamic scene.

A common form of tampering videos is to clone or duplicate frames or parts of a frame to remove people or objects from a video. A computationally efficient technique for detecting this form of tampering is discussed in [2]. In this the authors propose two different methods for frame duplication and region duplication.

2.1. Frame duplication

Partition a full length video sequence into short overlapping subsequences. A temporal correlation matrix of size nxn is to be defined such that the $(i,j)^{th}$ entry is the correlation coefficient between the i^{th} and j^{th} frame of the subsequence. It embodies the correlation between all pairs of frames in a subsequence and if there is little change across the sub-sequence then the matrix entries will each have a value near 1, whereas, if there is significant change, then the matrix entries will have values closer to -1.

The spatial correlations of each frame within a subsequence can be computed by first tiling each of the frame with m non overlapping blocks and finding the correlation matrix with its $(i,j)^{th}$ entry be the correlation coefficient between the i^{th} and j^{th} blocks. By suitably thresholding the temporal and spatial correlation matrices the tampering can be identified.

2.2. Region duplication

For a pair of frames $f(x,y,T_1)$ and $f(x,y,T_2)$, the spatial offset (d_x,d_y) corresponding to a duplicated region between these frames is to be calculated.

First calculate the normalized cross power

Where $F(w_x,w_y,T_1)$ and $F(w_x,w_y,T_2)$ are the Fourier transforms of the two frames, * is complex conjugate, and || . || is complex magnitude. Then take the inverse Fourier transform of $P(w_x,w_y)$. Phase correlation techniques are used to estimate spatial offsets by extracting peaks in p(x,y). Peaks in positions other than (0,0) represents the presence of duplication.

The method is effective in detecting large areas of duplication but fails to locate small regions.

A doubly compressed MPEG video sequence introduces specific static and temporal statistical perturbations whose presence can be used as evidence of tampering. Such a type of analysis is adopted in [4]. The major steps in the detection method are

Convert video into frames

Extract I frames and Mean motion error of P frames
Take the histogram of the extracted I frame

Find DFT of the histogram and motion errors

If there are spikes in the DFT plot it can be regarded as an evidence of tampering

The flowchart of the method is given in Fig.4

The method in [5] concentrates on video object contour and its Adjustable Width Object Boundary (AWOB) to trace the forgery in small scale by analyzing detail coefficients of Non-Subsample.

.

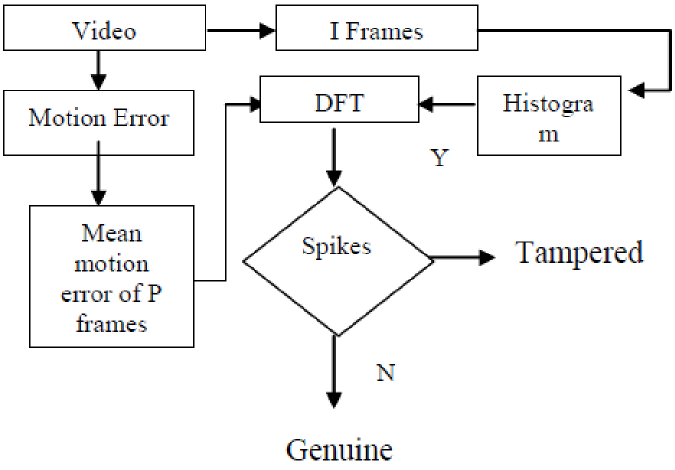

Fig. 4 Flow chart of double compression detection

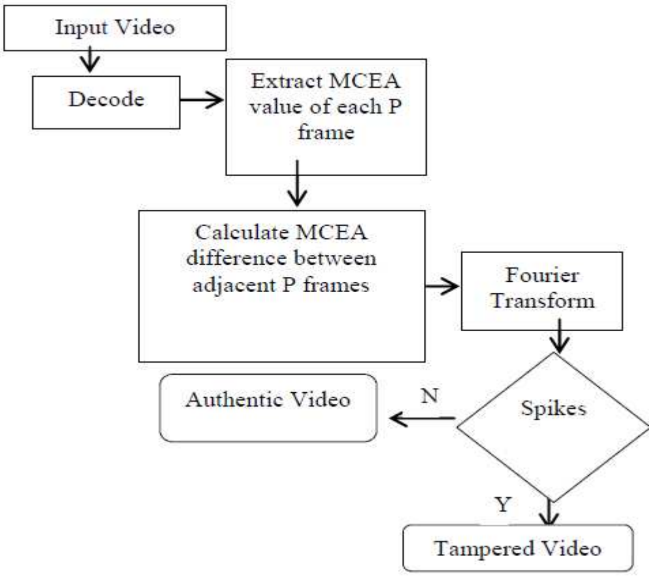

Fig.3 Flow chart of MCEA based method

Video forgery based on object consists of four steps: object detection, object manipulation, motion interpolation and background in-painting. For digital video forensics, the first step is object detection. Then, the object contour and its bounding area can be located and the statistical features are extracted in order to verify the originality and integrity of digital video. The Contour let transform is a two dimensional extension of the wavelet transform using multi scale and directional filter banks. The Contourlet expansion is composed of basis images oriented at various directions in multiple scales, with flexible aspect ratios. The flow chart of the method is shown in Fig.5.

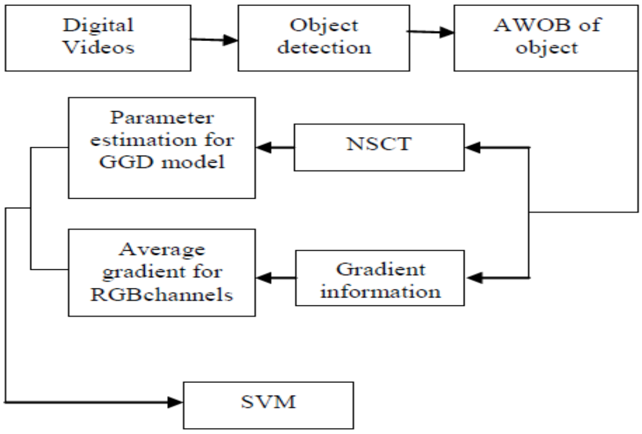

Fig.5 Flow chart of Non subsampled Contourlet based method

When frame duplication occurs, it is expected that there exists some duplicated clips in the processed video. Since there is a high correlation among these duplicated clips, the similarity between two clips as a feature can be used to find out those duplicated clips. A coarse to fine approach based on this concept is proposed in [6] and composed of three stages: candidate clip selection, spatial correlation calculation and frame duplication classification. To screen duplicated candidates in the temporal domain, the histogram difference of two adjacent frames in RGB color space is adopted. To evaluate the similarity of image content, a block-based algorithm is used to measure spatial correlation of each corresponding frame between the query clip and the candidate one. The duplicated frames can be localized by the analysis of spatial and temporal features. The overall procedure is given in Fig.6

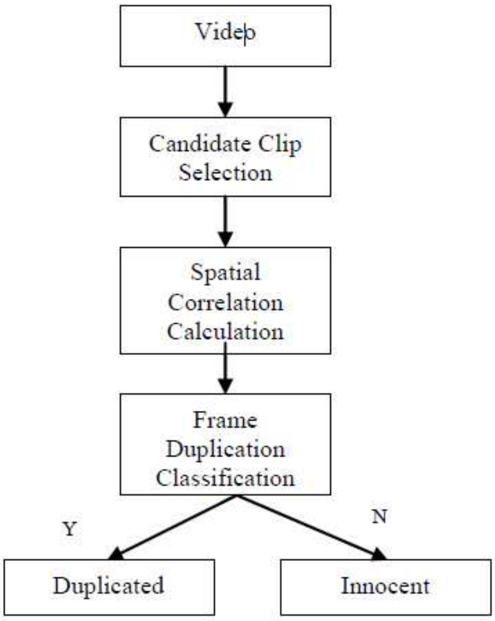
Videp
Candidate Clip Selection
Spatial Correlation Calculation
Frame Duplication Classification
Y
N
Duplicated
Innocent

Fig.6 Flow chart of Spatio-temporal analysis

A method that reveals video forgeries and localizes them in the spatio-temporal domain is discussed in [7]. It is completely an unsupervised approach. It detects whether a spatio temporal region of a sequence was replaced by either a series of fixed images repeated in time, or a portion of the same video taken from a potentially different time interval. It treats image based attack and video based attacks separately.

2.2.1. *Image based attack*

First analyze the zero motion video residual difference between pixels in the same spatial position on consecutive frames. Residual zero implies that the image is splices. Then search for frames with a region of zero residual that remains constant in time. Then find the largest 3D bounding volume that contains only zero residual values.

2.2.2. *Video based attack*

It first divides the residual matrix into non overlapping blocks and then search for similarity between each blocks.

In the image based tampering this method finds 75% of forged pixel and in video based tampering 90% of duplicated block sequences.

In [8] the authors propose a method for detecting insertion and deletion of whole frames in digital videos. The method is applicable even when different codecs are used for the first and second compression, and performs well even when the second encoding is strong as the first one. In this the authors focus on fixed- Group Of Pictures (GOP) encoding, where the GOP structure and size are kept constant. When encoding a frame, the encoder divides it in macro blocks (MBs) and codes each MB separately: MBs belonging to I frames are always encoded without making reference to other frames, while MBs belonging to predictive- coded frames, while MBs belonging to predictive-coded frames may also be encoded making reference to previous frames or even future frames. MBs that are encoded without temporal predictions are referred to as intra-coded and denote them as I MB and those MBs that are encoded making reference to other frames are referred to as P MB. Finally the encoder has the possibility to skip a MB, if this MB can be directly copied from a previous frame: these MBs are denoted as S MB s.

Variation Prediction Footprint (VPF) is the measure used for detection. Suppose a video is encoded twice using a fixed GOP size G_1 for the first encoding and a fixed GOP G_2 for the second encoding, and that only I and P frames are used. When a frame originally encoded as intra is re encoded as a P frame, an anomalous decrease in the number of S-MB s occur, together with an increment in the number of I-MB s.

Notations:
I(n) – number of intra coded MB’s used within the nth
frame s(n) – number of skipped MB’s

The set P is defined as containing only those frames that show, simultaneously, a higher number of I-MB and a smaller number of S-MB compared to the previous and following frames. Then for frames in P the strength of the VPF is evaluated by summing the product of the slopes as:

$$v(n) = \left|\big(i(n) - i(n-1)\big)\big(s(n) - s(n-1)\big)\right| + \left|\big(i(n+1) - i(n)\big)\big(s(n+1) - s(n)\big)\right|$$

While the v(n) is set to zero for frames not in P.

For a tampered video the plot of VPF show periodic peaks. This measure can also be used for recognizing the insertion and deletion separately.

This method detects tampering even if the second encoding is stronger than the first one. The drawback of this technique is that it cannot detect frame manipulations when the attacker removes or inserts a whole GOP.

3.CURRENT CHALLENGES

The five major challenge areas for digital forensics, gathered from a survey of research in the area:

1. The complexity problem, arising from data being acquired at the lowest (i.e. binary) format with increasing volume and heterogeneity, which calls for sophisticated data reduction techniques prior to analysis.

2. The diversity problem, resulting naturally from ever-increasing volumes of data, but also from a lack of standard techniques to examine and analyze the increasing numbers and types of sources, which bring a

plurality of operating systems, file formats, etc. The lack of standardization of digital evidence storage and the formatting of associated metadata also unnecessarily adds to the complexity of sharing digital evidence between national and international law enforcement agencies [Scanlon and Kechadi, 2014].

3. The consistency and correlation problem resulting from the fact that existing tools are designed to find fragments of evidence, but not to otherwise assist in investigations.

4. The volume problem, resulting from in-creased storage capacities and the number of devices that store information, and a lack of sufficient automation for analysis.

5. The unified time lining problem, where multiple sources present different time zone references, timestamp interpretations, clock skew/drift issues, and the syntax aspects involved in generating a unified timeline.

Numerous other researchers have identified more specific challenges, which can generally be categorized according to Raghavan's above classification. Examples include Garfinkel [2010], Wazid et al. [2013], and Karie and Venter [2015].

It is widely agreed that the volume of data that is potentially relevant to investigations is growing rapidly. The amount of data per case at the FBI's 15 regional computer forensic laboratories has grown 6.65 times between 2003-2011, from 84GB to 559GB [Roussev et al., 2013]. One cause of this is the growth in storage capacities that has occurred in recent years. Additionally, the increasing proliferation of mobile and (IoT) de-vices adds to the number of devices that require examination in a given investigation. Beyond the magnitude of the data, the use of cloud services means that it may not be clear what data exists and where it is actually located.

As advanced mobile and wearable technologies have continued to become more ubiquitous amongst the general population, they also now play a more prevalent role in digital forensic investigations. Over the past decade the capabilities of these smart devices have reached a point where they can function at a level near to that of the average household computer and are currently only limited by processing power and storage capacity. This contributes to the diversity problem, where a greater variety of devices become candidates for digital forensic investigation (e.g. Baggili et al. [2015] has reported on forensics on smart watches). Mobile and IoT devices make use of a variety of operating systems, file formats and communication standards, all of which add to the complexity of digital investigations. In addition, embedded storage may not be easily removable from devices, unlike for traditional desktop and server computers, and in some cases a devices will lack persistent storage entirely, necessitating expensive RAM forensics.

Investigating multiple devices also contributes to the consistency and correlation problem, where evidence gathered from distinct sources must be correlated for temporal and logical consistency. This is often performed manually: a significant drain on investigators' resources. The requirements for RAM forensics also becomes pertinent in cases of anti-forensics, where a digital criminal takes measures to avoid evidence being acquired, including the creation of malware that resides in RAM alone. The increasing sophistication of digital criminals' activities is also a substantial challenge.

Other issues include limitations on bandwidth for transferring data for investigation, the volatility of evidence, the fact that digital media has a limited lifespan that may possibly result in evidence being lost, and the increasing ubiquity of encryption in modern communications and data storage.

The following sections concentrate on a number of important emerging trends in modern computing that contribute to the problems outlined above.

3.1 Internet-of-Things

The Internet-of-Things (IoT) refers to a vision of everyday items that are connected to a network and send data to one another. Juniper Research [2015] estimate that there are already 13.4bn IoT devices in existence 2015, and they expect this figure to reach 38.5bn by 2020. These IoT de-vices are typically deployed in two broad areas: in the consumer domain (smart home, connected vehicles, digital healthcare) and in the industrial domain (retail, connected buildings, agriculture). Some IoT devices are commonplace items that have Internet connectivity added (e.g. refrigerators, TVs), whereas others are newer sensing or actuation devices that have been developed with the IoT specifically in mind.

The IoT has the potential to become a rich source of evidence from the physical world, and as such it poses its own unique set of challenges for digital forensic investigators [Hegarty et al., 2014]. Compared to traditional digital forensics, there is less certainty in where data originated from, and where it is stored. Data persistence may be a problem. IoT devices themselves typically have limited memory (and may have no persistent data storage). Thus any data that is stored for longer periods may be stored in some in-network hub, or sent to the cloud for more persistent storage. This therefore means that the challenges related to cloud forensics (as discussed below in Section 2.2) will likely apply in the IoT domain also.

Already, some efforts have begun to analyze IoT devices for forensics purposes (e.g. Suther- land et al. [2014] on smart TVs), however this work is in its early stages at present. The heterogeneous nature of IoT devices, including differences in operating systems, file systems and communication standards, adds significantly to the complexity, diversity and correlation problems for forensic investigators.

Ukil et al. [2011] outline some security concerns of IoT researchers, which feed directly into the desires of forensic investigators, incorporating issues such as availability, authenticity and non-repudiation, which are important for legally-sound use of the data. These are ad-dressed using encryption technologies, which are easy to incorporate into computationally powerful devices that are connected to mains energy. However it becomes more of a challenge for smaller, battery-operated, computationally-constrained devices, where such considerations may be sacrificed. This has inevitable consequences for the usefulness of the data in a legal context.

3.2 Emerging Cloud Computing or Cloud Forensic Challenges

Usage of cloud services such as Amazon Cloud Drive, Office 365, Google Drive and Drop box are now commonplace amongst the majority of Internet users. From a digital forensics point of view, these services present a number of unique challenges, as has been reported in the 2014 National Institute of Standards and Technology's draft report [NIST, 2014]. Typically, data in the cloud is distributed over a number of distinct nodes unlike more traditional forensic scenarios where data is stored on a single machine. Due to the distributed nature of cloud services, data can potentially reside in multiple legal jurisdictions, leading to investigators relying on local laws and regulations regarding the collection of evidence [Simou et al., 2014, Ruan et al., 2013]. This can potentially increase the time, cost and difficulty associated with a forensic investigation. From a technical standpoint, the fact that a sin-gle file can be split into a number of data blocks that are then stored on different remote nodes adds another layer of complexity thereby making traditional digital forensic tools redundant [Chen et al., 2015, Almulla et al., 2013].

Additionally, the Cloud Service Providers (CSP) and their user base must be taken into consideration. Investigators are reliant on the willingness of CSPs to allow for the acquisition and reproduction of data. The lack of standardization among the varying CSPs, differing levels of data security and their Service Level Agreements are obstacles to both cloud forensic researchers and investigators [Almulla et al., 2013]. The multi-tenancy of many cloud systems poses three significant challenges to digital forensic investigations. In the majority of cases the privacy and confidentiality of legitimate users must be taken into account by investigators due to the shared infrastructures that sup-port cloud systems [Morioka and Sharbaf, 2015]. The distributed nature of cloud systems along with multi-tenancy can require the acquisition of vast volumes of data leading to many of the challenges outlined below. Finally, the use of IP anonymity and the easy-to-use features of many cloud systems, such as requiring minimal information when signing up for a service, can lead to situations where identifying a criminal is near impossible [Chen et al., 2012, Ruan et al., 2013].

Cloud forensics also faces a number of challenges associated with traditional digital forensic investigations. Encryption and other anti-forensic techniques are commonly used in cloud-based crimes. The limited time for which forensically-important data is available is also an issue with cloud-based systems. Due to the fact that said systems are continuously running data, can be overwritten at any time. Time of acquisition has also proved a challenging task in regard to cloud forensics. Thethi and Keane [2012] showed that commonly-used forensic tools such as the Linux dd command and Amazon's AWS Snapshot took a considerable amount of time to acquire 30Gb of data from a cloud service.

While advances continue with regard to the tools and techniques used in cloud forensics, the aforementioned challenges continue to impede investigations. Henry et al. [2013] produced results showing that investigations on cloud-based systems make up only a fraction of all digital forensic investigations. Many investigations are stalled beyond the point of a perpetrator's owned devices and rarely extend into the cloud-based services they use. Results such as these form a strong argument for continued research in this field.

The critical review of all the discussed methods are shown in TABLE I

4. LITERATURE SURVEY

AUTHOR, TITLE & YEAR	PROBLEM THEY SOLVED	METHODOLOGY	DRAWBACKS
Digital video tampering detection: An overview of passive techniques 2016	Detects 75% of forged pixels in image based tampering and duplicated frames on 90% of sequences	Inter frame forgery, Region tampering, Multiple compression	Time consuming in Real time Videos
Current Challenges And Future Research Areas For Digital Forensic Investigation David Lillis, Brett A. Becker, Tadhg O'sullivan And Mark Scanlon 2016	Real time Video forgery detection	Video forgery detection using IoT, Cloud Computing using traditional techniques	Distributed Processing is time consuming, parallel processing in not possible, require high end GPU powered using multi threading
Detection Of Video Forgery: A Review Of Literature Omar Ismael Al-Sanjary, Ghazalisulong 2015	80% of result for all tested videos	Passive approach for tampered videos detection using Spatial domain, Temporal domain	By using temporal and spatial domain can't find the source and also multiple compression can't be found
A Survey On Video Forgery Detection Sowmya K.N. , H.R. Chennamma 2015	Reliability factor for digital video, can detect and localize the duplicated clip	Hybrid Spatio Temporal tampering at block and pixel level	High complexity
A video forensic technique fordetecting frame deletion and insertion A. Gironi, M. Fontani, IEEE, 2014	Variation prediction footprint as the detection measure	Tampering detection even if the second encoding is strong	Cannot Detect frame manipulation when the attacker removes or inserts a whole GOP

5. CONCLUSION

Detecting video forgery is one of the challenges of this digital era. Highly sophisticated and low cost video editing detection methods. Each method has its merits and demerits. A comparative study reveals that MCEA based forgery detection technique is the most promising one among the tools make it easier for any person to forge a video content without leaving any trace of tampering. In this paper we have surveyed some of the important passive video forgery

xisting methods since it can detect all type of tampering in a video by analysing the P frames. The only disadvantage of this method is that it considers only P frames and neglects the relevance of B frames in the tampering detection process.

REFERENCES

[1] Chih-Chung Hsu, Tzu-Yi Hung, Chia-Wen Lin, Chiou-Ting Hsu, ―Video forgery detection using correlation of noise residue‖ in Proc.IEEE, 2008, pp.170-174

[2] Weihong Wang, Hany Farid, ―Exposing Digital Forgeries in Video by Detecting Duplication‖, in Proc.IEEE 2007

[3] Qiong Dong, Gaobo Yang, Ningbo Zhu, ―A MCEA based passive forensics scheme for detecting frame based video tampering‖, Elsevier, 2012, vol.9, pp.151-159

[4] Weihong Wang, Hany Farid, ―Exposing video forgeries by detecting MPEG double compression‖ IEEE,2012

[5] Richao chen, Qiong Dong, Heng Ren and Jiaqi Fu, ―Video Forgery

detection Based on Non-Subsampled Contourlet Transform and Gradient Information||, Information technology Journal 11(10), 2012, pp.1456-1462

[6] Guo-Shiang Lin, Jie-Fan Chang and Cheng-Hung Chuang, ―Detecting Frame Duplication Based on Spatial and Temporal Analysis||, 6 th International Conference on Computer Science and Education (ICCSE 2011) , 2011

[7] A. Gironi, M. Fontani, T. Bianchi, A. Piva, M. Barni,||A video forensic technique for detecting frame deletion and insertion||, in Acoustics, Speech and Signal Processing(ICASSP), 2014 *IEEE International Conference*, pp.6226-623 0

[8] P. Bestagini, S. Battaglia, S. Milani, M. Tagliasacchi, S. Tubaro, ―Detection of temporal interpolation in video sequences||, Proc. IEEE, 2013, pp. 3033-3037

[9] Richao Chen, Qiong Dong, Heng Ren and Jiaqi Fu, ―Video forgery detection based on non-subsampled contourlet transform and gradient information|| in Information Technology Journal, 2012

[10] Saurabh Upadhyay, Sanjay Kumar Singh, ―Video Authentication- An Overview||

[11] Prof Ashok De, Himanshu Chandha, Sparsh Gupta, ―Detection of Forgery in Digital Video||

[12] Ho Hee- Meng, ―Digital Video Forensics: Detecting MPEG-2 Video tampering through Motion Errors||