*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 2, Ver. III (Mar. - Apr. 2018), PP 01-04*
*www.iosrjournals.org*

# A Review of Video Forgery and Its Detection

Rohini Sawant[1] and Manoj Sabnis[2]
[1](M.E. Scholar, Department of Information Technology, V.E.S.Institute of Technology, Mumbai, India)
[2](Associate Professor, Department of Information Technology, V.E.S.Institute of Technology, Mumbai, India)
*Corresponding Author: Rohini Sawant*

***Abstract:*** *With the mass consumption of digitally interactive multimedia like audio, images and video there is also a considerable rise in the mode and the motive to fabricate digital forgeries. Ubiquitous availability and low cost devices like cameras, camcorders and CCTVs has led to wide spread use of video information and services in our society for various purposes like video surveillances, forensics investigation, entertainment etc. Formerly Video editing techniques were essential used for enhancement of the digital content. However the growth and usage of affordable and effortless video editing software there has been a surge in the consequences and hazards of using such editing techniques. Video Forgery is thus a technique of generating altered or fake videos by combining, altering or creating new video. Thus the authenticity of such digital videos is questionable and needs to be verified. Forgery detection in videos aims at exposing and examining the underlying facts about a video to deduce whether the video contents have undergone any unethical post processing.*

***Keywords:*** *Video Forgery, Spatial and Temporal Tampering, Video Forgery Detection.*

---

Date of Submission: 28-03-2018 Date of acceptance: 12-04-2018

---

## I. Introduction

Presently in the digital era, our day to day life is permeated with digital video contents as one of the prominent means for communication. Developments in video technologies such as generation, transmission, storage and retrieval along with applications like Video sharing platforms, Video-conferencing etc have served the people and society in many ways. In the terms of social, economic and scientific development, the images and videos available on various video sharing and social networking platforms like YouTube, Face Book, Instagram etc. are of symbolic importance [1]. Besides this, other applications like entertainment industry, video surveillance, legal evidence, political videos, video tutorials, advertisements, etc. signify their unprecedented role in today's context.

As a matter of fact, videos can be generated, stored, transmitted and processed in digital format in a easy way, because of extensive use of the Internet and inexpensive and high quality cameras, computers and user-friendly editing tools. Any novice individual can utilize these techniques to make unauthorized modifications to the video content thereby affecting its integrity and authenticity. This possibility arises the need to validate whether the multimedia content available on the internet, obtained as a part of video surveillance system, or received by a broadcaster, is original or not.

Thus along with the exemplary behaviour of videos comes forward a gloomy side to it which is misusing or inaccurate projection of information through videos. Intentional modification or alteration of the digital video for fabrication is referred to as Digital Video Forgery [2]. Video forgery refers to manipulating a video in such a way that it changes the content perceptually. Video Forgery can be as simple as inserting advertisements during broadcasting of sporting events or as complex as removing people digitally from a video. Video Forgery can be divided into two parts Spatial Forgeries and Temporal Forgeries.

To solve this problem of forgery and to ensure the authenticity of digital videos, the domain of digital video forensics was perceived. Digital video forensics comprises of tools and techniques which help clarify whether the contents of a given digital video are verifiable or not. Digital video forensics is a part of Multimedia Forensic and is the scientific understanding and skill necessary to authenticate and enhance video. Digital video forensics can also be termed as Video Forgery Detection techniques. Video Forgery Detection aims at exposing and scrutinizing the concealed facts about a Video. It can be classified into two categories Active Video Forgery Detection and Passive Video Forgery Detection.

## II. Video Forgery

The digital content can now be easily manipulated, synthesized and tampered in numerous ways without leaving any visible clues. The integrity of digital videos can no longer be taken for granted. It has become difficult to differentiate in between a forged and an original video. Therefore, there is an increasing dissatisfaction and mistrust about the authenticity of these videos [3].

Deliberate alteration of the digital video for fabrication is referred to as Digital Video Forgery. Video forgery means manipulating a video in such a way that changes are made in its content perceptually. Video forgery means meddling the video by transforming or changing its contents. Theses modification when are implemented on the videos, they either affect visual data present in the frames sequence or the temporal reliance between the frames.

## III. Areas Affected By Video Forgery

The usage of videos in varied applications like entertainment industry, video surveillance, legal and law enforcement, social networking, video tutorials, advertising, etc. mark its unmatched role in today's life. However its repercussion depends on the circumstance and the area where it is used. Different areas affected by Video Forgery are:

***1. Video Surveillance***: Videos available from the Surveillance Systems present at the Airports, Railway Stations, Shopping Malls and at other public places would be easily altered copying, duplicating or removing certain objects or frames within the video sequence. Also it would be possible to insert into the video, certain objects, events or people present at different locations and cameras at different time. In this case, it is difficult to ensure that the video used as evidence, is the original one actually recorded by the surveillance camera.

***2.Forensic Investigations:*** This means scientific analysis and evaluation of video in legal matters. The forger may forge the video to hide an unsuitable event or object or may plan to embed erroneous evidences and proofs. Video evidence can be collected from diverse locations like stores, restaurants, malls, banks, parks etc which even assists the police in various cases. Thus forensic investigations need to ensure their originality.

***3. Law Enforcement:*** Images and Videos serve as very influential evidences in legal courts and general opinion. It is imperative to ensure the genuineness of videos and that the video evidence has not undergone any malpractice. Using the forging techniques criminals make use of forged video evidences which are indecisive in the court and exempt their punishment.

***4. Defamation:*** Video forgery in movies and politics has an evident impact as it used to defame a personality or conceal actuality. This is so because usage and sharing of videos on social media and video sharing platforms like WhatsApp, YouTube, Facebook etc has a huge impact on our daily lives [4].

## IV. Types of Tampering In Videos

Forgeries can be performed by tampering different domains associated with the video sequence. Using the regional property of the video, Video Forgeries include the following types of tampering domains:

***i. Spatial Tampering:*** This type of tampering is performed on visual contents of the frame along the x- y axis of the video. Spatially Tampering can be performed by manipulating the pixel bits in a frame or the adjacent ones in the video sequence. Thus Spatially Tampering can be performed at Pixel level, Block Level or Shot/Scene Level. The operations that can be included in this type of tampering are crop and replace, morphing, addition and deletion of object.

***ii. Temporal Tampering:*** This type of tampering is performed on the concatenated chain of frames in the video. Temporal Tampering works in progression across the time frame. It primarily affects the time sequence of visual data recorded by the device. The operations that can be included in this type of tampering are mostly performed at frame level and include addition or deletion of frame and shuffling of frames.

***iii. Spatio-Temporal Tampering:*** This type of tampering is a combination of both the above types of tampering. This tampering involves manipulating both the visual information along with the time sequences. Saptio-Temporal Tampering tampers the concatenated sequence of frames along with the visual contents available in the frames of the video [2].

## V. Video Forgery Detection

Video Forgery Detection is a significantly emerging discipline in Image Processing that acts as a countermeasure to intentional misuse of visual data like videos and different digital editing tools.Video Forgery Detection's aims to establish the authenticity of a video and to expose the potential modifications and forgeries that the video might have undergone [5]. Undesired post processing operations or forgeries generally are irreversible and leave some digital footprints. Video forgery detection techniques scrutinize these footprints in order to differentiate between original and the forged videos. When a video is forged some of its fundamental

properties change and to detect these changes is what is called as Video Forgery Detection techniques used for. Thus it is the scientific understanding and skill required to amplify and authenticate video recordings.

## VI. Need For Video Forgery Detection

Earlier, digital videos were thought of as accurate, but the easy availability of inexpensive and user friendly editing software along evolution of specialized forging techniques has headed to the awareness that this is no longer the scenario.

It is also conveniently thought of to make use of the Image Forgery Detection Techniques for videos thinking that they would be equivalently effective. Also many ideas and tools in video forgery detection draw its concepts from the Image Forensics there are quiet noteworthy differences between the two. Whilst it would be probable to analyze the video by application of image forensic tools to each frame separately, this approach would be impractical, mainly for these two reasons: Complexity and Reliability.

- ***Complexity:*** Techniques and tools for detecting forgeries in images are computationally more demanding.

- ***Reliability:*** Forgeries like replication or deletion of frames within a video would not be detectable by any Image Forgery Detection Techniques.

Also in processing videos, a large number of frames are dealt and analyzed with a total volume of data exceeding that of still images. Thus pre-dominantly complexity is a pitfall, limiting the array of techniques. Even a large module of the research activities are dedicated towards the still images. However, scientific investigations have been recently focusing on the issues related to video because of their characteristics and the wide array of probable alterations that can be made to them.

## VII. Types of Video Forgery Detection

There are two fundamental approaches for Video Forgery Detection: Active Approach and Passive Approach.

***i. Active Approach:*** Active Forgery Detection includes techniques like Digital Watermarking and Digital Signatures which are helpful to authentic Content Ownership and Copyright Violations. Tough the basic application of Watermarking and Signatures is Copyright protection it can be used for Fingerprint, Forgery Detection, Error concealment etc. There are several drawbacks to the active approach as it requires a signature or watermark to be embedded during the acquisition phase at the time of recording or an individual person to embed it later after acquisition phase at the time of sending. This limits the application of active approach due to the need of distinctive hardware like specially equipped cameras. Other issues which have an impact on the robustness of Watermarks and Signatures are factors like compression, scaling, noise etc [6].

***ii. Passive Approach:*** Passive Forgery Detection techniques are considered as an advancing route in Digital security. The approach works in contrast to that of the Active approach. This approach works in without the constraint for specialized hardware nor does it require any firsthand information about the video contents. Thus it is also called as Passive-Blind Approach. The basic assumption made by this approach is that Videos have some inherent properties or features which are consistent in original videos. When a video is forged these patterns are altered. Passive approaches extract these features from a video and analyze them for different forgery detection purposes [7].

Thus to overcome the inefficiency encountered in the Active Approach the use of Passive Approach for video forgery detection can be made. Passive Approach thus proves to be better than the Active ones as it works on the firsthand information without the need for extra information bits and hardware requirements. It totall relies on the available forged video data and its intrinsic features and properties without the need of original video data.

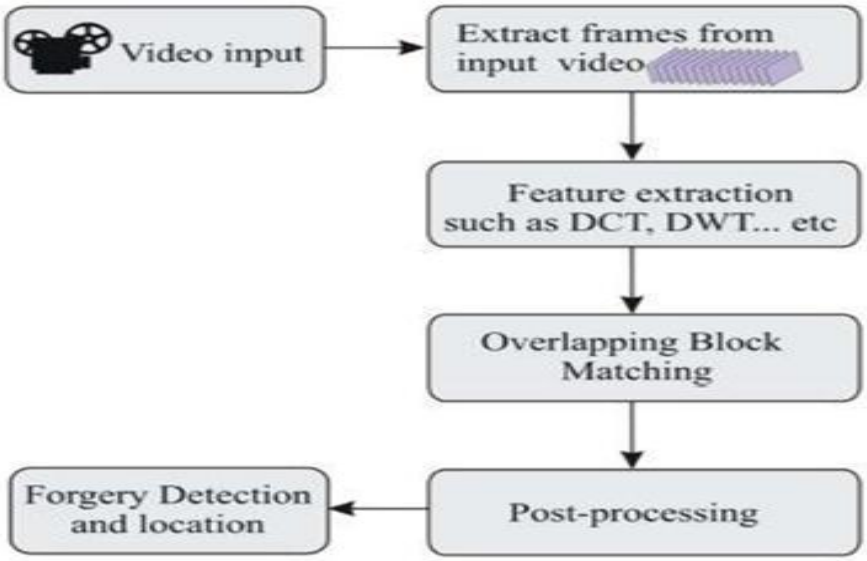


**Fig 1: The general Forgery Detection process.**

The general Passive Video Forgery Detection process depicted in Fig 1. comprises of Frame Extraction, Feature Extraction followed by Overlapping Block Matching which culminates into final decisive step that gives output result about Forgery Detection and its location [8]. During this process the first step is to divide source video and extract frames. Following this for Feature Extraction various techniques can be used like DCT, DWT. PCA etc. For Block Matching techniques like K-SVD tree and radix sort can be used. The final decisive step concludes to the type of Video Forgery and its location in the frame.

## VIII. Conclusion

The problem of Video Forgery is growing and needs to be combated to avoid its perennial impact. The Forgery Detection techniques have remains unsolved for videos and mostly the use of Image Forgery Detection techniques have been used for the same. There is thus an definite necessity to devise more effective methods to provide clear distinction between original and malicious digital videos. We also conclude that Passive Video Forgery Detection techniques work as an alternative and contrast to the Active Video Forgery Detection Techniques as such a-priori procedure leads the usage of Passive Video Forgery Detection techniques which work in absence of any watermark or special hardware. Video Forgery Detection has large unexplored forensic application in the real world because of the volume and the complexity of data been processed and its wide employment.

## References

[1] Mrs. J.D. Gavade, M. S. (2015). Review of Techniques of Digital Video Forgery Detection. Advances in Computer Science and Information Technology (ACSIT), Volume 2 .
[2] Sowmya K.N., H. C. (2015). A SURVEY ON VIDEO FORGERY DETECTION. International Journal of Computer Engineering Chih-Chung Hsu, T.-Y. H.-W.-T. (2008). Video forgery detection using correlation of noise residue.IEEE 10th Workshop on Multimedia Signal Processing. IEEE.
[3] Anderson Rocha, W. S. (2010). Vision of the Unseen: Current Trends andChallenges in Digital Image and Video
[4] Forensics. ACM Digital Library Ashish Kumar Kushwaha, A. P. (2015). Video Forensic Framework for Video
[5] Forgeries. International Journal of Innovative Research in Computer and Communication Engineering
[6] Ainuddin Wahid Abdul Wahab, M. A. (2014). Passive Video Forgery Detection Techniques: A Survey. 2014 10th International Conference on Information Assurance and Security. IEEE. .
[7] Staffy Kingra, N. A. (2016). Video Inter-frame Forgery Detection: A Survey. Indian Journal of Science and Technology, Vol 9 .
[8] Omar Ismael Al-Sanjary, G. (2015). DETECTION OF VIDEO FORGERY: A REVIEW OF LITERATURE. Journal of Theoretical and Applied Information Technology

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Rohini Sawant "A Review of Video Forgery and Its Detection ." IOSR Journal of Computer Engineering (IOSR-JCE) 20.2 (2018): 01-04.