Video Tampering and It's Detection Techniques: Review

Sangita Bhoyar[1], Dr. 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: Sangita Bhoyar

Abstract:

In the era of sophisticated video and image editing tools, the landscape of digital content authenticity is facing unprecedented challenges. The ease with which digital videos and images can be tampered without compromising their quality or leaving discernible visual evidence poses a significant threat. This review paper offers a comprehensive overview of various types of video forgery and the diverse array of techniques employed for its detection. The paper categorizes detection methods into passive and active forgery detection techniques, each serving a unique role in identifying tampering within digital videos. Passive techniques aim at uncovering visual artifacts or irregularities that may indicate tampering, while active techniques delve into assessing the integrity and authenticity of the video content. Throughout the review, the authors delve into the intricacies of different video tampering attacks, shedding light on the evolving landscape of digital deception. The focus on passive and active tampering detection techniques provides a refined understanding of the various challenges faced by researchers and practitioners in maintaining the trustworthiness of digital media.

Key Word**: **Vidéo Tampering, Vidéo Tampering Détection.

I. Introduction

In recent years, digital multimedia has become the popular medium to gain and exchange information. In recent times, rapid technological advancements have led to a substantial surge in the production of visual content, specifically billions of images and videos, on a daily basis through online platforms such as Facebook, Twitter, YouTube, and Instagram. These popular websites have become major facilitators, allowing individuals to effortlessly upload and distribute vast quantities of pictures. Use of digital media in various applications like Entertainment industry, video surveillance, legal and law Implementation etc. marks its unrivaled role in today's life, as image and video content are more convincing for people and regarded as representation to facts [1][2].

The widespread availability of modern camera technology and easily accessible video manipulation and photo editing software has created an environment where digital media content is increasingly vulnerable to forgery. The easy availability of tools and applications that facilitate the alteration of images and videos makes it challenging to maintain the integrity of visual content, as manipulations can be executed seamlessly, leaving behind little to no significant clues. In this context, the trustworthiness of digital media, particularly videos, faces a significant threat. The aftermath of forgery not only compromises the credibility of the content but also erodes the assumption that a video's authenticity can be taken for granted. Given these concerns, researchers and scholars have directed their efforts towards developing methods for detecting manipulated media, employing both manual and automated approaches [4] [5].

Digital forensics, as a discipline, plays a crucial role in this endeavor. It involves the systematic analysis of digital artifacts to determine whether a given video has undergone forgery or manipulation. Scholars in this field leverage a variety of techniques, such as metadata analysis, feature extraction, and advanced algorithms, to scrutinize the content for anomalies and irregularities. By examining the digital fingerprints left behind during the creation or manipulation of media, researchers aim to establish reliable methods for distinguishing between authentic and tampered visual content. The overarching goal is to create robust and effective tools that can automatically detect signs of manipulation in digital media. This not only contributes to maintaining the credibility of online visual content but also helps in countering the potential spread of misinformation, ensuring that consumers of digital media can trust the authenticity of the videos they encounter in the digital landscape [1] [3].

II. Video Forgery

Video forgery, also known as video manipulation or content manipulation, refers to the act of altering or creating misleading digital content of the video with the intent to deceive or manipulate the audience. This manipulation can occur in various forms of digital media. Few years ago, forging video was a daunting task which requires enormous amounts of money and resources, but the advancements in digital technology and easily available software tools have made it easier for individuals to create sophisticated forgeries that can be challenging to detect.

Types of tampering attacks in videos:

Video forgeries involve manipulating various aspects of a video sequence by tampering with different domains. By exploiting the regional properties of the video, these forgeries can be categorized into the following types of tampering domains [5] [6]:

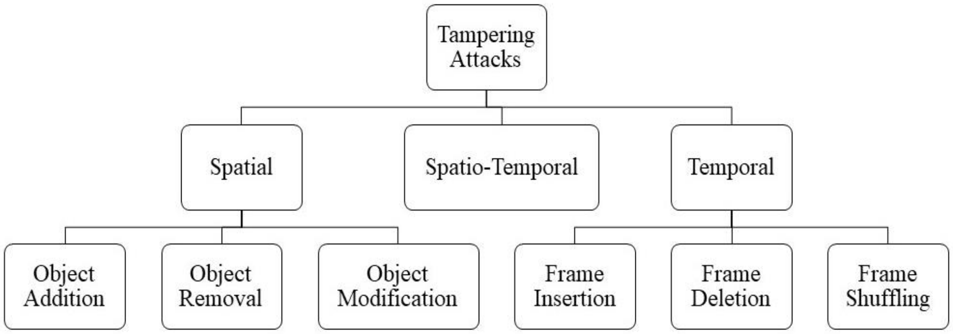
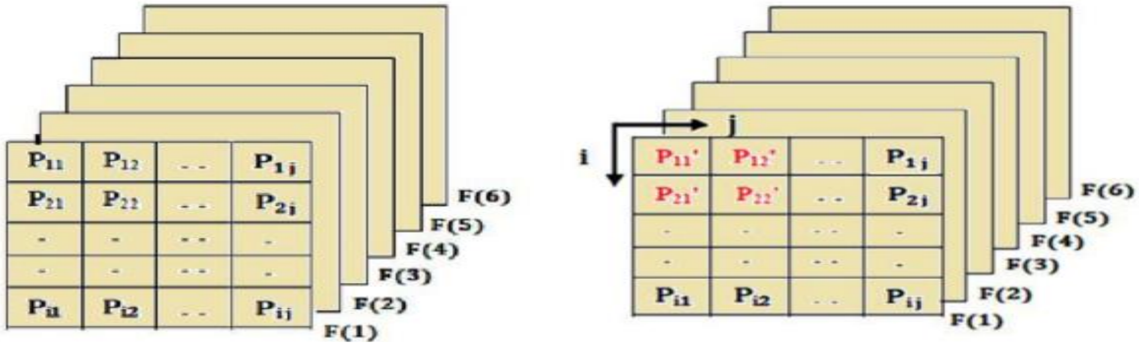


Figure1: Types of tampering attacks in videos

1. **Spatial Tampering:**

In spatial or intraframe editing, the malicious alterations impacts the contents of either a single frame or multiple frames. Specifically, intraframe tampering is represented in Figure 2, where the frame F(1) of the original input video V_O undergoes spatial tampering to generate the forged video V_T. Here, (i, j) represent the height and width of the frames of the input video V_O. Essentially, the contents of video frames are treated as objects, categorized into two classes: Foreground objects and Background objects. Foreground objects are elements captured individually in a frame, excluding the background. The background object encompasses the background portion of the frame, excluding all foreground objects.



1. Original Video (Vo)

2. Tampered Video (V_T)

Figure2: Spatial Tampering

Various types of spatial tampering attacks involve:

Object Removal: Eliminating specific elements or objects from the frame.

Object Addition: Introducing new objects into the frame that were not originally present.

Object Modification: Altering the characteristics or appearance of existing objects within the frame.
These tampering techniques aim to deceive by manipulating the visual elements within individual frames of the video sequence.

2. Temporal Tampering:

Temporal tampering involves manipulating the concatenated chain of frames within a video. This type of tampering operates in a sequential manner across the timeline of the video, primarily impacting the chronological order of visual data recorded by the device. The operations associated with temporal tampering predominantly occur at the frame level and encompass actions such as frame insertion, frame deletion and frame shuffling or frame reordering. Figure 3 represents the original video V_O that consists of six frames.

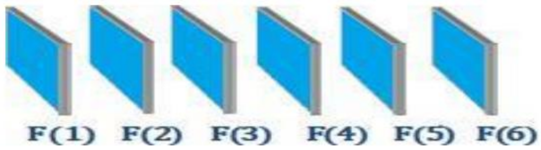


Figure 3: Original Video (V_O)

Frame insertion: In frame insertion attack, additional frames from another video, which has the same statistical properties, are intentionally inserted at some arbitrary locations in a given video. Figure 4 shows a typical example of the frame insertion, In which two frames F(a) and F(b) are inserted at random location in the original video V_O to produce the tampered video consisting of eight frames.

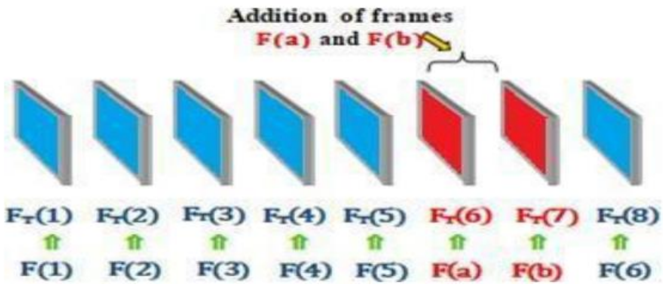


Figure 4: Frame insertion attack

Frame Deletion: In frame deletion attack the frames are deliberately removed, frames can be eliminated from different locations or it can be removed from a specific location. Figure 5 shows a typical example of frame deletion in which the frames labeled F(3) and F(4) are removed from original video V_O to generate tampered video consisting of only four frames.

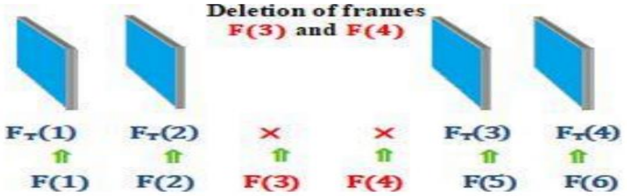


Figure 5: Frame deletion attack

Frame Shuffling: In frame shuffling attack, frames of a given video are rearranged or shuffled in such a manner that the actual video frame sequence is intermingled and erroneous information is produced by the video as compared to original video. Figure 6 shows a typical example of frame shuffling is shown in Where two frames labeled F(2) and F(5) of the original video V_O are shuffled.

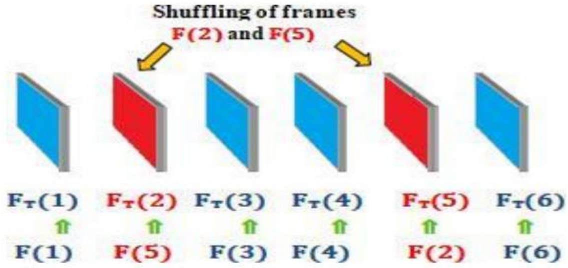
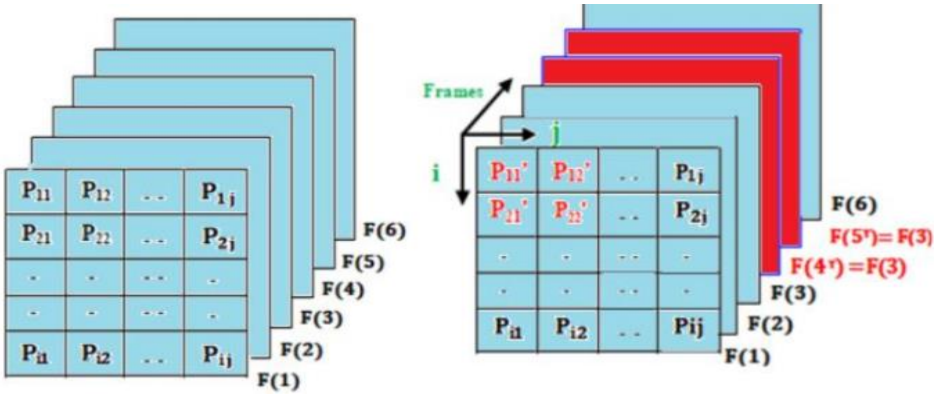


Figure 6: Frame Shuffling Attack

3. Spatio-Temporal Tampering:

Spatio-temporal tampering attacks involve a combination of spatial and temporal tampering, incorporating both Inter-frame forgery (temporal) and Intra-frame forgery (spatial). This fusion encompasses various tampering techniques observed in both spatial and temporal domains. For an authentication system to be effective, it needs to be robust enough to detect and recognize both types of tampering, ensuring comprehensive protection against alterations that occur within individual frames (spatial) as well as disruptions in the sequential flow of frames over time (temporal). Figure 7 shows example of Spatio temporal tampering; where V_T is the tampered video generated from source video V_O. As a result of the temporal tampering in frame F(4) and F(5) and spatial tampering in frame F(1) of the original source video V_O the spatiotemporally tampered video V_T is generated.



1. Original Video (Vo) 2. Tampered Video (V_T)

Figure7: Spatio Temporal Tampering

III. Areas affected by Video Tampering

Surveillance Systems: The integrity and authenticity of video evidence from surveillance systems, such as those in airports, railway stations, and shopping malls, can be compromised due to various manipulations. These manipulations include copying, duplicating, removing objects or frames, as well as inserting new objects, events, or people into the footage. As a result, it becomes challenging to verify whether the presented video is the original recording from the surveillance camera. In essence, the issue lies in the potential for tampering with the video content, making it difficult to ascertain its accuracy and reliability as evidence [3].

Forensic analysis: Forensic investigations entail scientifically analyzing and evaluating videos for legal purposes. In these investigations, the video content is scrutinized to detect any attempts at forgery, such as hiding incriminating events or objects, or planting false evidence. Video evidence can be sourced from various locations including stores, restaurants, malls, banks, parks, etc., and plays a crucial role in aiding law enforcement in numerous cases. Therefore, it is imperative for forensic investigations to verify the authenticity and originality of the videos to maintain their integrity and reliability as evidence [3].

Security services and Legal Proceedings: Legal proceedings and public perception, images and videos hold significant sway as compelling evidence. Ensuring the authenticity of these visual materials is crucial, as any tampering can undermine their credibility. Criminals often employ forging techniques to manipulate video evidence, rendering it unreliable in court and potentially leading to their exoneration. Thus, it's essential to safeguard against such malpractice to uphold the integrity of the legal process and ensure just outcomes [3].

Deepfake technology: Video manipulation in movies and politics has a noticeable influence as it can be employed to tarnish someone's reputation or distort the truth. This is primarily because videos are widely circulated and shared on social media and video-sharing platforms such as WhatsApp, YouTube, and Facebook, significantly impacting our everyday experiences and perceptions. Deepfake videos on social media platforms can contribute to the dissemination of false information and the manipulation of public sentiment [4].

IV. Framework for Video Forgery Detection

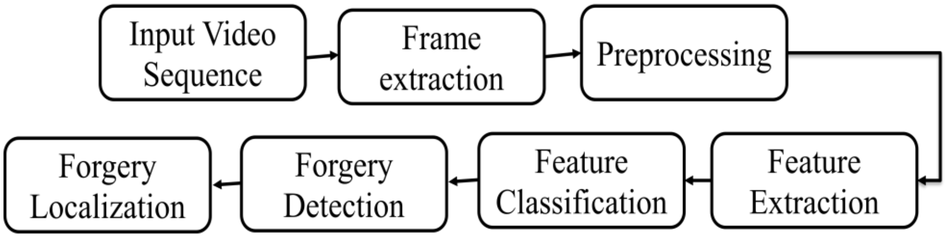


Figure 8: Generalized framework for Video Forgery Detection

Figure 8, shows generalized framework for video forgery detection [2] [3], consisting of frame extraction, Preprocessing, feature extraction, feature classification, forgery detection and localization. Feature extraction step is to divide the input video and extract frames from it. Feature extraction is followed by Pre-processing, which enhances performance by removing redundancy present in images. The operations involved in the pre-processing phase are image re-sizing, filtering, noise removal etc. The pre- processing technique is commonly used for the transformation of RGB (Red, Green and Blue) color channels to grayscale.

The feature extraction operation is performed over the pre-processed image. Feature extraction is a process through which certain features of interest are detected within an image and represented for further processing. Feature extraction is a crucial step determining both accuracy and efficiency of the detection system. In this stage, feature descriptors are generated from each block or keypoint obtained from previous processes.

After feature extraction classification of the similar types of features in an image are done to detect the forgery in an image or a video. Classification is usually done by using block-based and keypoint-based approaches. The final phase is to localize the forged regions.

V. Video Forgery Detection Techniques

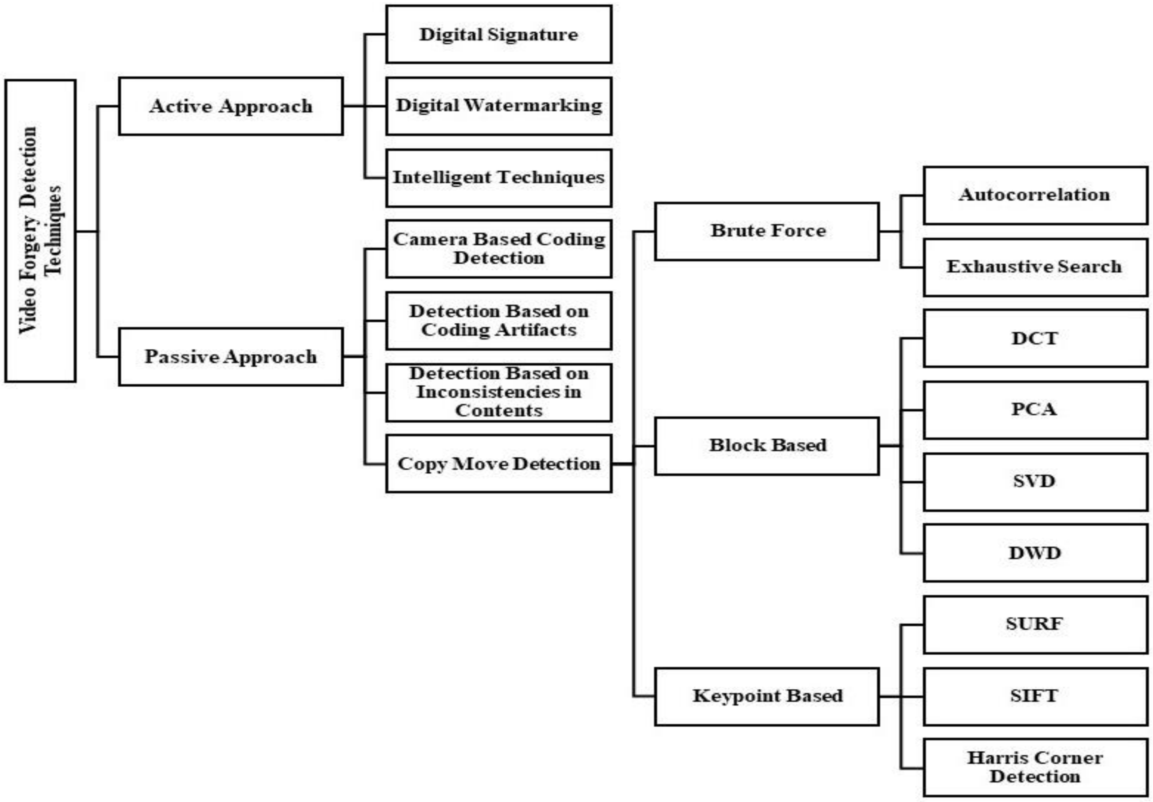


Figure 9: Video Forgery Detection Techniques

The methods used for identification of authenticity of videos are known as video forgery detection methods. They are mainly classified into two categories Active approach and Passive approach as shown in Figure 9 [1] [2].

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. Active approach is having certain drawback such 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, due to this limits the application of active approach as it requires distinctive hardware like specially equipped cameras. Active technique includes digital signature, intelligent techniques and watermark as shown in Figure 9.

Passive approach:

Passive Approach Passive Forgery Detection techniques are considered as an advancing route in Digital security. This it is also called as Passive-Blind Approach as it works without the constraint for specialized hardware and does not require any firsthand information about the video contents. This approach is working on the assumption that, videos have some inherent properties or features which are consistent in the original videos. And when the video if forged these patterns are altered. These features will be extracted and analysed by passive approach for different forgery detection purposes. Passive Approach thus proves to be better than the Active ones as it works on the firsthand information without the need for extra information and hardware requirements. It totally relies on the available forged video data and its intrinsic features and properties without the need of original video data. To be specific active techniques includes motion detection mechanisms and passive technique includes static mechanisms.

This approach includes Camera- based coding detection, Detection based on coding artifacts, Detection based on inconsistencies in the contents, and Copy–move detection as shown in Figure 9.

Camera- based coding detection: Camera-based coding detection for video forgery involves the use of techniques and algorithms to detect instances of video forgery or manipulation by analyzing the coding characteristics of the video content itself. This approach is particularly useful when examining videos that have been tampered with using different coding or compression methods.

Detection based on coding artifacts: Detection based on coding artifacts involves identifying specific traces or artifacts left in a video file due to the coding and compression processes applied during its creation or manipulation. Video codecs use various techniques to compress and represent video data, and the analysis of coding artifacts can reveal irregularities that may indicate forgery or tampering.

Detection based on inconsistencies in the contents: Detection based on inconsistencies (like Object Motion and Tracking, Shadow Analysis, Lighting Inconsistencies, Reflections and Glare, etc.) in the contents of a video involves analyzing the visual and audio elements within the video to identify irregularities or discrepancies that may indicate tampering or forgery.

Copy–move detection: Copy-move forgery detection involves identifying instances where a portion of video has been duplicated and moved within the same file. The methods used for copy-move forgery detection are:

- **Brute force,**
- **Block-based techniques,**
- **Keypoint based techniques**.

Exhaustive search and Autocorrelation are the techniques based on the brute force method. An exhaustive search is a technique where an image or a frame is used to scrutinize matching raisins with circularly shifted versions. It consists of a large number of comparisons, so it shows that the computational unpredictability is high. Autocorrelation is also called serial correlation and it is used to determine location change.

Block-based strategy divides a picture into overlapping or non-contiguous regions/blocks during the pre-processing phase, image features can be extracted using overlapping blocks. Then conduct feature extraction, block comparisons, evaluate related blocks (they depict the manipulation) and finally perform localization. The algorithms used for the block-based strategy are- DCT (Discrete Cosine Transform), PCA (Principal Component Analysis), SVD (Singular Value Decomposition), and DWT (Discrete Wavelet Transform).

Keypoint based approach is non-block based because the block division is not required in the preprocessing step. In this case, feature extraction is performed on the basis of distinctive local features (i.e. edges, corners and blobs) from the image. Each feature is shown with the set of descriptors. A descriptor is used to increase the reliability of the features of the refining transformation. To find similar regions in the image or frame, the features and descriptors are classified and compared with each other. The algorithms used in keypoint based feature extraction techniques are SIFT, SURF and Harris corner detector as shown in Figure 9.

VI. Conclusion

The problem of video forgery is indeed growing at an alarming rate, posing significant challenges and potential repercussions in various domains. As technology advances, the tools and techniques for manipulating videos have become more accessible and sophisticated, giving rise to a range of concerns. In this paper various types of video tampering attacks like spatial tampering, temporal tampering and spatio-temporal tampering, Generalized framework for video forgery detection and video tampering detection techniques like passive and active techniques has been discussed.

References

[1]. Walid El-Shafai, Mona A. Fouda, El-Sayed M. El-Rabaie, Nariman Abd El-Salam, "A comprehensive taxonomy on multimedia video forgery detection techniques: challenges and novel trends", In Springer, Multimedia Tools and Applications (2024) 83:4241–4307

[2]. Himani Sharma, Navdeep Kanwal, Ranbir Singh Batth, "An Ontology of Digital Video Forensics: Classification, Research Gaps & Datasets," in IEEE 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) December 11–12, 2019, Amity University Dubai, UAE.

[3]. Rohini Sawant, Manoj Sabnis, "A Review of Video Forgery and Its Detection", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 20, Issue 2, Ver. III (Mar. – Apr. 2018).

[4]. Yogesh Patel, Sudeep Tanwar, Rajesh Gupta, Pronaya Bhattacharya, Innocent Ewean Davidson, Royi Nyameko, Srinivas Aluvala, And Vrince Vimal, "Deepfake Generation and Detection: Case Study and Challenges", In IEEE Access 2024 Digital Object Identifier 10.1109/ACCESS.2023.3342107

[5]. Ruksana Habeeb, Dr. L. C. Manikandan, "A Review : Video Tampering Attacks and Detection Techniques", In Researchgate, Article in International Journal of Scientific Research in Computer Science Engineering and Information Technology, October 2019 DOI: 10.32628/CSEIT195524

[6]. Sowmya K.N., H.R. Chennamma, "A Survey On Video Forgery Detection", International Journal of Computer Engineering and Applications, Volume IX, Issue II, February 2015.