INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 377-382

e-ISSN : 2583-1062

Impact Factor : 5.725

REVIEW OF TECHNIQUES OF DIGITAL VIDEO FORGERY DETECTION

Varun Ghatage[1], Dr. Mohammed Rafi[2]

[1]Student CSE, Shivanand M N, Student CSE, University BDT College of engineering, Davangere, India.

[2]Professor, CSE, University BDT College of engineering, Davangere, India.

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.

Keywords: Noise residue, Copy-move forgery, optical flow, copy- move forgery, Motion brightness Multimedia data, Forgery detection, Video forensic, Video processing techniques, future researchetc.

1. INTRODUCTION

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. 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.

In response to these challenges, the paper systematically presents and evaluates a range of techniques proposed in the literature. These techniques are designed to address and rectify issues related to accuracy and privacy, ensuring a thorough examination of the strategies available to mitigate potential pitfalls. The dual focus on both the promise and challenges of Forgery detection, along with the insightful exploration of proposed solutions, positions the paper to contribute meaningfully to the ongoing discourse surrounding the responsible and effective implementation of video forgery detection systems in the public sector(here). 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.

Video Forgery: actuality. This is so because usage and sharing of videos on The digital content can now be easily manipulated, social media and video sharing platforms like WhatsApp, synthesized and tampered in numerous ways without YouTube, Facebook etc has a huge impact on our daily leaving any visible clues. The integrity of digital videos lives [4]. can no longer be taken for granted. It has become difficult.

Image Manipulation: 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.

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:

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, Imagery manipulation (IM) is a process of editing an image or video using some operation via computer software or other digital devices like mobile and tablets. IM is also known as image editing.

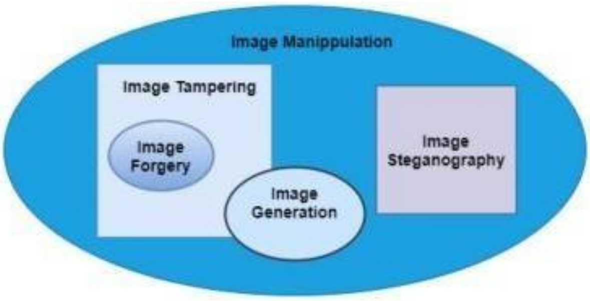

Fig. 1 Image manipulation and its types

Nowadays, cameras are substituted by mobiles which can generate high-quality digital photographs and are also equipped with some editing applications like movie, videos, etc. Digital photographs are becoming an integral part of our daily life. From birthdays to marriage ceremonies, photographs are used to remember and store ones personal memory. Image editing applications are used to add some visual effects to images and videos that make them look beautiful in such images. In this paper, the term image manipulation is used instead of digital image editing for clarification purposes. Image manipulation and its types are shown in Fig. 1. The image manipulation can include operations like resampling which is a pixel- level operation to remove and add objects within an image

Types of Tampering In Videos

Forgeries can be performed by tampering different banks, parks etc which even assists the police in various domains associated with the video sequence. Using the cases.T hus forensic investigations need to ensure their regional property of the video, Video Forgeries include the originality.

Law Enforcement: following types of tampering domains: Images and Videos serve as very influential evidences in Spatial Tampering: This type of tampering is legal courts and general opinion. It is imperative to ensure performed on visual contents of the frame along the x- y the genuineness of videos and that the video evidence has axis of the video. Spatially Tampering can be performed by not undergone any malpractice. Using the forging manipulating the pixel bits in a frame or the adjacent ones twehchicnhiquaerse cirnimdeinciaslisvemaikne uthsee oc fo fuorrt geadnd videexo emevpitdetnhceeisr punishment.

Defamation: Video forgery in movies and politics has an evident impact as it used to defame a personality or concealin 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.

Temporal Tampering: This type of tampering is Image Forgery Detection Techniques. Also in processing performed on the concatenated chain of frames in the videos, a large number of frames are dealt and analyzed video. Temporal Tampering works in progression across with a total volume of data exceeding that of still images. the time frame. It primarily affects the time sequence of Thus pre-dominantly complexity is a pitfall, limiting the visual data recorded by the device. The operations that can array of techniques.

be included in this type of tampering are mostly Even a large module of the research activities are dedicated performed at frame level and include addition or deletion towards the still images. However, scientific investigations of frame and shuffling of frames. have been recently focusing on the issues related to video because of their characteristics and the wide array.

Spatio-Temporal Tampering: This type of probable alterations that can be made to them. tampering is a combination of both the above type.

Types of Video Forgery Detection

tampering. This tampering involves manipulating both the There are two fundamental approaches for Video Forgery visual information along with the time sequences. Detection: Active Approach and Passive Approach. Saptio Temporal Tampering tampers the concatenated sequence of frames along with the visual contents available in the frames of the video [2].

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.

Detection of Video and Multimedia Copy-Move Forgery using Optical Algorithm and GLSM Clustering.

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.

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].

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 would be impractical, mainly for these two reasons: Thus to overcome the inefficiency encountered in the Complexity and Reliability.

Approach the use of Passive Approach for video.

- Complexity: Techniques and tools for detecting forgery detection can be made. Passive Approach thus forgeries in images are computationally more demanding. proves to be better than the Active ones as it works.
- Reliability: Forgeries like replication or deletion of firsthand information without the need for extra frames within a video would not be detectable by any information bits and hardware requirements. It totall relies on the available forged video data and its intrinsic features 1. Data collection and training and properties without the need of original video data.

2. METHODOLOGY

- Applying Optical Algorithm to determine consistency and feature extraction
- Applying GLCM and clustering the features

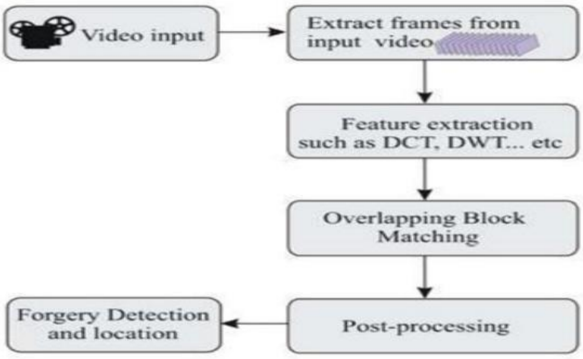
Video input
Extract frames from input video
Feature extraction such as DCT, DWT... etc
Overlapping Block Matching
Post-processing
Forgery Detection and location

Fig 1: The general Forgery Detection process.

The block diagram of the proposed methodology is given 4. Predicting if the video is forged or not Data collection below: and training: The first module deals with the code(algorithm) to import the video and process it (into grayscale) for which a learning model is used. The Logistic regression is used to create the model for training the data sets. The data sets are collected from Surrey University Library for Forensic Analysis (SULFA) and then trained Applying Optical Algorithm to determine consistency and feature extraction: After conversion into grayscale we apply the optical flow algorithm to determine the consistency in the frames. Also the image block processing concept is used for breaking the frame in a smaller size for edge detection. Applying GLCM and clustering the features: The third module consists GLCM algorithm to do The methodology of the proposed model is defined as a the texture analysis and determining any tampering in the conceptual model that defines the structure, behavior and video frame. the views of the system. The architectural behavior explains the structure and the behavior of the system. T similar. The K-nearest neighbour algorithm classification and clustering of video frames that are is used for Predicting if the video is forged or not: The module uses deep learning algorithms like SVM, Naïve Fourth here have been efforts to formalize languages to describe system architecture, collectively these are called architecture description languages (ADLs). A Machine Learning Algorithm named Logistic Regression is used to train the system and create a model from the available data set. The data set consists 2 types of videos- Forged and non-Forged(original). Initially, these videos are converted

Image warping and morphing

into a number of frames which they represent. These The process of manipulating a digital image such that the frames are then converted into greyscale and the optical shape of the objects present in the image is/are transformed flow map is generated for the given video. From th- or distorted. Warping is the geometric deformation of a is optical flow map, the features like motion are extracted. single object in a given image. Warping can be used for The optical sum consistency is tested to determine the correcting image distortion as well as for creative purposes. suspected tampered points. After that the GLCM and On the other hand, image morphing interpolates two or validation check algorithms are applied to further reduce more graphical objects. It means morphing is a any kind of tampering go undetected. The system then combination of image warping and blending techniques to returns if the video is forged or not forged. The first ph- interpolate objects to create a novel object. The goal is t ase of the project involves converting videos into frames that take an input image and gradually distort it while rthat represent a still image. Then the RGB image/frame generating the target image. In practice, morphing is converted into a Grayscale image, here we use the image commonly used in the entertainment industry for instance, block processing concept followed by coarse-to-fine in movies, animations, and TV shows Coarse Detection In the second module of the project, the Optical flow algortihms is used to find the sum of consistency and detect any suspected tampered points in the frame sequence.

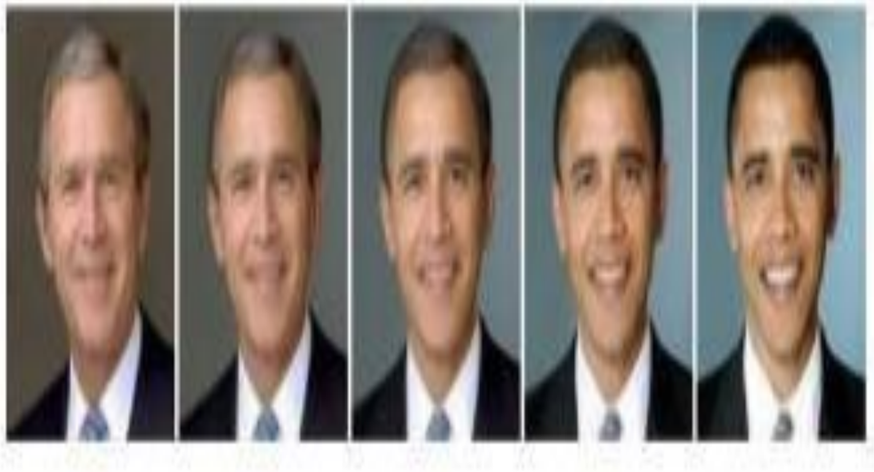

Fig. 2 Image morphing

Fine Detection In the next phase of the project, the GLCM algorithm is applied to detect any duplication in frames (i.e., adding or removal of any object) followed by frame detection and frame validation algorithms to further detect any tampering and recover the original frame/image.

The proposed system first train a machine learning model to preprocess the dataset of videos The proposed model is developed for four modules.

3. VIDEO TAMPERING DATASETS

Video forgery also plays a crucial role in media forensics and has even more severe implications for society than fake images. The recent progress of synthetic video generation and manipulation can cause significant problems like spreading false information, loss of trust in digital content, and fake news. In this section, we discuss some popular video manipulation and tampering datasets used to generate synthetic videos and how hard is to detect such videos, either by using deep learning techniques or by humans.

The most relevant DeepFake video datasets are discussed and compared in Table 5. 3.2.1 First- generation datasets UADFV dataset contains 49 real as well Deepfake videos generated using FakeApp [55]. Later, Korshunova et al. [56] introduced a dataset named Deep Fake-TIMIT, which contains 640 fake videos generated using faceswapGAN.16 Rossler et al. [57] introduced Face forensics which is one of the largest facial forgeries dataset containing roughly 1.8 million manipulated images. The tampered images are created with four state-of-the-art methods, namely Face2Face [58], DeepFake [59], Face Swap [60], and Neural Textures

[61].

The aim is to help researchers to use deep learning approaches in forgery detection. Apart from the novel dataset, the authors also provide a benchmark for facial manipulation detection. The dataset17 is easily accessible after filling a google form for research purposes. 3.2.2 Second-generation datasets.

The databases consisting of second generation are released in late 2019. These datasets goals are to provide high quality synthetic videos that are available on the Internet.

18 Deepfake Detection [62] dataset contains around 3K videos generated from 28 consented individuals from different ages, sex, and ethnic groups.

The DFD dataset is available in three levels of video quality:

- Original quality (RAW),
- Low quality (LQ),
- High quality (HQ).

The DFDC [53] dataset is from the Facebook Deepfake detection challenge which contains around 4K fake videos generated from 66 consented individuals of various ages, sex, and ethnic groups. In 2020, Jiang et al. [63] introduced a real-world fa forgery detection dataset.

The Deeper Forensics-1.0 dataset19 contains both images and videos from 100 paid actors giving consent to use and manipulate their faces.

4. IMAGE MANIPULATION

Imagery manipulation (IM) is a process of editing animage or video using some operation via computer software or other digital devices like mobile and tablets. IM is also known as image editing.

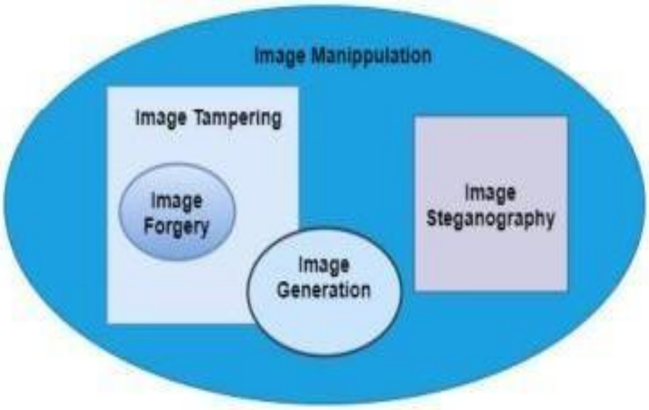

Fig. 1 Image manipulation and its types

Nowadays, cameras are substituted by mobiles which can generate high-quality digital photographs and are also equipped with some editing applications like movie, videos, etc. Digital photographs are becoming an integral part of our daily life. From birthdays to marriage ceremonies, photographs are used to remember and store ones personal memory. Image editing applications are used to add some visual effects to images and videos that make them look beautiful in such images. In this paper, the term image manipulation is used instead of digital image editing for clarification purposes. Image manipulation and its types are shown in Fig. 1. The image manipulation can include operations like resampling which is a pixel- level operation to remove and add objects within an image.

5. CONCLUSION

Throughout this literature survey, a number of video forgery detection mechanisms and techniques have been discussed with different perspectives. Video tampering is done using different methods. So it is obvious that there should be different methods to detect these different types of video forgery. No single detection method works best for every situation. So what video forgery detection method is appropriate for a given situation depends on a number of reasons such as:

- Techniques used for video forgery
- Available technology
- Computational restrictions
- Video quality
- Video formats So it is essential to understand the requirement and the environmental parameters as described above in video forgery detection.

6. REFERENCES

[1] Liu, Yuqing & Huang, Tianqiang. (2015). Exposing video inter-frame forgery by Zernike opponent chromaticity moments and coarseness analysis.

[2] Hsu, Chih-Chung & Hung, Tzu-Yi & Lin, Chia-Wen & Hsu, Chiou-Ting. (2008). Video forgery detection using correlation of noise residue. MMSP. 170-174. 10.1109/MMSP.2008.4665069.

[3] Kingra, Staffy & Aggarwal, Naveen & Singh, Raahat. (2017). Inter-frame forgery detection in H.264 videos using motion and brightness gradients.

[4] Survey on keypoint based copy-move forgery detection methods on image. (2014) Devanshi Chauhan, Dipali Kasat, Sanjeev Jain, Vilas Thakar.

AUTHOR PROFILE

[5] Varun Vijay Ghatage received the B.E. degree in Computer Science & Engineering from University BDT College of Engineering, Davanagere, under VTU, Belgaum.

[6] Shivanand M N received the B.E. degree in Computer Science & Engineering from University BDT College of Engineering, Davanagere, under VTU, Belgaum.