International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Video Legacy Prediction using Scalar Features andMachine Learning

Aakash[1], Bala[2], Vishwa[3], Prof Baskar[4]

[1]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: amaakash15@gmail.com
[2]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: balanmt1929@gmail.com
[3]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: sv737712@gmail.com
[4]Assistant professor, EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India
E-Mail: baskar@egspec.org

ABSTRACT

Nowadays with the ongoing development of video editing techniques, it becomes increasingly easy to modify the digital videos. How to identify the authenticity of videos has become an important field in information security. Video forensics aims to look for features that can distinguish video forgeries from original videos. Thus, people can identify the authenticity of a given video. A kind of distinguishing method which is based on video content and composed of copy-move detection and inter-frame tampering detection becomes a hot topic in video forensics. In the current times the level of video forgery has increased on the internet with the increase in the role of malware that has made it possible for any user to upload, download and share objects online including audio, images, and video. Specifically, Video Editor and Adobe Photoshop are some of the multimedia software and tools that are used to edit or tamper medial files. Added to this, manipulation of video sequence in a way that objects within the frame are inserted or deleted are among the common malicious video forgery operations. In this project, video forgery is detected that use video forgery detection in the form of features extraction from frames and matched with original videos. We can implement Scale Invariant Feature Transform (SIFT) are improved for detection of copy move attacks. In this method, firstly image key points are extracted and multi-dimensional feature vector named as SIFT descriptor is generated for each key point. Then, these key points are matched using distance among their descriptors. Although this method is good at detection of copy move attacks. We can provide results about total percentage of forged and identify which frame to be forged. And design the application as window-based application with image processing techniques.

Keywords:Video forgery detection, Deep Learning algorithm

1. INTRODUCTION

Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems. Digital video evidence is most commonly created by passive and active recording systems. A passive recording system is a recording system that doesn't store information in its memory system. An active recording system is a recording that stores information in its memory system. Active recording systems are most commonly produced with a digital storage medium such as a HDD, SSD or Volatile (flash) memory. Video recorders create digital video recordings in these types of formats:

* Bala.Phone.no:+916369345940.
E-mail address: balanmt1929@gmail.com

Open-source format: An open-source format is a file format for storing digital data, defined by a published specification usually maintained by a standards organization, and which can be used and implemented by anyone.
Proprietary format: A proprietary format is a file format of a company, organization, or individual that contains data that is ordered and stored according to a particular encoding-scheme. This scheme is designed by the company or organization to be secret, such that the decoding and interpretation of this stored data is easily accomplished only with particular software or hardware that the company itself has developed. These formats are more common when video evidence is extracted directly from the system that created it, because they are a more secure and higher quality formatting. These proprietary formats also contain digital information like Meta Data and Telemetry Data that can assist a video forensic investigation.
Courtroom ready format: A copy of the video recording that is easily playable in a court of law using a computer, projection system, or large television. This digital format today should be tested on the system that it will be played through prior to presentation in court. Often times this format is deliverable in the form of a flash drive, DVD or Data Disc. Although the playable copy will be encoded in a common video format (MP4, AVI, WMV) it still may require a freeware player like VLC player or DVD playback software to advance frames as well as play or decode smoothly. Forensic video analysis and authentication is the scientific processes performed by a trained video forensic expert in order to determine events that occurred at the time of the video recording. CCTV cameras do not see the same as the human eye. Some of the video recordings we examine in our lab have been altered either with malice or unintentionally using processes that alter the integrity of the evidence. As video forensic experts we help our client attorneys understand any anomalies in the video recording we are asked to analyze and perform several scientific tests to determine the nature of any anomalies. The existence of digital video and digital image editing tools has made it challenging to accurately authenticate multimedia content. The current manipulation technique and the dynamic multimedia technology evolution made it possible even for a novice to easily delete an object from a video sequence, or add an object from another video source, or insert an object developed by graphics software designer. It has become complicated to comprehend and differentiate an authentic video from a tampered one.

2. METHODOLOGY

VIDEO ACQUISITION:

In this module, we can upload the videos that are considered as query videos. Admin can have original videos which are known as reference videos. We can convert the videos into frames at every 0.5 seconds using video file reader coding. Each frame is considered as single image.

VIDEO FEATURES EXTRACTION:

Feature extraction involves reducing the number of resources required to describe a large set of data. When performing analysis of complex data one of the major problems stems from the number of variables involved. Feature extraction is a general term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient accuracy. In this module, we can extract the features of each frame such as color, shape of object, background features and so on. These features are extracted for future integrity checking.

SEGMENTATION OF VIDEOS:

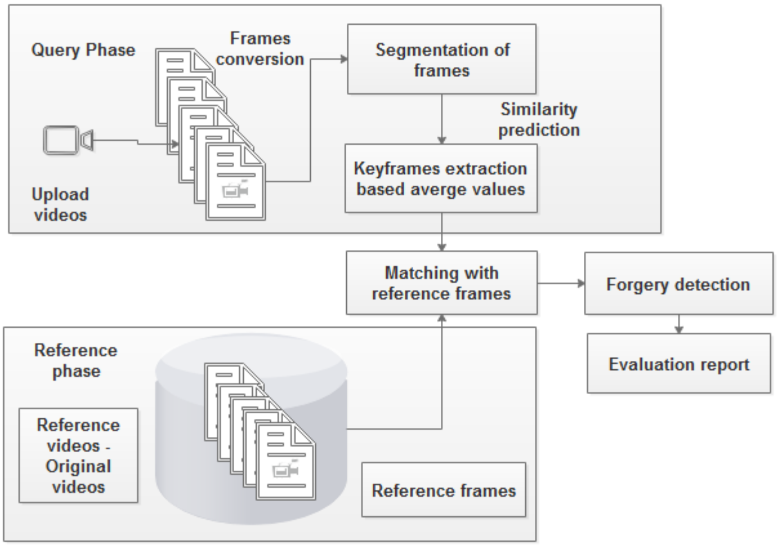
Segmentation means grouping of frames based on video features. Video segmentation is a way of dividing frames into meaningful segments. In the context of video capture, segmentation is best applied to captured screen presentation that the presenter goes through slide after slide. The program compares and calculate the similarity of each video frames to consider whether there is a change in the scenery or not. If they are a change, we break the video here and finally we will break the video into shots. We assume the first frame of each shot as the key frame and output the key frame to the users. We follow the basic idea of Color Indexing to compare the similarity of two video frames. In this module, key frames are extracted and stored as segmented frames.

VIDEO FRAMES CLASSIFICATION:

After segmentation, we can list out possible frames which are less than the total video frames. In this module, query video segmented frames are matched with reference segmented video frames. Similarity values are calculated based on both frames. These values are calculated based on color, shape and texture values of each frame.

3. MODELING AND ANALYSIS

In this project, video forgery is detected that use video forgery detection in the form of features extraction from frames and matched with original videos. We can implement Scale Invariant Feature Transform (SIFT) are improved for detection of copy move attacks. In this method, firstly image key points are extracted and multi-dimensional feature vector named as SIFT descriptor is generated for each key point. Then, these key points are matched using distance among their descriptors. Although this method is good at detection of copy move attacks. We can provide results about total percentage of forged and identify which frame to be forged. And design the application as window-based application with image processing techniques.



Future Enhancement

In future, some other techniques can be used to detect forgery from videos so as to validate other methodologies with present technique. In the future we can use real time videos to detect the copy and paste part with the help of frames and masking. To detect these different techniques applied that is SURF, correlation and filters.

4. RESULTS AND DISCUSSION

Existing System

In recent years due to easy availability of video and image editing tools it has become a difficult task to authenticate the multimedia content. Due to the availability of inexpensive and easily-operable digital multimedia devices (such as digital cameras, mobiles, digital recorders, etc.), together with high-quality data processing tools and algorithms, has made signal acquisition and processing accessible to a wide range of users. As a result, a single image or video can be processed and altered many times by different users. This fact has severe implications when the digital content is used to support legal evidences since its originality and integrity cannot be assured. Important details can be hidden or erased from the recorded scene, and the true original source of the multimedia material can be concealed. Moreover, the detection of copyright infringements and the validation of the legal property of multimedia data may be difficult since there is no way to identify the original owner. Digital videos and images having fraudulent content are used for illegal activities. Therefore, integrity of digital content needs to be verified. This can be done by analyzing the properties of the digital media. The existing method divides the test video into frames, and partitions each frame into non-overlapping 12 × 12 sub-blocks. It applies discrete cosine transform (DCT) to each sub-block at each frame and transforms them into the frequency domain. Average DCT value for each sub-block is calculated, and a row vector is obtained from each frame that contains averaged DCT values. The obtained row vectors for each frame are then binarized. The proposed method calculates a correlation matrix from binary row vectors and creates a correlation image for the current test video. Brighter pixels in the correlation image denote similar frames.

Disadvantages

- Difficult to identify forged video frames
- Time complexity can be occurred to check integrity of digital content
- Image forgery only analyzed in existing system
- Need advanced tools for check video originality

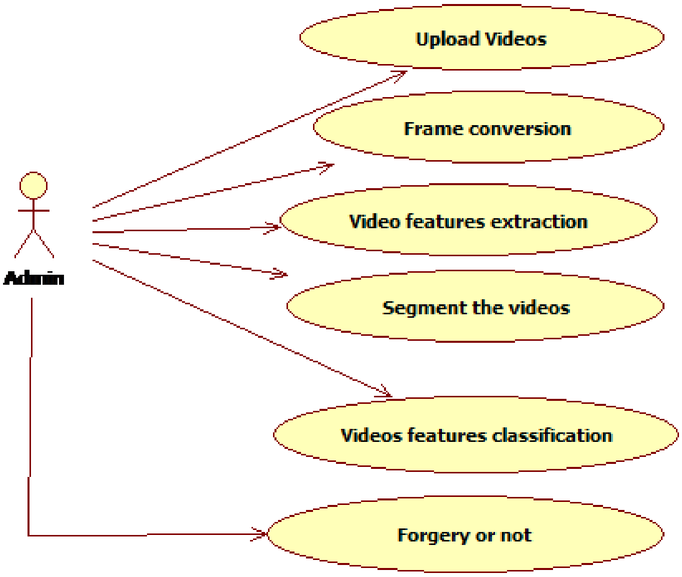
Proposed System

When a video sequence is captured, there is typically a great deal of redundancy between the successive frames of video. The MPEG video compression technique exploits this redundancy by predicting certain frames in the video sequence from others, then by encoding the residual difference between the predicted frame and the actual frame. Because the predicted difference can be compressed at a higher rate than a frame in its entirety, this leads to a more efficient compression scheme. Performing compression in this manner has its drawbacks, however, because error introduced from one frame will propagate to all frames predicted from it. To prevent error propagation, the video sequence is divided into segments, where each segment is referred to as a group of pictures (gop). Frame prediction is performed within each segment, but never across segments, thus preventing decoding errors in one frame from spreading throughout video sequence. Within each group of pictures, frames are divided into three types: intra-frames (I-frames), predicted-frames (P-frames), and bidirectional-frames (B-frames). Each gp begins with an I-frame, followed by a number of P-frames and B-frames. No prediction is performed when encoding I-frames; therefore, each I-frame is encoded and decoded independently. During encoding, each I-frame is compressed through a loss process similar to JPEG compression. P-frames are predicatively encoded through a process known as motion estimation. SIFT features are extracted from gray-level image and tend to be invariant to most of the post processing methods. They are used in a variety of image processing applications ranging from medical to space-based application. It is the most widely studied algorithm and also has a variety of modified versions to it.

Advantages

- Easily identify the forged video frames
- Time is consuming to check the integrity of videos
- There is no need to implement tools for checking forged videos
- Can be detect the tampered regions in video frames

Use Case Diagram



Algorithm

DEEP LEARNING ALGORITHM

Deep learning, a subset of machine learning, utilizes a hierarchical level of artificial neural networks to carry out the process of machine learning. The artificial neural networks are built like the human brain, with neuron nodes connected together like a web. While traditional programs build analysis with data in a linear way, the hierarchical function of deep learning systems enables machines to process data with a nonlinear approach. Artificial Intelligence and machine learning are the cornerstones of the next revolution in computing. These technologies hinge on the ability to recognize patterns then, based on data observed in the past, predict future outcomes. This explains the suggestions, Amazon offers as you shop online or how Netflix knows your penchant for bad 80s movies. Although machines utilizing AI principles are often referred to as “smart,” most of these systems don’t learn on their own; the intervention of human programming is necessary. Data scientists prepare the inputs, selecting the variables to be used for predictive analytics. Deep learning, on the other hand, can do this job automatically.

5. CONCLUSION

Digital video forensics aims at validating the authenticity of videos by recovering information about their history. Copy paste forgery, wherein a region from a video is replaced with another region from the same video (with possible transformations). Because the copied part come from the same video, its important properties, such as noise, color palette and texture, will be compatible with the rest of the video and thus will be more difficult to distinguish and detect these parts. The goal of video copy detection is to develop automated video analysis procedure to identify the original and modified copies of a video among the large amount of video data for the purposes of copyright control, monitoring and structuring large video databases. Digital video forensics is a brand-new research field which aims at validating the authenticity of videos by recovering information about their history. The fundamental problems which research found in the literature can be categorized into the natural, forgery detection, flow mapping, and source identification. Therefore, the originality and authenticity of videos or data in many cases become challenging problem. In this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We use segmentation-based forgery detection for forensic tasks such as identifying cut-and-paste forgeries from JPEG compressed videos and SIFT. This SIFT based technique is dependent on feature extraction by using key point detection.

REFERENCES

[1] Saddique, Mubbashar, et al. "Spatial video forgery detection and localization using texture analysis of consecutive frames." Advances in Electrical and Computer Engineering 19.3 (2019): 97-108.
[2] Aloraini, Mohammed, et al. "Statistical sequential analysis for object-based video forgery detection." Electronic Imaging 2019.5 (2019): 543-1.
[3] Du, Mengnan, et al. "Towards generalizable forgery detection with locality-aware autoencoder." arXiv preprint arXiv:1909.05999 (2019).
[4] Amerini, Irene, et al. "Deepfake video detection through optical flow based cnn." Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops. 2019.
[5] Zampoglou, Markos, et al. "Detecting tampered videos with multimedia forensics and deep learning." International Conference on Multimedia Modeling. Springer, Cham, 2019.
[6] Stütz, Thomas, Florent Autrusseau, and Andreas Uhl. "Non-blind structure-preserving substitution watermarking of H. 264/CAVLC inter-frames." IEEE Transactions on Multimedia 16.5 (2014): 1337-1349.
[7] Pun, Chi-Man, Xiao-Chen Yuan, and Xiu-Li Bi. "Image forgery detection using adaptive oversegmentation and feature point matching." IEEE Transactions on Information Forensics and Security 10.8 (2015): 1705-1716.
[8] Mol, Jacob Jan-David, et al. "The design and deployment of a bittorrent live video streaming solution." 2009 11th IEEE International Symposium on Multimedia. IEEE, 2009.
[9] Thouin, Frederic, and Mark Coates. "Video-on-demand networks: design approaches and future challenges." IEEE network 21.2 (2007): 42-48.
[10] Carlsson, Niklas, and Derek L. Eager. "Server selection in large-scale video-on-demand systems." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 6.1 (2010): 1-26.