IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

VIDEO FORENSIC ANALYSIS USING SCALAR INVARIENT FEATURE TRANSFORM ANALYSIS

[1]K.Kowsalya, [2]M.Janaki, [3]R.Malavika, [4]A.Sumathi

, [1] B.E CSE Student, [2]B.E CSE Student, [3]B.E CSE Student, [4]Assistant Professor
[1,2,3,4]Department of Computer Science and Engineering,
[1,2,3,4] Sri Ramakrishna College of Engineering, Perambalur, Tamil Nadu

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.

Index Terms **– Video forensics, authenticity, Scale Invariant Feature Transform, Image processing.**

I. 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.

II. LITERATURE SURVEY

1. Title: Spatial Video Forgery Detection And Localization Using Texture Analysis Of Consecutive Frames

Author: Mubbashar Saddique

In spatial domain, forgery can be done in two different ways (i) copy move and, (ii) splicing. In copy move forgery, the object is copied and pasted in the frames of the same video, whereas in splice forgery, the object is taken from another video and pasted in the frames of a video. Spatial video forgery detection aims to find whether the video is forged or not? Whereas, the localization digs out which frames of the video are forged and the exact regions, where an object or some parts are tampered in these frames. In this research, the focus is on both the detection of forged video segments (VSs) and localization of forged frames. During spatial domain video tampering, the texture of micro-patterns is changed in tampered frames, which is a very strong clue to detect this kind of forgery. And applied texture descriptor Histogram of Oriented Gradients (HOG) to model the tampering traces in video frames. This descriptor and its variants employ gradient orientation, which cannot describe local texture micro-patterns and variations effectively. HOG gives only shape information due to occurrences of gradient orientation, hence not robust to noise and scale variations Local Binary Pattern (LBP) are another popular texture descriptor, which is investigated for image forgery detection. It has been used for many classification tasks. This descriptor is robust against monotonic illumination changes and contrast variation; however, it is sensitive to noise and small gray-level fluctuations. Moreover, LBP also does not incorporate the edge strengths.

DISADVANTAGES

- Only analyzed single frames.

2. Title: Statistical Sequential Analysis For Object-Based Video Forgery Detection

Author: Mohammed Aloraini

For many years, surveillance videos have become essential for social security that monitors many organizations, and thus, it is important to ensure the reliability of these surveillance videos. If these recorded videos are abused, it could lead to many critical problems that are related to public security or legal evidence. That is, the fundamental challenge is to determine whether a recorded video is authentic or not especially when it is used as critical evidence for judgment. Furthermore, with the advent of powerful and easy-to-use media editing tools, it enables an attacker to maliciously forge a video sequence through adding or deleting an object in a scene with invisible traces and little effort. This forged video is often eye-deceiving and appears in a way that is realistic, hence believable. That is, newspapers are sometimes tricked to use forged videos as if they are authentic. As a result, video contents should be carefully analyzed to ensure its originality and integrity, thus reducing digital crimes. In this paper, we study the problem of detecting object-based video forgery. It is difficult to add moving objects without leaving invisible traces due to possibly different motions and illuminations in videos. We propose an approach to detect removed moving objects from a video scene that is taken from a static camera and estimate a movement of removed objects. In this paper, object-based video forgery is investigated and we have proposed an approach based on sequential analysis. Furthermore, we have shown that the proposed approach can estimate a movement of different sizes of removed objects using spatial decomposition and it can detect temporal changes that are nearly invisible using sequential analysis. Results show that our approach not only outperforms the other approach in terms of Precision, Recall, and F1 score but it is also more robust against compressed and lower resolution videos. Our further research will focus on improving the detection speed of the proposed approach since sequential analysis stage is computationally expensive.

Disadvantages

- Not implemented in real time videos

3. Title: Towards Generalizable Forgery Detection With Locality-Aware Autoencoder

Author: Mengnan Du

With advancements of deep learning techniques, it is now possible to generate super-realistic fake images and videos. These manipulated forgeries could reach mass audience and result in adverse impacts on our society. Although lots of efforts have been devoted to detect forgeries, their performance drops significantly on previously unseen but related manipulations and the detection generalization capability remains a problem. To bridge this gap, in this paper we propose Locality-aware AutoEncoder (LAE), which combines fine-grained representation learning and enforcing locality in a unified framework. In the training process, we use pixel-wise mask to regularize local interpretation of LAE to enforce the model to learn intrinsic representation from the forgery region, instead of capturing artifacts in the training set and learning spurious correlations to perform detection. We further propose an active learning framework to select the challenging candidates for labeling, to reduce the annotation efforts to regularize interpretations. Experimental results indicate that LAE indeed could focus on the forgery regions to make decisions. The results further show that LAE achieves superior generalization performance compared to state-of-the-arts on forgeries generated by alternative manipulation methods. In this work, based on aforementioned observations, we introduce Locality-aware AutoEncoder (LAE) for better generalization of forgery detection. LAE considers both finegrained representation learning and enforcing locality in a single framework for image forensics. To guarantee finegrained representation learning, our work builds upon an autoencoder, which employs reconstruction losses and latent space loss for capturing the distribution for the trained images. To guard against spurious correlations learned by the autoencoder, we augment local interpretability to the antoencoder and use extra pixel-wise forgery ground truth to regularize the local interpretation. As such, the LAE is enforced to capture discriminative representations from the forgery region.

Disadvantages

- Time complexity is high

4 .Title: Deepfake Video Detection through Optical Flow Based Cnn
Author: Irene Amerini

Deep learning techniques are escalating technology sophistication regarding creation and processing of multimedia contents. A new phenomenon, known as Deep Fakes (DF), has recently emerged: it permits to quite simply create realistic videos where people faces, or sometimes only lips and eyes movements, are modified in order to likely simulate the presence of another subject in a certain context or to make someone speak coherently with a different and, probably compromising, speech. The effects can be straightforwardly imagined when this fake information is deliberately used to harm a person such a public figure or a politician, or even an organization like a political party. The impact of Deep Fakes can also be amplified by the action of social networks that deliver information quickly and worldwide. According to this, machine learning community has dedicated a particular and twofold attention to this phenomenon. In this extended abstract, a new technique able to detect deep fake-like videos from original ones is introduced. In particular, unlike state-of-the-art methods which usually act in a frame-based fashion, we present a sequence-based approach dedicated to investigate possible dissimilarities in the temporal structure of a video. Specifically, optical flow fields have been extracted to exploit inter-frame correlations to be used as input of CNN classifiers. In this work, the idea to exploit optical flow field dissimilarities as a clue to discriminate between deep fake videos and original ones has been introduced and investigated. This is a very innovative attempt to take into account possible anomalies in the temporal dimension of the sequence. In this initial experiment, to solve the problem to use pre-trained network, motion vectors have been represented as 3-channels image and then considered as input for a neural network.

Disadvantages

- Computational steps are complex

5. Title: Detecting Tampered Videos With Multimedia Forensics And Deep Learning
Author: Markos Zampoglou

With the proliferation of multimedia capturing devices during the last decades, the amount of video content produced by non-professionals has increased rapidly. Respectable news agencies nowadays often need to rely on User-Generated Content (UGC) for news reporting. However, the videos shared by users may not be authentic. People may manipulate a video for various purposes, including propaganda or comedic effect, but such tampered videos pose a major challenge for news organizations, since publishing a tampered video as legitimate news could seriously hurt an organization's reputation. This creates an urgent need for tools that can assist professionals to identify and avoid tampered content. Multimedia forensics aims to address this need by providing algorithms and systems that assist investigators with locating traces of tampering and extracting information on the history of a multimedia item. Research in automatic video verification has made important progress in the recent past; however, stateof-the-art solutions are not yet mature enough for use by journalists without specialized training. Currently, real-world video forensics mostly rely on expert verification, i.e. trained professionals visually examining the content under various image maps (or filters4) in order to spot inconsistencies. In this work, we explore the potential of two such novel filters, originally designed for human visual inspection, in the context of automatic verification. The filter outputs are used to train a number of deep learning visual classifiers, in order to learn to discriminate between authentic and tampered videos. Besides evaluations on established experimental forensics datasets, we also evaluate them on a dataset of well-known tampered and untampered news-related videos from YouTube to assess their potential in real-world settings.

Disadvantages

- There is no proper approach in video forgery detection

III. 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

IV.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.

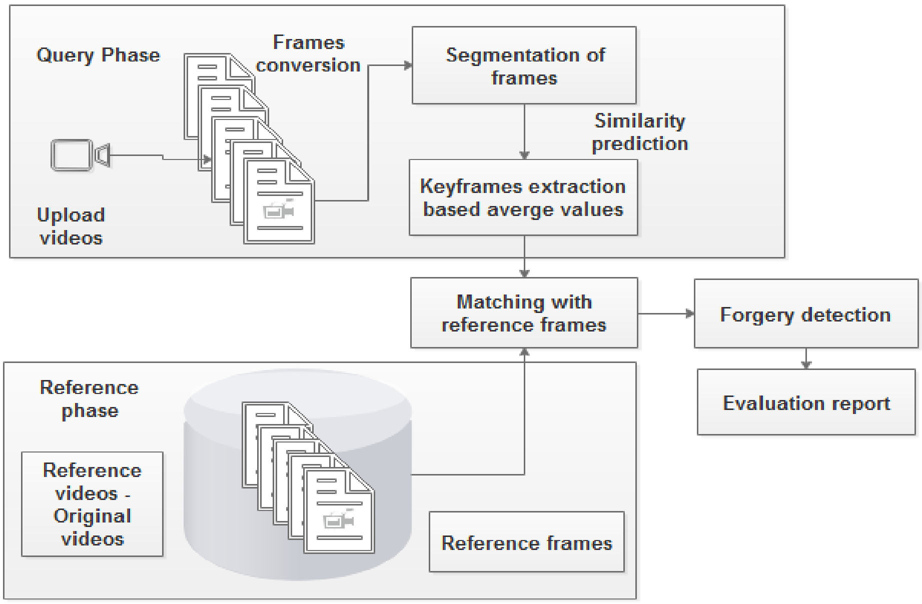

Fig 1. System Architecture

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

V.MODULES

1. 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.

2. VIDEO FEATURES EXTRACTION:

Feature extraction involves reducing the amount 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.

3. SEGMENTATION OF VIDEOS:

Segmentation means grouping of frames based on video features. Video segmentation is a ways 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 compare 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.

4. 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.

5. FORGERY PREDICTION:

If the similarity values are not same means, video should be considered as forgery videos. Otherwise, consider as original values. If it is forgery means, predict the forgery frames from query videos.

VI.CONCLUSION

Digital video forensics aims at validating the authenticity of videos by recovering information about their history. Copy paste forgery, wherein a region from an 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, colour 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. This strategy is for the most part used to Location of vindictive control with computerized recordings (advanced frauds) if there should arise an occurrence of duplicate move assault. The proposed work has been discovered viable result as correlation with leaving model. 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.

VII.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.