International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 865-869 www.ijaem.net ISSN: 2395-5252

Video Forensic Analysis Using Scalar Invariant Methodology

Dr.J.Arun,[1] M.E., Ph.D., Head Of The Department, K.Anitha,[2] S.Aswinimeenatchi,[3] R.Bavithra,[4] P.Jeyasurya[5]
Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur.

Submitted: 05-05-2021 Revised: 17-05-2021 Accepted: 20-05-2021

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.

I. INTRODUCTION

Computer forensics 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.

APPLICATIONS OF NEURAL NETWORK

Neural networks are broadly used, with applications for financial operations, enterprise planning, trading, business analytics and product maintenance. Neural networks have also gained widespread adoption in business applications such as forecasting and marketing research solutions, fraud detection and risk assessment. A neural network evaluates price data and unearths opportunities for making trade decisions based on the data analysis. The networks can distinguish subtle nonlinear interdependencies and patterns other methods of technical analysis cannot. According to research, the accuracy of neural networks in making price predictions for stocks differs. Some models predict the correct stock prices 50 to 60 percent of the time while others are accurate in 70 percent of all instances. Some have posited that a 10 percent improvement in efficiency is all an investor can ask for from a neural network.

DEEP LEARNING

Deep learning is an artificial intelligence (AI) function that imitates the workings of the human brain in processing data and creating patterns for use in decision making. Deep learning

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 865-869 www.ijaem.net ISSN: 2395-5252

is a subset of machine learning in artificial intelligence that has networks capable of learning unsupervised from data that is unstructured or unlabeled. Also known as deep neural learning or deep neural network. Deep learning is an AI function that mimics the workings of the human brain in processing data for use in detecting objects, recognizing speech, translating languages, and making decisions. Deep learning AI is able to learn without human supervision, drawing from data that is both unstructured and unlabeled. Deep learning, a form of machine learning, can be used to help detect fraud or money laundering, among other functions. Deep learning has evolved hand-in-hand with the digital era, which has brought about an explosion of data in all forms and from every region of the world. This data, known simply as big data, is drawn from sources like social media, internet search engines, e-commerce platforms, and online cinemas, among others. This enormous amount of data is readily accessible and can be shared through fintech applications like cloud computing.

II. LITERATURE SURVEY

2.1 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.

DISADVANTAGES

- Only analyzed single frames

2.2 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.

DISADVANTAGES

- Not implemented in real time videos

III. SYSTEM ANALYSIS

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,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 865-869 www.ijaem.net ISSN: 2395-5252

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

IV. SYSTEM IMPLEMENTATION

MODULES DESCRIPTION

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.

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

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 865-869 www.ijaem.net ISSN: 2395-5252

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:

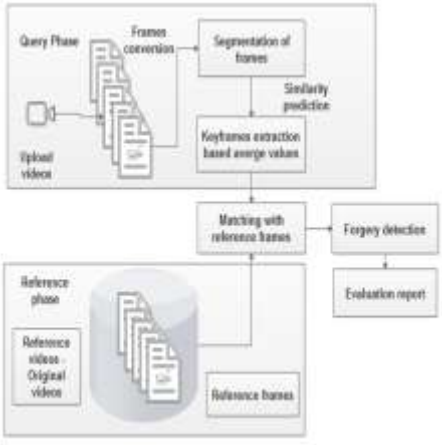
After segmentation, we can list out possible frames which are less than the total video frames. In this module, query video segmented frames are matched with reference segmented video frames. Similarity values are calculated based on both frames. These values are calculated based on color, shape and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

V. SYSTEM DESIGN

SYSTEM ARCHITECTURE



VI. SOFTWARE DESCRIPTION

FRONT END - ANDROID STUDIO

Android (stylized as android) is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smart phones and tablets. Android's user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input. In addition to touch screen devices, Google has further developed Android TV for televisions, Android Auto for cars, and Android Wear for wrist watches, each with a specialized user interface. Variants of Android are also used on notebooks, game consoles, digital cameras, and other electronics. World is contracting with the growth of mobile phone technology. As the number of users is increasing day by day, facilities are also increasing. Starting with simple regular handsets which were used just for making phone calls, mobiles have changed our lives and have become part of it. Now they are not used just for making calls but they have innumerable uses and can be used as a Camera , Music player, Tablet PC, T.V. , Mobile browser etc . And with the new technologies, new software and operating systems are required.

DEFINITION OF ANDROID OPERATING SYSTEM

Operating Systems have developed a lot in last 15 years. Starting from black and white phones to recent smart phones or mini computers, mobile OS has come far away. Especially for smart phones, Mobile OS has greatly evolved from Palm OS in 1996 to Windows pocket PC in 2000 then to Blackberry OS and Android. One of the most widely used mobile OS these days is ANDROID. Android does a software bunch comprise not only operating system but also middleware and key applications. Android Inc was founded in Palo Alto of California, U.S. by Andy Rubin, Rich miner, Nick sears and Chris White in 2003. Later Android Inc. was acquired by Google in 2005. After original release there have been number of updates in the original version of Android.

FEATURES & SPECIFICATIONS

Android is a powerful Operating System supporting a large number of applications in Smart Phones. These applications make life more comfortable and advanced for the users. Hardware's that support Android are mainly based on ARM architecture platform. Some of the current features and specifications of android are:

- Android comes with an Android market which is an online software store. It was developed by Google. It allows Android users to select, and download applications developed by third party developers and use them. There are around 2.0 lack+ games, application and widgets available on the market for users.
- Android applications are written in java programming language. Android is available as open source for developers to develop applications which can be further used for selling in android market. There are around 200000 applications developed for android

with over 3 billion+ downloads. Android relies on Linux version 2.6 for core system services such as security, memory management, process management, network stack, and driver model. For software development, Android provides Android SDK (Software development kit).

VII. APPLICATIONS

These are the basics of Android applications:

- Android applications are composed of one or more application components (activities, services, content providers, and broadcast receivers)
- Each component performs a different role in the overall application behavior, and each one can be activated individually (even by other applications)

Google, for software development and application development, had launched two competitions ADC1 and ADC2 for the most innovative applications for Android. It offered prizes of USD 10 million combined in ADC1 and 2. ADC1 was launched in January 2008 and ADC 2 was launched in May 2009. These competitions helped Google a lot in making Android better, more user friendly, advanced and interactive.

Applications ("apps"), which extend the functionality of devices, are written using the Android software development kit (SDK) and, often, the Java programming language, which has complete access to the Android APIs. Java may be combined with C/C++, together with a choice of non-default runtimes that allow better C++ support;[70][71][72] the Go programming language is also supported since its version 1.4, which can also be used exclusively although with a restricted set of Android APIs. The SDK includes a comprehensive set of development tools, including a debugger, software libraries, a handset emulator based on QEMU, documentation, sample code, and tutorials. Initially, Google's supported integrated development environment (IDE) was Eclipse using the Android Development Tools (ADT) plugin; in December 2014, Google released Android Studio, based on IntelliJ IDEA, as its primary IDE for Android application development. Other development tools are available, including a native development kit (NDK) for applications or extensions in C or C++, Google App Inventor, a visual environment for novice programmers, and various cross platform mobile mobile applications frameworks. In January 2014, Google unveiled an framework based on Apache Cordova for porting Chrome HTML 5 mobile applications to Android, wrapped in a native application shell.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

Digital video forensics aims at validating the authenticity of videos by recovering information about their history. Copypaste 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, 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.

FUTURE ENHANCEMENTS

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.

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.