International Journal of Research Publication and Reviews

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

Video Forensic Analysis Using Scalar Invariant Feature Transform And Deep Learning Algorithm

Prabakaran G M *[a], Naveen Kumar M *[b], Balaji G *[c], Poongavanam N *[d]

[*a,*b,*c] *UG student, Department of Computer Science and Engineering, Anjalai Ammal Mahalingam Engineering College,Thiruvarur, Tamilnadu, India*

[*d] *Assistant professor, Department of Computer Science and Engineering, Anjalai Ammal Mahalingam Engineering College,Thiruvarur, Tamilnadu, India*

ABSTRACT

Nowadays with the constant growth of video editing techniques, it becomes more and more easy to modify the digital videos. Video forensics aims to look for aspect that can discriminate video forgeries from original videos. A kind of discriminate method which is formed on video content and collected of copy-move detection and inter-frame tampering detection becomes a headline in video forensics. In recent times the forgery level has viral on the internet with the grow in the role of malware that has made it possible for any user to upload, download and share files including audio, images, and video. 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 Scalar Invariant Feature Transform improved for detection of copy move attacks. In this method, image keypoints are extracted and multi-dimensional feature vector named as SIFT descriptor is generated for each keypoint. Then, these keypoints are paired using space among their caption. 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:Fake video, Forensics analysis, Forgery detection, Feature learning, Video tampering, Splicing

1. Introduction

Computer forensics (also known as computer forensic science) is a branch of digital forensic science concern to proof found in computers and digital storage media. The goal of computer forensics is to test the digital media in a forensically sound method with the aim of identifying, conserving, recovering, analyzing and presenting reality and belief about the digital information. Although it rare related with the inspection of a broad variety of computer crime, computer forensics may also be used in civil activities. The discipline involves same techniques and concept to data retrieval, but with additional instructions and practices sketched to create a lawful vet trail. Evidence from computer forensics inspection is usually subjected to the same recommendation and practices of other digital evidence. It has been used in a number of prominent cases and is becoming widely accepted as reliable within U.S. and European court systems. Digital video proof is most frequently created by passive and active recording systems. A complaint write down system is a recording system that doesn't store data in its memory system. An active recording system is a recording that stores data in its memory system. The systems are most often assembled with a digital storage medium such as a HDD, SSD or Volatile (flash) memory. Video recorders make video recordings in these types of formats.

.

* *Corresponding author.*
E-mail address: prabakaran192000@gmail.com

- **Open source format:** An open source format is a file format for keeping digital data, defined by a issued identification usually maintained by a standards organization, and which can be used and executed by anyone.
- **Proprietary format:** A proprietary format is a format of file of the organization, individual or company that contains information saved using particular encoding-scheme which is instructed. This scheme is planned by the company or organization to be classified, such that the decoding and explanation of this stored information is easily accomplished only with particular software or hardware that the company itself has developed. These formats are more common when video proof 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 help a video forensic investigation.
- **Courtroom ready format:** A copy of the video recording that is easily take-part in a judiciary using a computer, projection system, or large television. This digital format today should be tested on the system that it will be played through foregoing to granting in judiciary. Most frequent times this format is giving in the form of a flash drive, DVD or Data Disc. Although the frolic copy will be encoded in a common video format (MP4, AVI, WMV) it still may require a free software player like VLC player or DVD playback software to proceed frames as well as play or decode easily. Forensic video analysis and verify the scientific procedure performed by a trained video forensic expert in order to control events that befall at the time of the video recording. CCTV cameras do not see the identical as the human eye. Some of the video recordings we test in our lab have been adjust either with malice or unintended using processes that alter the honesty of the evidence. As video forensic experts we help our client attorneys acknowledge 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 demanding to accurately validate multimedia content. The current contrive technique and the dynamic multimedia technology development 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 evolved by graphics software designer. It has become tangled to comprehend and differentiate an original video from a tampered one.

2. Background

2.1 Forensic video analysis

Forensic video analysis is the scientific scrutiny, comparison and/or evaluation of video in lawful matters. This definition was created by recognized video forensic agencies around the country and internationally.

2.2 Three categories of video forensic scientists

Technician: Intake of the proof, duplicates and converts media, performs preparatory upgrade and other assessments.
Analyst: Includes all technician skills, performs image comparison investigations, aspect ratio calibration, color correction, reverse projection, photogrammetry, authentication, motion tracking, image authentication.
Expert Witness: Includes all technician and analyst skills, provides consultation with litigators, generate formalized reports, peer/technical review, formulating opinions, evidence recovery. With the rapid multiplication of surveillance cameras in public and private places, law enforcement agencies and litigators are increasingly making use of these recordings as proof. Fixed and mobile digital video recorders and other portable video recording CCTV systems are making it easier to capture crime scene video that may be used as proof in judiciary.

2.3 Video analysis and authentication

Forensic video analysis and validate is the scientific procedure performed by a instructed video forensic expert in order to determine events that occurred at the time of the video recording. CCTV cameras do not see the identical as the human eye. Some of the video recordings we test in our lab have been adjust either with malice or unintended using processes that alter the honesty of the evidence. As video forensic experts we help our client attorneys acknowledge any anomalies in the video recording we are asked to analyze and perform several scientific tests to determine the nature of any anomalies.

2.4 Existing system

In recent years due to easy accessibility of video and image editing tools it has become a difficult task to validate the multimedia content. Due to the accessibility of inexpensive and easily-operable digital multimedia devices (such as digital cameras, mobiles, digital recorders, etc.), together with high-quality information altering tools and algorithms, has made signal acquisition and altering reachable to a broad range of users. As a result, a single image or video can be processed and adjust many times by different users. This fact has critical conclusion when the digital content is used to support lawful proof since its originality and honesty cannot be assured. Important details can be hidden or deleted from the recorded scene, and the true original source of the multimedia material can be cover-up. Moreover, the detection of copyright breach and the validation of the lawful property of multimedia information may be hard since there is no way to point-out the original owner. Digital videos and images having counterfeit content are used for unlawful works. Therefore, honesty of digital content needs to be proved. 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 and every one of the sub-block at each and every one of the frame and transforms them into the frequency realm. Average DCT value for each sub-block is calculated, and a row vector is obtained from each frame that contains averaged DCT values. The secure row vectors for each and every one of the frame are then bipartile. The proposed method computes a connection matrix from binary row vectors and creates a connection image for the current trail video. Brighter pixels in the connection image denote same frames.

2.5 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 constriction technique exploits this redundancy by predicting certain frames in the video order 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 forbid error propagation, the video order is divided into segments, where each segment is referred to as a group of pictures (gop). Frame prediction is performed within each and every one of the segment, but never across segments, thus controlling and 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 gop 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 pull-out from gray-level image and tend to be invariant to most of the post processing methods. They are used in a different types 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.

2.6 System architecture

Architecture diagram can split into two phases such as training and testing phase. In training phase, upload the videos into pages. And perform segmentation algorithm to group the frames. Extract the key frames and matched with reference frames. Finally identify the forged frames with improved accuracy rate (see Figure 1).

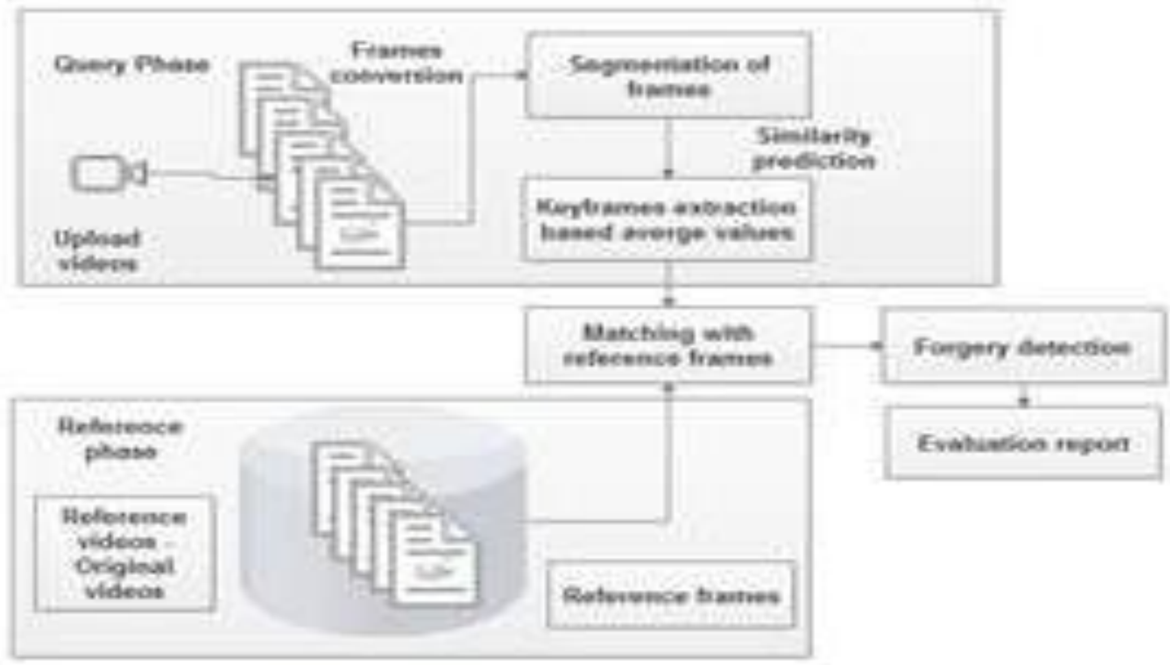


Fig.1- system architecture

3. Methodology

3.1 Modules

- Video acquisition
- Video features extraction
- Segmentation of frames
- Video frames classification
- Forgery prediction

3.2 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 and every single frame is considered as single image.

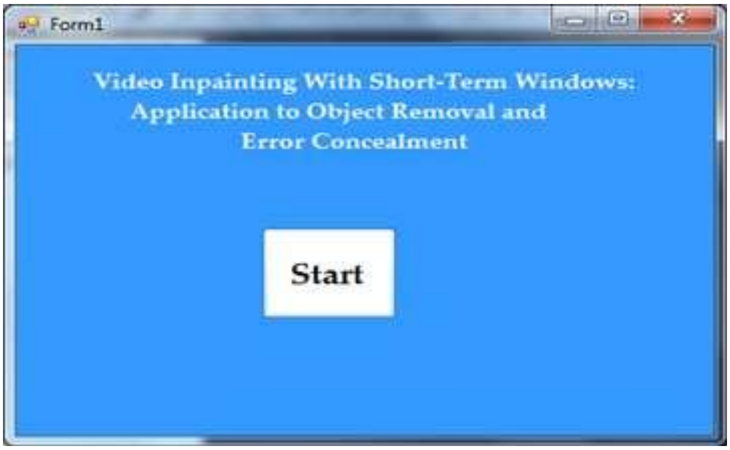
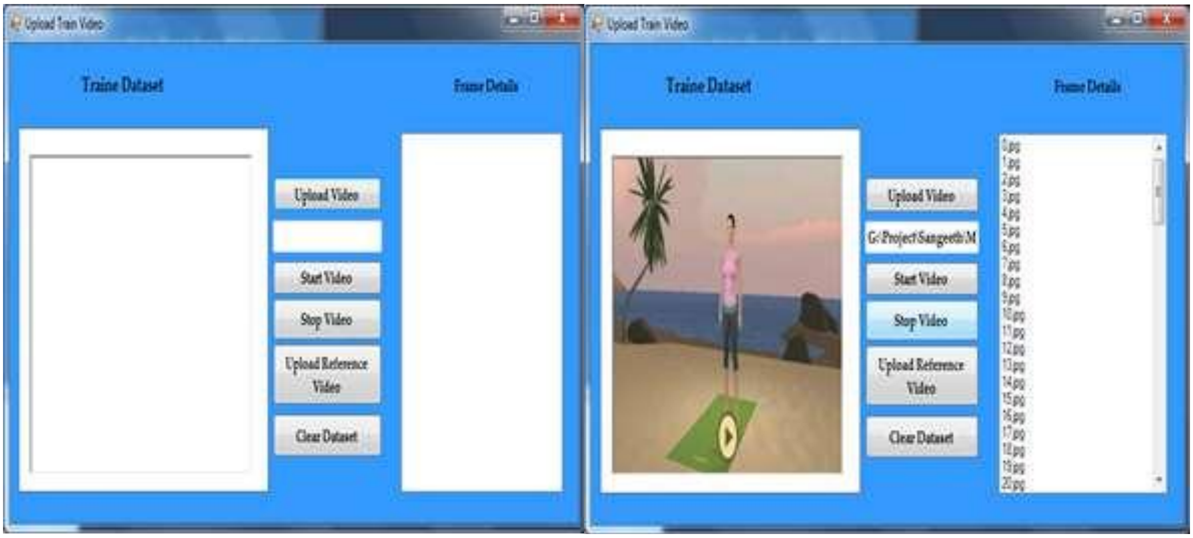
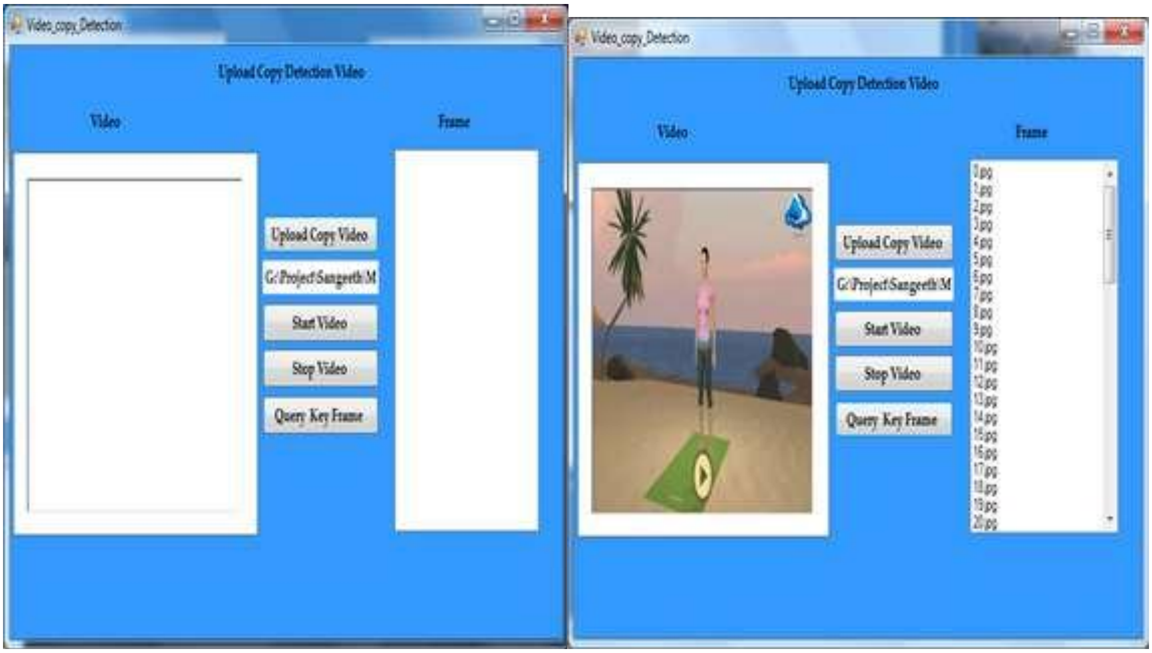

Form1
Video Inpainting With Short-Term Windows: Application to Object Removal and Error Concealment
Start

Fig.2- starting page



a **b**

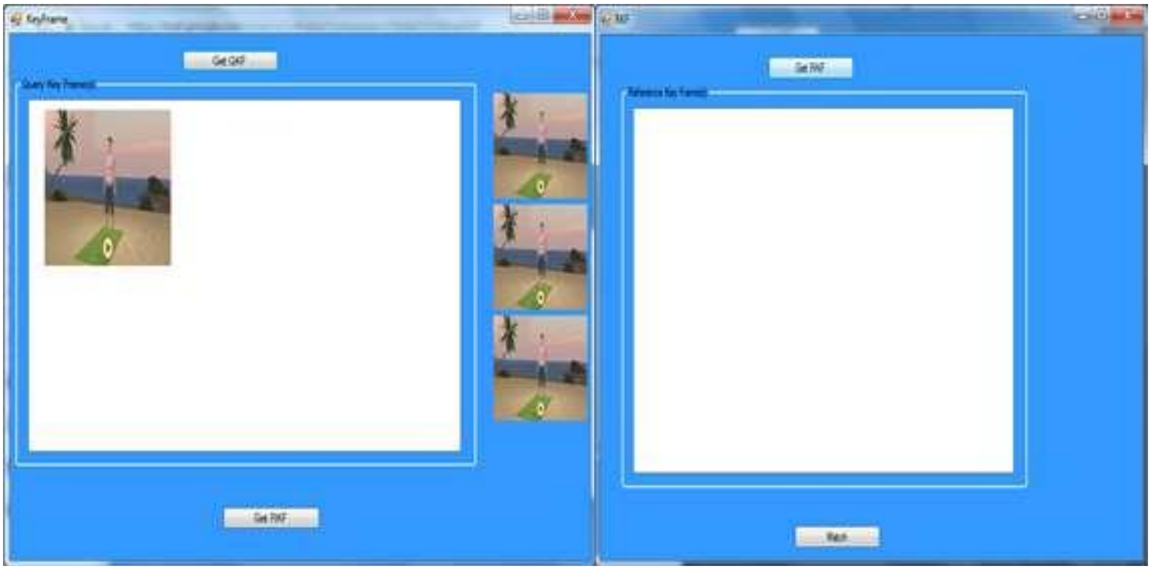


c d

Fig.3- (a) before uploading reference video; (b) after uploading reference video; (c)before uploading copy detection video; (d) after uploading copy detection video.

3.3 Video features extraction

Feature extraction includes decreasing the amount of resources required to narrate a large set of data. When implementing analysis of complex information one of the major problems stems from the number of variables includes. Feature extraction is a common term for methods of building amalgam of the fickle to get around these problems while still describing the data with enough accuracy. In this module, we can extract the features of each and every single frame such as color, shape of object, background features and so on. These features are extracted for future integrity checking.



a b

Fig.4- (a) query key frames; (b) reference key frames

3.4 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 put in to record the screen presentation that the presenter goes through slide after slide. The program differentiate and compute the similarity of each video frames to consider whether there is a change in the scenery or not. If they are a change, we split the video here and finally we will split the video into shots. We assume the first frame of each and every shot as the key frame and output the key frame to the users. We follow the fundamental idea of Color Indexing to differentiate the similarity of two video frames. In this module, key frames are extracted and stored as segmented frames.

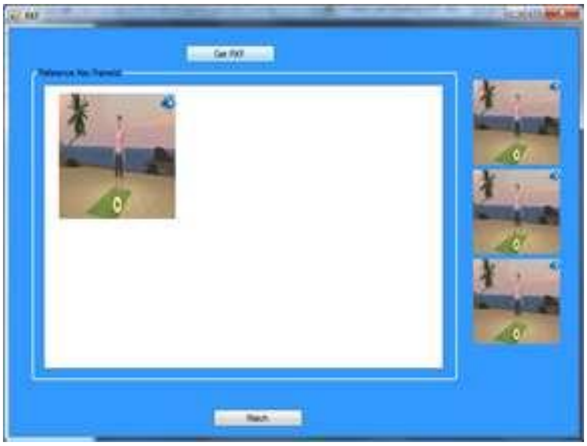
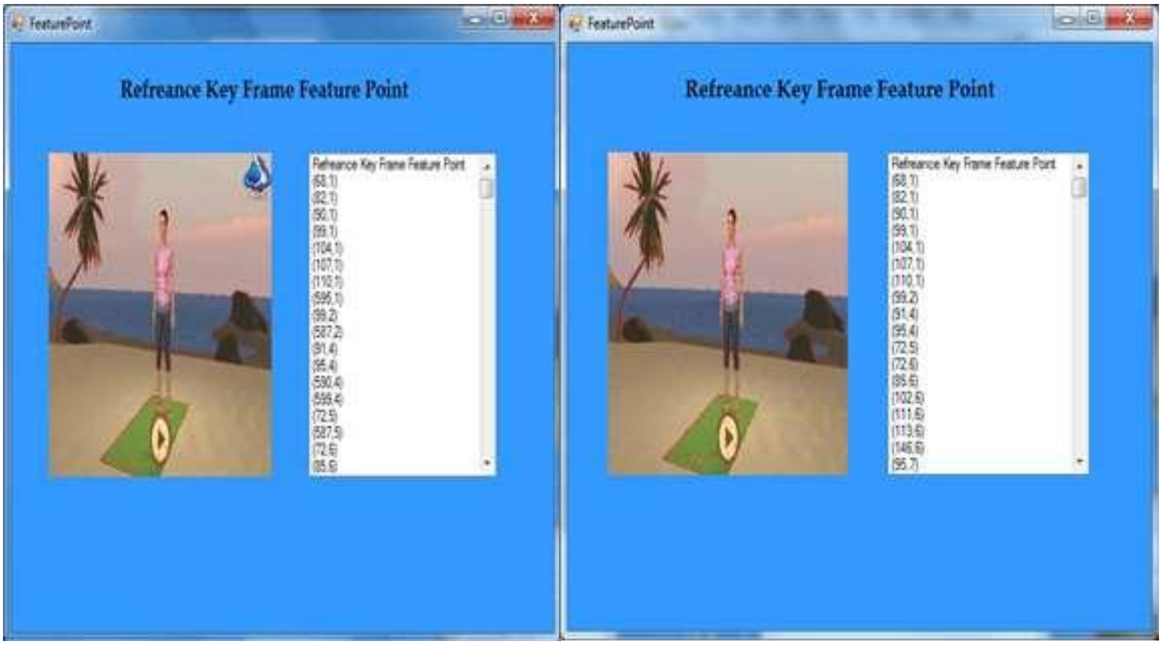


Fig.4- matching the reference key frame

3.5 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.



Refreance Key Frame Feature Point

```
Refreance Key Frame Feature Point
(68,1)
(82,1)
(90,1)
(99,1)
(104,1)
(107,1)
(110,1)
(595,1)
(99,2)
(587,2)
(91,4)
(95,4)
(590,4)
(599,4)
(72,5)
(587,5)
(72,6)
(85,6)
```

Refreance Key Frame Feature Point

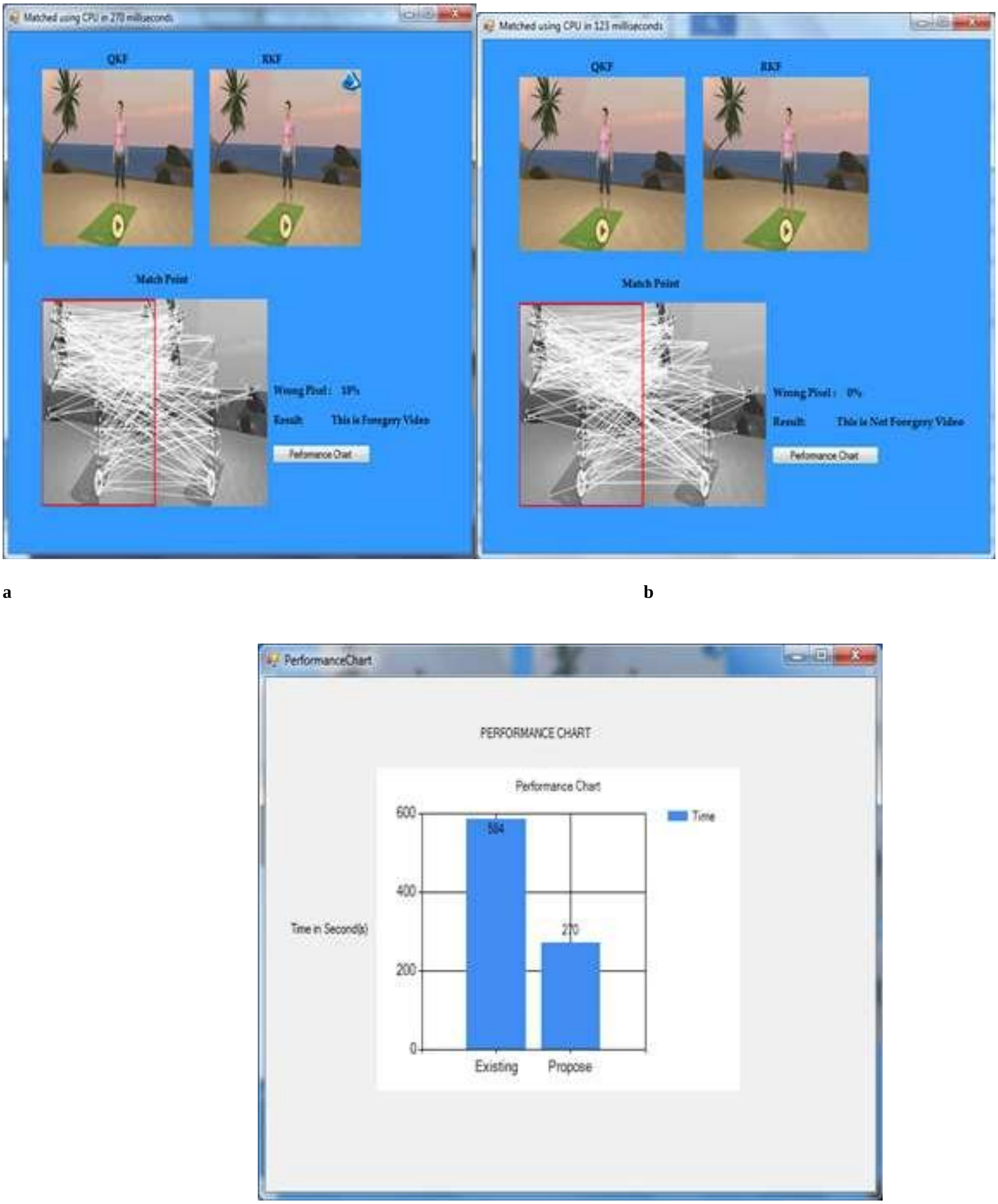
```
Refreance Key Frame Feature Point
(68,1)
(82,1)
(90,1)
(99,1)
(104,1)
(107,1)
(110,1)
(99,2)
(91,4)
(95,4)
(72,5)
(72,6)
(85,6)
(102,6)
(111,6)
(113,6)
(146,6)
(95,7)
```

a **b**

Fig.5- (a) reference key feature point for forged video; (b) reference key feature point for non forged video.

3.6 Forgery detection

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.



Matched using CPU in 270 milliseconds

Wrong Pixel : 10%

Result This is Foregery Video

Matched using CPU in 123 milliseconds

Wrong Pixel : 0%

Result This is Not Foregery Video

a

b

C

Fig.6- (a) Forgery detected; (b) No forged detected; (c) Performance test

4. Result

The proposed video copy detection system utilizes simple but efficient approach for generating features of any input video. The generated features for a particular video is robust, discriminant compact and tolerable for different types of attacks on video signal, including noise addition, changes in brightness/contrast, rotation, spatial/temporal shift and frame loss. After the generation of features, proposed work is to be efficient search of matching against the video database by using fast search methods to find whether an input or query video is pirated or not.

5. Conclusion

Digital video forensics aims at certifying the legality of videos by recovering data about their history. Copy-paste forgery, where in a region from an video is restored with another region from the same video (with possible transformations). Because the duplicated part come from the same video, its important properties, such as noise, color palette and texture, will be adaptable with the rest of the video and thus will be more hard to discriminate and detect these parts. The goal of video copy detection is to develop automated video analysis plan of action to identify the original and modified duplicates of a video among the large amount of video data for the motive of copyright control, monitoring and structuring large video databases. Digital video forensics is a brand new research field which targets at certifying the legality of videos by recovering data about their past. The basic problems which researcher found in the literature can be classified into the natural, forgery detection, flow mapping, and source identification. Therefore, the originality and legality of videos or data in many cases become difficult problem. In this paper of study, we put forward several new digital forensic ideas to detect proof of editing in digital multimedia content. We use segmentation based forgery detection for forensic jobs such as identifying cut-and-paste forgeries from JPEG compressed videos and SIFT. This SIFT based idea 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.

Future enhancements

In future, some other techniques can be used to identify the 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 bit with the help of frames and masking. To detect these different techniques applied that is SURF, correlation and filters.

References

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

Aloraini, Mohammed, et al. "Statistical sequential analysis for object-based video forgery detection." Electronic Imaging 2019.5 (2019): 543-1

Du, Mengnan, et al. "Towards generalizable forgery detection with locality-aware auto-encoder." arXiv preprint arXiv:1909.05999 (2019)

Amerini, Irene, et al. "Deepfake video detection through optical flow based cnn." Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops. 2019

Zampoglou, Markos, et al. "Detecting tampered videos with multimedia forensics and deep learning." International Conference on Multimedia Modeling. Springer, Cham, 2019

Stütz, Thomas, FlorentAutrusseau, and Andreas Uhl."Non-blind structure-preserving substitution watermarking of H. 264/CAVLC inter-frames." IEEE Transactions on Multimedia 16.5 (2014): 1337-1349

Pun, Chi-Man, Xiao-Chen Yuan, and Xiu-Li Bi. "Image forgery detection using adaptive over-segmentation and feature point matching." IEEE Transactions on Information Forensics and Security 10.8 (2015): 1705-1716

Mol, Jacob Jan-David, et al. "The design and deployment of a bit-torrent live video streaming solution." 2009 11th IEEE International Symposium on Multimedia. IEEE, 2009

Thouin, Frederic, and Mark Coates. "Video-on-demand networks: design approaches and future challenges." IEEE network 21.2 (2007): 42-48

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