ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

Analysis of Video File Container Using Feature Descriptor

Khatib Abulais [1], Swarup Fuse[2], Parag Joshi[3], Rahul Bhutra[4], Shafali Gupta[5]

UG Student, Department of Computer Engineering, RMD, Pune Maharashtra, India[1]

UG Student, Department of Computer Engineering, RMD, Pune Maharashtra, India[2]

UG Student, Department of Computer Engineering, RMD, Pune Maharashtra, India[3]

UG Student, Department of Computer Engineering, RMD, Pune Maharashtra, India[4]

Asst. Professor, Department of Computer Engineering, RMD, Pune Maharashtra, India[5]

ABSTRACT: Video Forensics continues growing new innovations to check the validness and the honesty of digital videos. While a large portion of the current techniques depend on the examination of the video information stream, as of late, another line of research was investigate with explore video life cycle dependent on the investigation of the video container. Anyway, existing contributions in this field depend on manual comparison of video container structure and content, or, in other words and mistake inclined. In this work we will introduce a method for unsupervised analysis of video file containers, and present main forensic applications of such method: the first one deals with video integrity verification, based on the dissimilarity between a reference and a target video file container. Scale-Invariant Feature Transform (SIFT) will use for video frame feature extraction. And by using this features will check the actual content loss and forgery in data. The identification of the content loss based on the analysis of containers structure and content of video file.

KEYWORDS: Forensics Analysis, Video Processing, Scale-Invariant Feature Transform (SIFT), Feature Extraction, Forgery Data.

I. INTRODUCTION

Video processing is a particular case of image processing, which often employs video filters and where the input and output are video files or video frames.Digital visual contents are one of the preferred ways to share information through the web. So in case internet traffic, the important data can be lost. Digital videos gained importance also from the intelligence point of view: since they may include sensitive information about an occurred event or the identity of people in the scene, they can represent an important source of evidence during an investigation.

In such a scenario, it is not surprising thatdigital videos gained importance also from the intelligencepoint of view: since they may include sensitive informationabout an occurred event or the identity of people in the scene,they can represent an important source of evidence during aninvestigation. For this reason, Video Forensics has designedseveral tools to blindly deduce the digital history of the videounder analysis, based on the fact that any step in the medialife cycle leaves distinctive traces on the content itself.

Accordingto the Best Practices for Image Content Authenticationof the Scientific Working Group on Digital Evidences,indeed, “content authentication is used to determine whetherthe visual content depicted in imagery is a true and accuraterepresentation of subjects and events”, while “integrity ensuresthat the information presented is complete and unaltered fromthe time of acquisition until its final disposition”. There arecases where authenticity of a video is more important thanits integrity (think to a video found on YouTube showingthe preparation of a terrorist attack: the integrity is surelycompromised by YouTube re-encoding process, yet the contentcould be authentic and worth of attention); there are casesinstead where integrity is more important than authenticityitself (for example, if the

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

previously mentioned video is found, on a suspect's smartphone, it is of prominent importance tounderstand whether it is compatible with the hypothesis ofbeing captured by that device or not). Noticeably, while itis possible to conduct authenticity analysis in a totally blindfashion (that is, without any background knowledge on theoriginating device), it is very difficult to reliably assess theintegrity of a digital content without any information about itssource:

II. RELATED WORK

In this work they introduce a new forensic footprint and, based on it, propose a method for detecting whether a video has been encoded twice; if this is the case, they also estimate the size of the Group Of Pictures (GOP) employed during the first encoding. Advantage is its presence in the twice encoded video without the need of re-compression. If the video is re-encoded after that some frames have been removed [1].

They propose a method for detecting insertion and deletion of whole frames in digital videos. They start by strengthening and extending a state of the art method for double encoding detection, and propose a system that is able to locate the point in time where frames have been deleted or inserted, discerning between the two cases. The advantage is the being able to work when different coding algorithms are used in the first and second compression, a situation that is very common when dealing with DVs [2].

They present a fast forgery detection algorithm based on Exponential-Fourier moments (EFMs) for detecting region duplication in videos. The algorithm first extracts EFMs features from each block in the current frame, and performs a fast match to find potential matching pairs. The advantage is the higher detection accuracy and computational efficiency than those of previous algorithms [3].

The proposed analysis approach enables basic investigations of image authenticity and documents a much better trustworthiness of EXIF metadata than commonly accepted. Manipulations created with the renowned metadata editor ExifTool and various images processing software can be reliably detected. This work makes the creation of convincing forgeries considerably more difficult and provides a valuable method for the toolbox of forensic investigator [4].

This work examines the authenticity of digital video evidence and in particular it proposes a machine learning approach to detecting frame deletion. A number of discriminative features are extracted from the video bit stream and its reconstructed images. The proposed solution works for detecting forged videos regardless of the number of deleted frames, as long as it is not a multiple of the length of a group of pictures [5].

In this work, a Markov based approach in DCT technique and DWT technique domain is proposed for picture splicing detection. The proposed feature vector contain of two kinds of Markov features generated from the transition probability matrices; say the expanded Markov features in DCT domain and the Markov features in DWT domain [6].

In this work, propose a passive copy move picture forgery detection method using a steerable pyramid transform (SPT) technique and Local Binary Pattern (LBP) technique. SPT technique is applied on a grayscale version or one of the YCbCr channels of a picture. LBP technique is applied to describe the texture in each SPT technique sub band. Then the support vector machine (SVM) technique uses the LBP technique feature extracted from SPT technique sub-bands in classifying pictures into tampered or authentic pictures [7].

In this work, they have adopted key point-based features for copy–move picture forgery detection on images; however, our emphasis is on accurate and robust localization of duplicated regions. In this context, they are interested in estimating the transformation (e.g., affine) between the copied and pasted regions of picture more accurately as well as extracting these regions as robustly by reducing the number of false positives and negatives. To address these issues, we propose using a more powerful set of key point based features, called MIFT, which shares the properties of SIFT technique features but also are invariant to mirror reflection transformations [8].

This study proposes a copy-move picture forgery detection technique using Hessian features and a center-symmetric local binary pattern (CSLBP) technique. The proposed method consists of four steps: (1) detecting the object based on normalized cut segmentation, (2) localizing the local interest points of each object based on the Hessian technique, (3) extracting CSLBP features, and (4) detecting duplicated regions in picture forgeries. Experiment results show that the method is robust to post processed copy-move forgery detection under scaling, and JPEG compression [9].

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

III. SYSTEM OVERVIEW

Video Forensics keeps developing new technologies to verify the authenticity and the integrity of digital videos.In this work we introduce a method for unsupervised analysis ofvideo file containers, and present main forensic applications. We will take one reference video and one target video as input to system. After that we will extract all frames from both reference video and target video.All frames will be extracting with same size and stored in specific folder. Then will apply feature extraction techniques to extract the all features from all frames and this features also stored. Then using that all features will check the content of both reference video and target video frame. Finally will shows the content loss and extra content result.

System Architecture

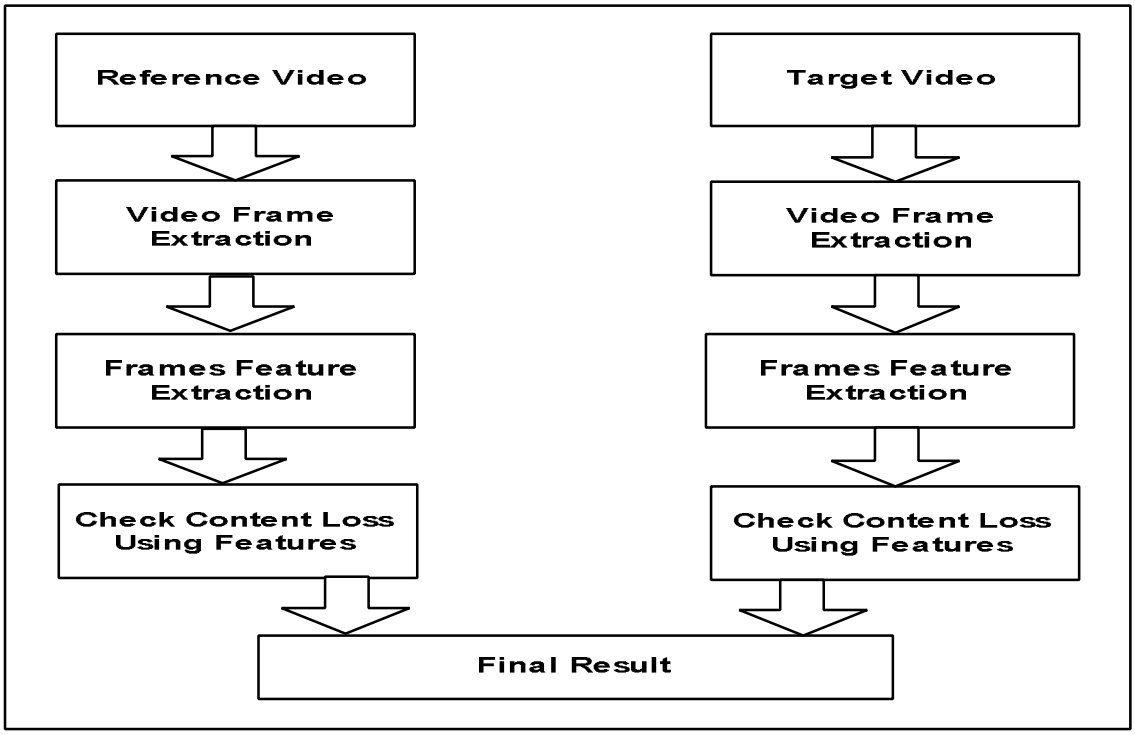

Fig: Proposed System Architecture

IV. ALGORITHM

Scale-Invariant Feature Transform (SIFT)

A SIFT key point is a image region with an orientation. It is described by a geometric frame of four parameters: the key point center coordinates x and y, its scale (the radius of the region), and its orientation (an angle expressed in radians). The SIFT detector uses as key points image structures which resemble “blobs”. By searching for blobs at multiple scales and positions, the SIFT detector is invariant (or, more accurately, covariant) to translation, rotations, and are scaling of the image.

The key point orientation is also determined from the local image appearance and is covariant to image rotations. Depending on the symmetry of the key point appearance, determining the orientation can be ambiguous. In this case,

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

the SIFT detectors returns a list of up to four possible orientations, constructing up to four frames (differing only by their orientation) for each detected image blob.

Steps:

- Initialize a SIFT filter object with **vl_sift_new ()**. The filter can be reused for multiple images of the same size (e.g. for an entire video sequence).
- For each octave in the scale space:
  - Compute the next octave of the DOG scale space using either **vl_sift_process_first_octave()** or **vl_sift_process_next_octave()** (stop processing if **VL_ERR_EOF** is returned).
  - Run the SIFT detector with **vl_sift_detect ()** to get the key points.
  - For each key point:
    - Use **vl_sift_calc_keypoint_orientations ()** to get the key point orientation(s).
    - For each orientation:
      - Use **vl_sift_calc_keypoint_descriptor ()** to get the key point descriptor.
- Delete the SIFT filter by **vl_sift_delete ()**.

To compute SIFT descriptors of custom key points, use **vl_sift_calc_raw_descriptor ()**.

V. RESULT AND DISCUSSION

In the experiments in this section, shows that the various techniques comparison on frames features extraction to find all the duplicated or forgery fake areas were created or not. SVD, LBP techniques were used in previous work for the video frames extraction. In our proposed system we are using SIFT descriptor for the video frames feature extraction. So this result shows that the proposed algorithm (SIFT descriptor) takes minimum time for frames feature extraction compared with existing techniques.

Graph:

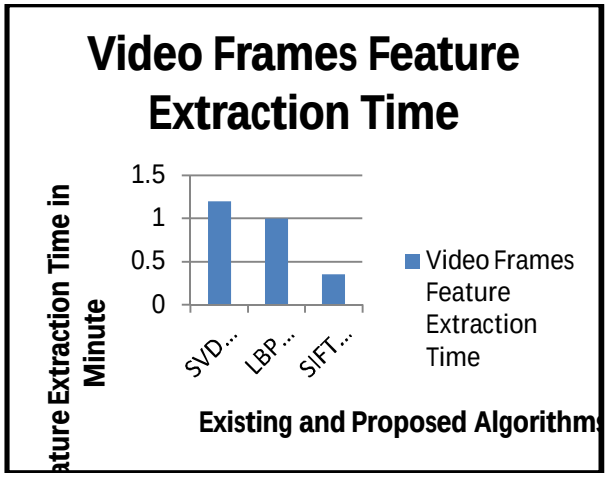

Fig: Feature Extraction Time Comparison Graph

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

Table: Feature Extraction Time Comparison

Existing and Proposed Techniques	Video Frames Feature Extraction Time (Minute)
SVD (Existing System)	1.2 M
LBP (Existing System)	1 M
SIFT (Proposed System)	0.35 M

VI. CONCLUSION

In this work we introduced a novel technique for unsupervised forensic analysis of video file containers. To achieve the differences in the video file content defined by different manufacturers, models and software processing. Proposed work will use SIFT descriptor technique for feature extraction. The proposed technique is shown to be able to automaticallydetect manipulations that are performed without videoencoding, which is an unprecedented achievement in videoforensics state of the art. Will proposed the first formal approach to perform integrity verification and difference identification and classification based on such features which is more and more approved by the forensic community as the appropriate way

REFERENCES

[1] D. Vazquez-Padin, M. Fontani, T. Bianchi, P. Comesa˜na, A. Piva, and M. Barni, “Detection of video double encoding with gop size estimation,” in IEEE 2012 International Workshop on Information Forensics and Security (WIFS). IEEE, 2012, pp. 151–156.
[2] A. Gironi, M. Fontani, T. Bianchi, A. Piva, and M. Barni, “A video forensic technique for detecting frame deletion and insertion,” in IEEE 2014 International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2014, pp. 6226–6230.
[3] L. Su, C. Li, Y. Lai, and J. Yang, “A fast forgery detection algorithm based on exponential fourier moments for video region duplication,” IEEE Transactions on Multimedia, 2017.
[4] T. Gloe, “Forensic analysis of ordered data structures on the example of jpeg files,” in IEEE International Workshop on 2012 Information Forensics and Security (WIFS),. IEEE, 2012, pp. 139–144.
[5] T. Shanableh, “Detection of frame deletion for digital video forensics,” Digital Investigation, 2013.
[6] He, Z., W. Lu, Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern Recognition 45(12), 4292-4299 (2012)
[7] G. Muammad, M.H. Al-Hammadi, M. Hussain, A. M. Mirza, and G. Bebis,” Copy Move Image Forgery Detection Method Using Steerable Pyramid Transform and Texture Descriptor” in Proc. EUROCON 2013. Image Processing and Analysis.
[8] Jaberi, M., Bebis, G., Hussain, M., Muhammad, G., Accurate and robust localization of duplicated region in copy-move image forgery, Machine Vision and Applications, 25(2), 451-475 (2014).
[9] Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab, “Copy Move Image Forgery Detection Using Hessian and Center Symmetric Local Binary Pattern”, 2015 IEEE Conference on Open Systems (ICOS), August 24-26, 2015, Melaka, Malaysia