DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5680

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

VIDEO FOREGERY DEDUCTION OF INTERFRAME DUPLICATION

Nandhini. R
Department of CSE
University College of Engineering,(BIT Campus)
Tiruchirapalli, India

Nasima Begum. M
Department of CSE
University College of Engineering,(BIT Campus)
Tiruchirapalli, India

Mrs.Blessy Selvam M.E.
Department of CSE
University College of Engineering,(BIT Campus)
Tiruchirapalli, India

Abstract: Video forgery detection aims to distinguish video forgeries from original videos. Video forgery detection in the form of features extraction from clustering the frames and matched with original videos. Scale Invariant Feature Transform (SIFT) are improved for detection of copy move attacks. Image keypoints are extracted and multi-dimensional feature vector named as SIFT descriptor is generated for each keypoint. Then, these keypoints are matched using distance among their descriptors. The experimental results show that our proposed algorithm has good at detection of copy move attacks. Total percentage of forged identify which frame to be forged and designed application as window based application with image processing techniques**.**

Keywords: Video forgery,Clustering, Feature extraction, SIFT algorithm, Keypoint descriptor.

I. INTRODUCTION

With the rapid development of multimedia technology and user-friendly editing softwares (e.g., Photoshop, Premiere by Adobe, and Mokey by Imagineer Systems), manipulating videos and changing their content is becoming a trivial task. For example, you can add or delete significant information, such as an object, from a video, without leaving any visible signs of such tampering. Sometimes, these manipulations are not innocent, involving for example tampering videos acquired in surveillance systems and used as evidence. Consequently, there is an increasing research interest in video forensics, which is used to authenticate the veracity and integrity of videos.

Using video-editing software to copy and paste specific existing contents from one region to another disjoint region in the same frame is one of the most common methods for video forgery. Fig. 1 shows an example of region duplication in a video downloaded from the Internet. In the figure, the top and bottom rows show the authentic sequences and their forged version, respectively. In the forged sequences, the cars are selected and duplicated, concealing the real information of the video.

Fig. 1. An example of video intra-frame region duplication: authentic (top) and tampered video (bottom)

2. RELATED WORK

Several researches have developed and implement the video forgery which detect the correlation between the original region and duplicate region J,Gauch.et.al[1] introduces an automated technique for locating previous unknown commercials by using continuous monitoring broadcast television signals.It will achieve more accuracy for identifying new commercials using repeated video sequence detection.M.Douze.et.al[2] INRIA-LEAR's video copy detection system approach applied to deciding whether the query video is a copy video which is obtained from indexed data set in not and the detection consumed less time.M.Kobayashi.et.al[3] this approach detect suspicious regions in video recorded from a static scene by noise characteristics. It will reduce a computational complexity X.Bo, W.Junwen.et.al [4] proposed a method to identifying image copy-move forgery detection based on SURF(Speed Up Robust Features)descriptors ,which are invariant to transformations. In this approach keypoint matching is done between two subsets of test image as shown in Fig;2. I.Amerini.et.al[5] proposed an SIFT based forensic method for copy-move attack detection and transformation recovery.It gives high reliability to estimate the geometric transformation parameters and also deals with multiple cloning. B.L.Shivakumar.et.al[6] proposed a method to determine if a particular image is authentic or not. It is used to detect copy-move forgery based on SURF,KD-Tree for multidimensional data matching .It will detect copy-move forgery with minimum false match for images with high resolution. Pravin Kakar.et al[7] introduce a noval technique based on transform invariant features from the MPEG-7 image signature tools It will exposing post processed copy-paste forgery through transform like scaling, rotation, flipping,lossy compression

noise addition and blurring invariant features.This algorithm gives high true positive rate to detect cloned regions and more accuracy in features matching.H.Yin.et al[8] is proposed an alogirthm that extract the feature points in current frame the tampered areas in the current frame are then searched. Which is implemented using spatio temporal algorithm learning and output gives detection results

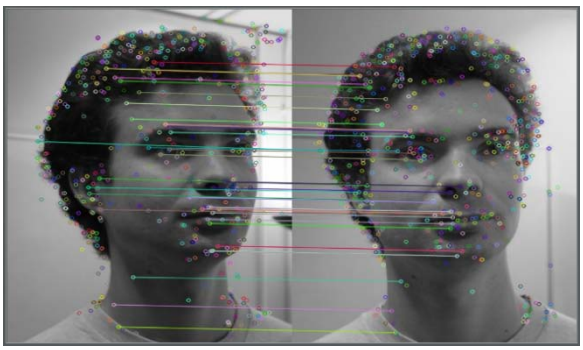


Fig. 2 An example for operations performed on region of copy area.

3. EXISTING SYSTEM

The eigenvector matrix of the video is populated by extracting the Tamura texture features of each frame, and their variants of the frames are compared to detect copy-move sequences. Using video-editing software to copy and paste specific existing contents from one region to another disjoint region. Histogram of Oriented Gradients (HOG) feature matching and video compression properties are used to detect the forged pixels in images.

Disadvantages of an Existing System

- 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

4. PROPOSED SYSTEM

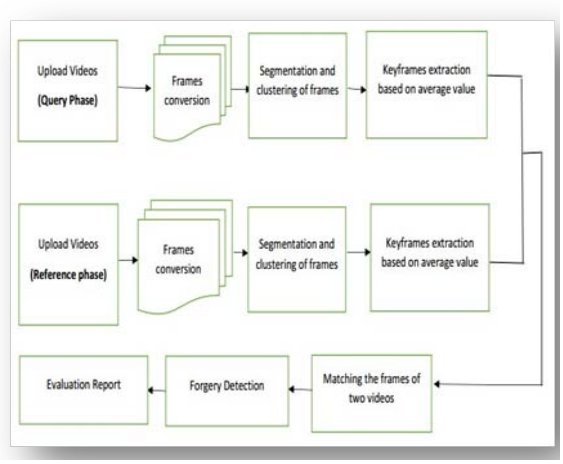
In this paper we propose to trace a query video snip in a video file or database.It held in detecting video copies for copyright protection and reduces storage redundancies.

Techniques

- Split a videos into a frames
- Features extraction
- Clustering technique and segmentation approach
- Extract the key frames using SIFT(Scale In-variant Feature Transform)
- Predict the forgery with matching original video

5. SYSTEM ARCHITECTURE

The below diagram represents the system architecture of our proposed system.Uploaded videos provides the videos from the database.It can be converted into frames by segmentation and clustered using keyframe extraction.Similarly the reference video is also converted into frames by segmentation and clustered using keyframe extraction.These two videos where applied by SIFT algorithm to predict forged from orginal. Finally, It provide the evaluation report of video forgery(percentage of video forged).



A. *Feature Vectors of Keyframes*

Keyframe extraction algorithms select a subset of the most informative frames from videos. Key frame extraction finds applications in several broad areas of video processing research such as video summarization, video indexing, and prints from video. In the proposed approach, we exploit image epitome to measure dissimilarity between frames of the input video. The dissimilarity scores are further analyzed using a keys to extract the desired number of key frames from the input video. A comparison of the results obtained by this method with the ground truth agreed by multiple judges clearly indicates the feasibility of the proposed approach.

Algorithm require

Input:
v: The input video stream
t_s:The size of threshold
t_o:The temporal object appearance threshold
t_d:The temporal detection threshold

Output:
k:The list of keyframe labels

for each frame f in v
/*Moving region extraction*/
Extract the set of moving regions R_f
for each element r in R_f
if size(r) c t_s
Remove r from R_f
else
Increment temporal-appearance(r)
/*inverted tracking*/
if temporal-appearance(r)>to
Set the cell(r) to 1 in MAM_f
/*keyframe detection*/
if is keyframe(MAM_f)
Compute keyframe label l_f
Increment temporal-count(l_f)
if temporal-count(l_f)>t_d
Push l_f onto k
$MAM_{f-1} \leftarrow M_f$

Clear M_f
end for

B.Clustering of Feature Vectors

Video contains huge amounts of data which needs to be organized and compressed in an efficient manner (e.g., one hundred hours of video contains about 10 million frames requiring about 7:5TeraBytes of data. During the parsing process, video clips are segmented into scenes. Scenes are further segmented into shots which are each represented in terms of a few keyframes. A shot is defined as a sequence of frames that represent a continuous action in time and space. It is thus desirable to represent each shot with a minimal set of keyframes that capture the semantic content of the shot. Automatic schemes for shot detection and subsequent keyframe extraction have been reported in the literature. However, a video clip may contain a number of shots. For example, Yeung et al. Report upto 300 shots in a 15 minute clip of Terminator 2 and a 30 minute clip of sitcom "Frasier". Assuming an average of 3 keyframes per shot, close to 1; 000 keyframes would be required to represent these video clips. In a digital library with over 100 hours of digitized video, about 100; 000 keyframes may be extracted. Indexing and clustering of these keyframes would then allow the users to jump across video clips to location of their interest. Our goal is to develop a scheme for automatic classification of keyframes (and hence the corresponding shots) into various categories based on their content. Once the shots have been clustered based on the keyframes, it would be possible to represent the shots at a higher level of abstraction (such as city shots, landscapes, etc.) that allows the user to get an idea of the contents of the shots without actually looking at the frames contained in the shots.

C.SIFT(Scale In-variant Feature Transform)

Detect an interesting patch with an interest operator. Patches are translation invariant.Determine its dominant orientation.Rotate the patch so that the dominant orientation points upward. This makes the patches rotation invariant.Do this at multiple scales, converting them all to one scale through sampling.Convert to illumination "invariant" form.

Over all process of SIFT:

- **Scale-Space Extrema Detection:**
  Search over multiple scales and image locations.
- **Keypoint Localization:**
  Fit a model to determine location and scale.Select keypoints based on a measure of stability.
- **Orientation Assignment:**
  Compute best orientations for each keypoint region.
- **Keypoint Description:**
  Use local image gradients at selected scale and rotation to describe each keypoint region.

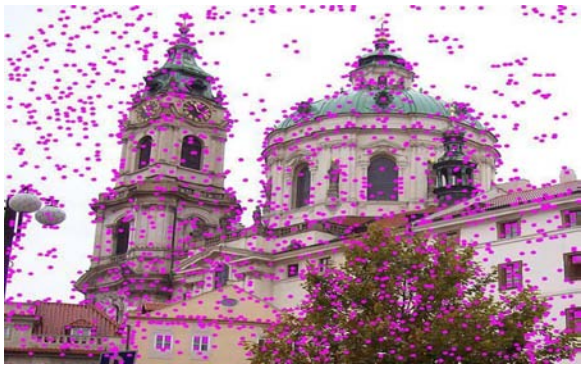


Fig. 3 Detection of keypoints using SIFT algorithm

6. CONCLUSION

In this paper, we present a Video forgery detection based on feature extraction for the detection of inter-frame region duplication. Our algorithm first extracts keypoints from each block in the current frame, and performs a segmentation and clustering to find potential matching pairs. Then key frame extraction method is designed to eliminate falsely matched pairs and locate the altered regions in the current frame. Finally, SIFT algorithm is used to track the tampered regions in the subsequent frames. The experimental results show that our proposed algorithm has higher detection accuracy and computational efficiency than those of previous algorithms.
In future research, we will extend our method to detect more challenging types of video forgery.

REFERENCES

[1] J. Gauch and A. Shivadas, "Identification of new commercials using repeated video sequence detection," in Proc. IEEE Int. Conf. Image Processing, vol. 3,2006.
[2] M. Douze, A. Gaidon, H. Jegou, M. Marszalek, and C. Schmid "INRIA-LEARs video copy detection system," in Proc. TRECVID Workshop, 2008.
[3] M. Kobayashi, T. Okabe, and Y. Sato, "Detecting Video Forgeries Based on Noise Characteristics," in Advances in Image and Video Technology, Third Pacific Rim Symposium,PSIVT 2009, Tokyo, Japan, pp. 306-317, 2009.
[4] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, pp. 889-892,2010.
[5] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, vol. 6, pp. 1099-1110, 2011.
[6] B. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," IJCSI International Journal of Computer Science Issues, vol. 8, 2011.
[7] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," Information Forensics and Security, IEEE Transactions on, vol. 7, pp. 1018-1028, 2012.
[8] H. Yin, W. Hui, H. Li, C. Lin, and W. Zhu "A Novel Large-Scale Digital Forensics Service Platform for Internet Videos," IEEE Transactions on Multimedia, vol. 14, pp. 178-186, 2012.