Detection and Localization of Video Copy-Move Forgery in Temporal and Spatial Domain

Mili Rosline Mathews, Sreelekha Sreedharan

Abstract— Digital videos are widely used and accessed nowadays. Moreover several video editing softwares are also available. Forgeries done within a single video cannot be recognized easily. The signs of forgery are very low in such cases. So the credibility of a video clip in the court as a proof is crucial for legal applications. Different types of video forgeries exist. Copy-move forgery is one of the most common type of video forgery. Our approach is detection and localization of forgery in temporal and spatial domain. The forgeries which can be done within a single video are considered for detection of forgery. For the detection of temporal copy-move forgery the structural similarity between the frames of a video is used. The difference of pixels between adjacent frames is used for identifying the spatially forged region in each frame. We propose an effective system to detect the copy-move forgery in videos.

Index Terms— Copy-move forgery, Difference operation, Structural similarity index measure, Video forgery.

I. INTRODUCTION

A large variety of digital multimedia devices and video editing tools are easily available and accessible today. It is becoming easy to alter the contents of the video. So images and videos cannot be considered as a proof or evidence for legal applications. In this manner digital video forensics has become an important research issue. Video forensics can be classified into active forensics and passive forensics. Some pre-embedded specific information which could not be perceived in the video is needed for active forensics. Digital watermarks and digital signatures are used in active forensics. In active forensics, one can determine whether the video is tampered or not by detecting the integrity of the information. In passive forensics, there is no requirement on specific information. It uses some inherent properties of videos. Video forgeries are of different types. One of the most common type of video forgery is Copy-move forgery. Spatial tampering and temporal tampering exist in videos. This can be categorized as intra and inter frame techniques. In intra frame copy-move operation a portion of the frame itself is replicated. It is used to hide or replicate some objects. In inter frame copy-move operation some frames are replaced with a copy of another frames. The purpose is to hide something that entered the scene in the original video. Several techniques for detecting forgeries in video are in literature. A method based on double compression of MPEG videos [1] is used to detect video forgery. The algorithm is specifically for frame deletion forgery. The techniques used exploit the fact that static and temporal artifacts are introduced as a result of double MPEG compression of a video sequence. It is unable to find the tempering area and the number of frames deleted. It is sensitive to noise and the change of Group of Pictures (GOP). Double quantization can introduce statistical artifacts. It can be quantified, measured, and used to detect tampering [2]. The limitation of this technique is that it is only effective when the second compression quality is higher than the first compression quality. A method for detecting duplication is introduced in [3]. Correlation coefficient is used as a measure of similarity. Computational cost of the algorithm is the drawback. A passive scheme to achieve frame duplication detection for video is proposed in [4]. The proposed scheme is a coarse-to-fine approach and composed of candidate clip selection, spatial correlation calculation, and frame duplication classification. A method based on discontinuity in the optical flow variation sequence [5] can be used for detecting forgeries in videos. An algorithm based on optical flow consistency [6] can be used for inter frame forgery detection.

II. FORGERY DETECTION

Video forgeries that exist within a single video are of great importance since it is not easily recognizable. Among different types of forgeries copy-move has high significance. Two types of copy-move forgery are temporal or inter-frame copy-move forgery and spatial or intra-frame copy-move tampering. In inter-frame copy-move operation a group of frames is copied into another location whereas in intra-frame copy move operation a region in a frame is copied to another frame or the frame itself.

A. Temporal Copy-move Forgery Detection

The temporal copy-move forgery can be detected in videos based on the Mean Structural Similarity(MSSIM) between the frames or images [7]. The input video is converted to frames and each frame is converted to gray scale images. Then these frames are grouped into overlapping blocks or sub-sequences. Each block is taken as a reference block and the similarity reference block and subsequent blocks are measured. The value of similarity measurement is compared against the threshold. If the MSSIM values between all the corresponding frames in reference block and subsequent block are greater than the threshold value, which is set by the user, the block is detected as copied. The whole process shown in Fig.1 is used for detection of temporal copy-move forgery.

Revised Version Manuscript Received on June 09, 2015.

Asst. Prof. Mili Rosline Mathews, Department of Electronics, College of Engineering, Karunagapally, Kollam, India.

Sreelekha Sreedharan, PG Scholar , Department of Electronics, College of Engineering, Karunagpally, India.

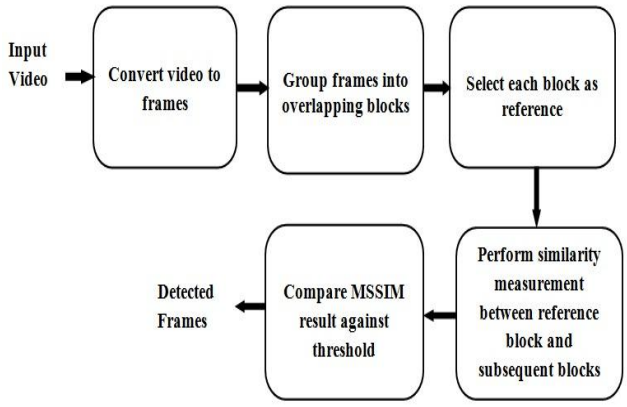

Fig. 1: Block diagram for temporal copy-move detection

Structural Similarity (SSIM) can be extended to evaluate the similarity between two frames. Video sequence can also be considered as a flow of successive images in the temporal domain. So to measure the similarity between two frames of a video Mean Structural Similarity (MSSIM) can be used. Higher the value of MSSIM between two images indicates better similarity between these images. The SSIM metric measures the similarity with three statistical components, which are luminance comparison, contrast comparison, and structural comparison. Let Y be the distorted image of X, for any two pixels x in X and y in Y, the SSIM metric is as follows,

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^{\,2} + \mu_y^{\,2} + C_1)(\sigma_x^{\,2} + \sigma_y^{\,2} + C_2)} \quad (1)$$

where μ_x and μ_y are the means of the local windows with a size of 11×11centered at x and y respectively. σ_x and σ_y are the standard variance, σ_{xy} is the covariance of the two windows. C_1 and C_2 are small constants. To evaluate the overall image quality, Mean Structural Similarity (MSSIM) is used.

$$MSSIM(x,y) = \frac{1}{M}\sum_{i=1}^{M} SSIM(x,y) \quad (2)$$

where M is the number of local windows in the image. To evaluate the video sequence for finding whether copy-move operation is done or not, MSSIM can be used. For this first extract the frames in that video. Then convert each color frame into gray scale and compute MSSIM value for each pairs of frames. The MSSIM value between two frames can be used for detecting duplicated frames. This can be done by setting a threshold value for MSSIM value. This can be done by evaluating all the MSSIM values between the consecutive frames in a video and determine an upper value as threshold. Because the maximum similarity occurs between adjacent frames in a normal video. The number of frames or images is an important parameter. Let the number of frames in a full length video be N. Each frame in the video is extracted and converted from color to gray scale. Then a full length video sequence is divided into short overlapping sub-sequences each of length M as shown in Fig.2. For the measurement of temporal similarity between frames of a video, the temporal similarity between short overlapping sub-sequences is used. First sub-sequence is obtained by taking first M frames in the video and the second sub-sequence is obtained by sliding one frame to the right. In the Fig.2 the number of first frame in the sub-sequence is used as the sub-sequence number. Each sub-sequence is taken as a reference sequence and the similarity between this reference sequence and all other sub-sequences in the evaluation sequence excluding the reference sequence is found. If two sub-sequences show replication relationship it means that exceed the threshold value of MSSIM for the M time similarity measurement. When taking a reference sequence and a sub-sequence in the evaluation sequence to find the similarity measurement between them, the MSSIM value between the M frames should be greater than the threshold for detecting the copy-move operation.

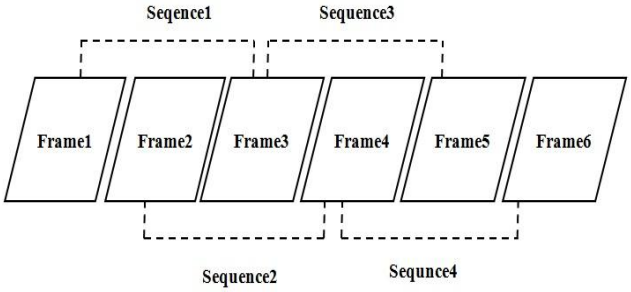

Fig. 2: Example for dividing the frames into sub-sequencs

B. Spatial Copy-move Forgery Detection

In spatial copy-move forgery a group of pixels are copied from one frame to another. The difference of pixels between consecutive frames does not exceed a threshold value for a group of pixels or a region in normal videos. But in spatially copy-move tampered videos the difference between the tampered frame and normal frame exceeds certain values. The difference image has some peaks in pixel values corresponding to the spatially forged regions in the frame.

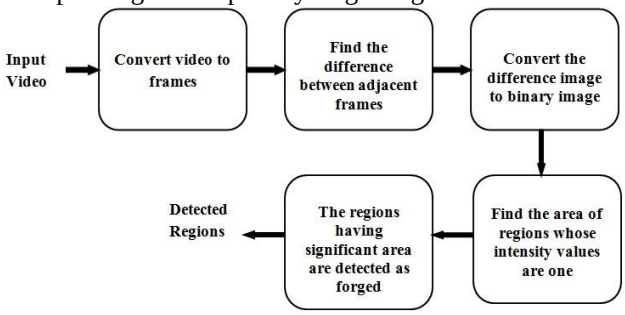

Fig. 3: Block diagram for spatial copy-move detection

The whole process for detecting spatial copy-move forgery is shown in Fig.3. The video is converted to frames. Based on the threshold the difference image is converted into binary image and all the one valued regions with a minimum size 3×3 is considered for further processing. This eliminates false positives and also contribution due to noise.

III. RESULTS AND DISCUSSION

The forgery detection algorithm for temporal and spatial copy-move forgery was simulated on a set of surveillance videos. The algorithm proves to be efficient and takes less time compared to the existing ones.

A. Temporal tampering

For the detection of temporal copy-move tampering the video is converted to group of frames or sub-sequences. We consider copying a group of frames as temporal copy-move tampering instead of a single frame. Each sub-sequence is compared with all other sub-sequences to find whether forgery exist or not. Each sub-sequence is numbered. The pair of sub-sequences involving in forgery are displayed. A number of videos are checked for detecting copy-move operation. For all the test videos the copy-move forgery is detected correctly. It can localize the exact position of sub-sequence that was copied. In a test video the frames 1, 2 and 3 are copied to the frame locations 24, 25 and 26. The algorithm localizes these groups of frames and result is shown in Fig.4 and Fig.5.

Fig. 4: Frames 1,2 and 3 extracted from the test video

Fig. 5: Frames 24,25 and 26 extracted from the test video

Similarly the frames 4,5 and 6 are copied to the frame locations 12,13 and 14. The algorithm localize these group of frames and result is shown in Fig.6 and Fig.7.

Fig. 6: Frames 4,5 and 6 extracted from the test video

Fig. 7: Frames 12, 13 and 14 extracted from the test video

B. Spatial tampering

The spatial copy-move tampering within the video is detected for surveillance videos. The difference between adjacent frames is used to detect tampering. These differences are converted to binary images and then tampered region is detected and marked. The test videos are tested for detecting the spatially tampered regions. The tampered regions are marked correctly as shown in Fig.8(c).

(a) The original frame **(b) The tampered frame**

(c) Region detected by using the algorithm

Fig. 8: Results showing spatial forgery detection

IV. CONCLUSION

This paper proposes a new algorithm for detecting copy-move forgery in videos for both spatial and temporal tampering. On analysis of the simulation results, the method used in the algorithm is able to detect and localize the copied frames and copied regions within video correctly. It is used to detect the copied frames or regions within a single video. The localization of tampered frames or regions is also possible.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

ACKNOWLEDGMENT

We would like to thank all those who have guided and supported throughout the completion of this paper.

REFERENCES

1. Wang W, Farid H, ``Exposing digital forgeries in video by detecting double MPEG compression," In: Proceedings of the 8th workshop on multimedia and security, doi: 10.1145/1161366.1161375, 2006.
2. Wang W, Farid H, ``Exposing digital forgeries in video by detecting double quantization," In: Proceedings of the 11th ACM workshop on multimedia and security. doi:10.1145/1597817.1597826, 2009.
3. Weihong W, Hany F, ``Exposing digital forgeries in video by detecting duplication," In:Proceedings of the 9th workshop on multimedia and security. doi: 10.1145/1288869.1288876, 2007.
4. Lin G-S, Chang J-F, ``Detection of frame duplication forgery in videos based on spatial and temporal analysis," Int J Pattern Recognit Artif Intell 26(7):1–18, 2012.
5. Wan Wang, Xinghao Jiang, Shilin Wang, ``Identifying Video Forgery Process Using Optical Flow," IWDW, pp. 244–257, 2013.
6. Qi Wang, Zhaohong Li, Zhenzhen Zhang, Qinglong Ma, ``Video Inter-frame Forgery Identification Based on Optical Flow Consistency," Sensors and Transducers, Vol. 166, Issue 3, pp. 229-234., 2014.
7. Fugui Li. Tianqiang Huang, ``video copy-move forgery detection and localization based on structural similarity," Proceedings of the 3rd International Conference on Multimedia Technology, 2013.
8. Simone Milani, Marco Fontani, Paolo Bestagini, Mauro Barni, Alessandro Piva, Marco Tagliasacchi and Stefano Tubaro, ``An overview on video forensics," APSIPA TransSignal Inf Process.1:e2. doi:10.1017/ATSIP.2012.2, 2012.
9. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP, ``Image quality assessment: from error visibility to structural similarity" IEEE Trans Image Process 13(4):600–612,2004.