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 7, July 2019

Identification and Localization of Duplicated frames in Tampered Video

Rati R. Ghaisas[1], Sanjeevani K. Shah[2]

PG Student, Dept. of E & TC Engineering, STES'S Smt. Kashibai Navale College of Engineering, Pune, India[1]

HOD E&TC, Dept. of E & TC Engineering, STES'S Smt. Kashibai Navale College of Engineering, Pune, India[2]

ABSTRACT:With the arrival of exceptional digital video cameras and complex video modifying software. It is miles becoming less difficult to tamper with virtual movies. A not unusual form of manipulation is to clone or replica frames or parts of a body to put off human beings or objects from a video. To search for this interfering form, we describe computationally efficient approach. After detection of frame duplication, localization of frame collection has additionally been achieved. Detection in addition to localization of forgery are determined better than the other strategies.

KEYWORDS: Frame duplication, Detection, Localization, Correlation, Sub blocking, RMSE

I. INTRODUCTION

In 20th century, the digital world has a long way to go. Every person is immersed in the sea of digital multimedia. Thousands of pictures and videos of knowledgeable or strangers come regularly in their daily lives. These things are established somewhere in the human mind. Images and videos are a powerful channel to express information as well as emotional impact. That is why, depending on the color, texture, size and the moving image or video of the viewer, what he/she feels. Due to the fact that some major frauds (colors, textures and movements) sometimes leave a long-standing emotional imprint to the viewers, the truth comes in truth, but the harm has already been done. This leads to serious consequences, depression increases and dissatisfaction occurs in many daily life applications andinteractions.

With the high quality digital video cameras and cutting- edge video editing software, it is easy to tamper with digital videos. A common type of tampering is to duplicate or duplicate parts of a frame or frame to remove people or objects from the video. In this paper, we describe a computationally effective technique to look at this type of interfering.

Objective of frame duplication are as follows:

1. To hide the contents of the actual event

   and/or

2. Repeat any event so that the audience will mislead visible.

To hide the sequence, a group of frames must be replaced with the second group of frames from the same video on priority. Whenever you want to recreate an event, group of frames with the desired event is included elsewhere in the same video order. However, in order to search for both cases, the group of frames is duplicated from the preference to the same video.

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 7, July 2019

II. RELATED WORK

Different methods for detection and localization of duplicated frames are presented below.

Using detection method, digital tampering exposed [1], in which they have got used very apparent method to examine correlation of the two consecutive frames. To overcome with complexity problem, they have used set of frames to conquer complexity. Effects are appropriate up to 90% of accuracy.

With the help of noise characteristics, detection of video forgery [2], proposed used consistency of noise degree characteristics in each frames is sufficient to distinguish among attacked and original vicinity. However, this approach is good only for static digital camera and overall performance substantially decreases because the compression is executed at the videos. Consequently this technique is not appropriate to find such forgeries.

Gaussian mixture model (GMM) [3], which is used however nevertheless difficulty exists with accuracy and complexity. In spatial and temporal analyses [4], histogram difference is used and this reduces time complexity and located extra correct than previoustechnique.

Local tampering detection [5], proposed a technique to identify a spatio-tamporal forgeries with the aid of analyzing left footprints. However, effects became now not that distinguished on all kind of videos.

Using sensor's pattern noise [6], proposed a method to stumble on whole frame duplication and item insertion. Supplied approach also claim to be a few stage of invariance of MPEGcompression.

Using sub-block based feature [7], nine functions to suit suspected frames those nine function also are considered in this paper however the sub blocking technique ischanged.

Numerous demanding situations are encountered whilst detecting above duplication kind of forgery. Being very high-priced, trivial methods have restricted reach because of the involved computational price.

III. PROPOSED METHODOLOGY

In case of body duplication sort of forgery, targeted video is first divided into frame with the aid of frames. When you consider that our objective is to hit upon comparable frames for this reason some appropriate frame matching set of rules wishes to be implemented. The technique which is used for stated purpose is mentioned as under:

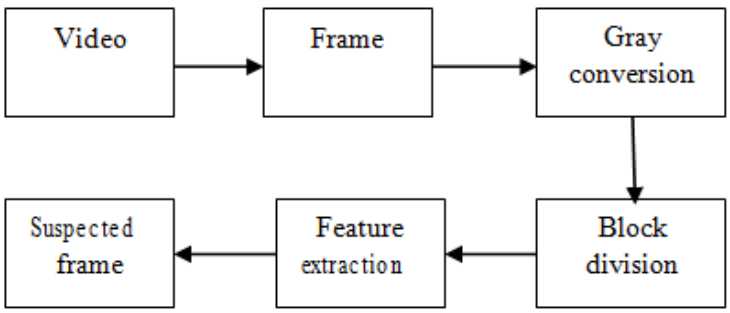

Fig. 1: Block Diagram

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 7, July 2019

A. *Conversion of video series in frames and then to the gray scale*

Video collection is a set of pictures called as frames. Frames of centered videos are extracted. Every frame have three different channels R (Red), G (Green) and B (Blue). To reduce computation, RGB frames are converted into their equal gray scale frames the usage of equation 1 conversion method.

$$I_t(x,y) = 0.2989 \times R_t(x,y) + 0.5870 \times G_t(x,y) + 0.1140 \times B_t(x,y)$$

Where,

I_t = particular frame at a time t

$R_t(x,y)$, $G_t(x,y)$, $B_t(x,y)$ = intensity values at location (x,y)

B. *Detection of Suspected Frame Duplication*

To extract similar frames, correlation among frames are computed. All frames with high correlation taken into consideration to be 'key frames' and kept as suspected frames. For N variety of frames, N^2 computation are required for assessment of each frame with each different. Trivial technique of exact matching of frames requires excessive amount of computation and hence is appeared as inefficient for larger video length. Forgery is detected at Key frames.

C. *Sub Blocking, Feature Selection and Extraction*

After you have key frames, the crucial part of matching set of rules is to select appropriate capabilities. Various researchers have used correlation as an identical characteristics. Afterwards, we divided every frame in four part as shown in fig. 2. This sort of sub blocking allowed generally pixel contribution in characteristic making.

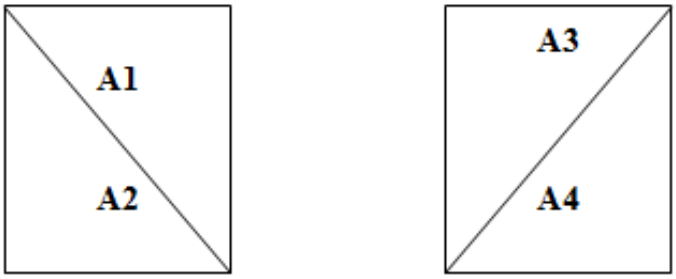

Fig. 2: Single frame division

D. *Suspected Frame Selection*

After getting all function vectors for N quantity of frames, root mean square error is calculated between each feature vectors of two consecutive frames I and j. Suspected frames should be considered as pairs of frames with RMSE zero or almost zero. Minimum distance class techniques is one of the strategies used for classifying the pictures. The minimum distance is initialized to be the high value. The Euclidean distance from every unknown pixel to the suggest vector for every magnificence iscalculated.

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 7, July 2019

E. *Localization of Forgery*

After retrieval of the duplicated clips effectively, it is vital to locate the original and duplicated frames inside the video series that allows you to enable anyone get convinced that frame duplication type of forgery has honestly been crafted and the result found is sequence of frames which is much like another series of frames. As a result if collection starting from i^{th} body is much like j^{th} body, then for each frames correlation with the previous frame is tested. Whichever of these two frames show higher correlation with its previous body, such clip containing frames are seemed as the case of duplication.

IV. EXPERIMENTAL RESULTS

To take a look at the result of the proposed technique, range of experiments had beenexecuted.

Fig. 3: Snapshot of Video

In this paper to detect duplication of frames, we take one of the video which is in Avi format of 1 second time length. It is of 515 kbps data rate and frame rate is 30 frame/second with resolution of 454 x 232pixel.

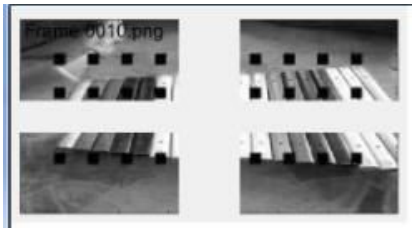

Fig. 4: Frames division of Suspected frame

First, this video is converted in frames and this color frames is converted into gray scale. With the help of correlation of two consecutive frames in static scene, the suspected frame is selected at frame 10.

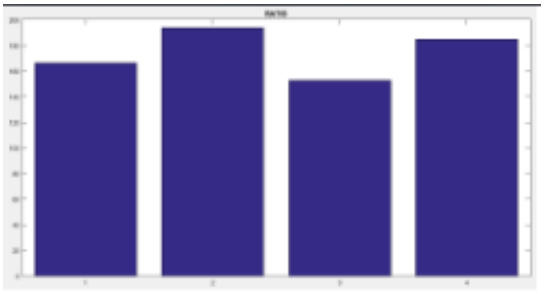

Fig. 5: Bar graph of frame 10

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 7, July 2019

After this for further processing the suspected frame is divided into four parts. After that we get bar graph for frame 10. From this bar graph, we discovered duplicated frames. After this, we find out the location of duplicated frames.

V. CONCLUSION

We have proposed sub blocking set of rules to discover body duplication on the basis of similarity analysis among frames. We extracted symmetrical capabilities of every frames and applied Euclidean distance technique. Subsequently suspected duplication is located such key frames located are then in addition processed in 2nd step to verify the duplication in movies.

REFERENCES

[1] Wang, W., Farid, H.: Exposing digital forgeries in video by detecting duplication. In: Proceedings of ACM 9th Workshop on Multimedia and Security, pp. 35–42(2007).
[2] Kobayashi, M., Okabe, T., Sato, Y.: Detecting video forgeries based on noise characteristics. In: Pacific-Rim Symposium on Image and Video technology, pp. 306-317 (2009).
[3] Hsu, C. –C., Hung, T.-Y., Lin, C.-W., Hsu, C.-T.: Video forgery detection using correlation of noise residue. In: Proceedings of the IEEE 10th Workshop on Multimedia SignalProcessing, pp. 170-174 (2008)
[4] Lin, G.S., Chang, J.F., Chuang, C.H.: Detecting frame duplication based on spatial and temporal analyses. In: Proceedings of the IEEE Conference on Computer Science and Education, pp. 1396–1399 (2011).
[5] Bestagini, P., Milani, S., Tagliasacchi, M., Tubaro, S.: Local tampering detection in video sequences. In: IEEE International Workshop on Multimedia Signal Processing, pp. 488–493(2013).
[6] Mondaini, N., Caldelli, R., Piva, A., Barni, M., Cappellini, V.: Detection of malevolent changes in digital video for forensic applications. In: Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505(2007).
[7] Singh, V.K., Pant, P., Tripathi, R.C.: Detection of frame duplication type of forgery in digital video using sub-block based features. In: James, J., Breitinger, F. (eds.) Digital Forensics and Cyber Crime. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 157. Springer, Cham(2015).