IJCERT

International Journal of Computer Engineering in Research Trends

Multidisciplinary, Open Access, Peer-Reviewed and fully refereed

Research Paper Volume-6, Issue-12, 2019 Regular Edition E-ISSN: 2349-7084

Copy Create Video Forgery Detection Techniques Using Frame Correlation Difference by Referring SVM Classifier

Govindraj Chittapur*[1], S. Murali[2] , Basavaraj S. Anami [3]

[1] Department of Computer Applications, Basaveshwar Engineering College, Bagalkot India*
[2] Department of Computer Science and Engineering, Maharaja Institute of Technology, Mysore, India
[3] Department of Computer Science and Engineering, KLE Institue of Technology, Hubli, India

e-mail: gbcmc@becbgk.edu, murali@mit.ac.in, anami_bassu@hotmail.com

**Corresponding Author: gbchittapur@gmail.com,*

Available online at: http://www.ijcert.org

Received: 06/01/2020, Revised: 12/01/2020, Accepted: 16/01/2020, Published: 20/01/2020

Abstract:- Video Forensic is a new research avenue in computer forensics. Usually, passive forgery detection techniques have much more import then active forgery techniques to resolve the cost and efficiency of computational video. Forgery detection methods available in copy-move and copy-paste type of forgery. here we propose an algorithm for copy create, which is a combination of copy-move and copy-paste region of video forgery by using frame correlation differences between sets of I-frame in the forged video by using SVM Classifier. We are successful in authenticating the tested video is original or forgery at the same time it returns good result identifying the different I-frame sequence in given forgery videos. Forgery video inputs are customized by referring standard available data set like SULPA, REWIND, VTD, and CVIP.

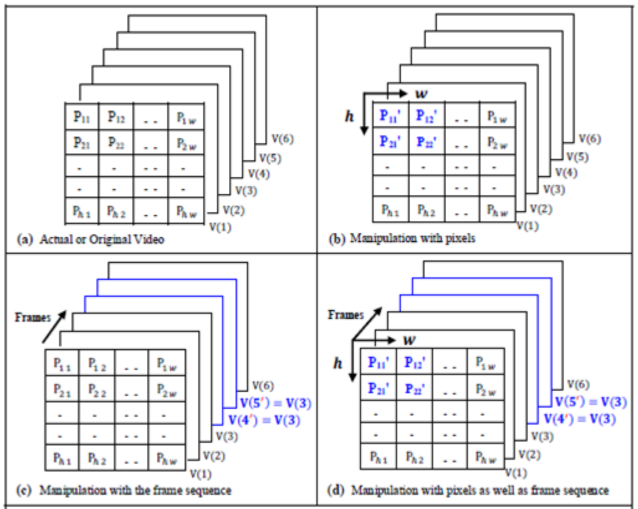
Keywords: Video Forensic, copy-move, copy-paste, copy-create, frame correlation, I-frame, and SVM

1. Introduction

With the widespread availability of advanced and affordable digital video cameras and the prevalence of video sharing sites such as Instagram, YouTube, Google, Ixquick and Bing, and so forth. Digital videos are playing a more critical role in our daily life. Since digital videos manipulated, authenticity cannot be grant immediately. While it is undoubtedly true that tampering with a digital video is more time consuming and challenging than tampering with a single picture. Advanced digital video editing software made more accessible to tamper videos. Not every video forgery is equally consequential; the tampering with footage of a pop star may matter less than the alteration of footage of a crime in advance. However, the alterability of video undermines our common-sense assumptions about its accuracy and reliability as a representation of reality. As digital video editing techniques become more and more advanced, it is ever more necessary to develop instruments for detecting video forgery. Depending upon the domain in which manipulation is performed, there can be following types of video tampering.

1.1 Video Tempering Domain: There as four tempering domain as shown in the figure below: These can be considered as
1.1(a) tampering in the spatial domain
1.1 (b) Tampering in the temporal domain
1.1 (c) Tampering spatiotemporal domains,

https://doi.org/10.22362/ijcert/2019/v6/i12/v6i1201



(a) Actual or Original Video

(b) Manipulation with pixels

(c) Manipulation with the frame sequence

(d) Manipulation with pixels as well as frame sequence

An example of **(a)** Actual video **(b)** Spatially tampered video **(c)** Temporally tampered video and **(d)** Spatio-temporal tampered video. Where $V(i)$ represents the i^{th} frame and P_{ij} is the pixel intensity. $V(i')$ is the manipulated i^{th} frame and $P_{ij'}$ is the manipulated pixel intensity.

Fig 1.1 Video Tempering Domain

A forger can alter the source of videos spatially by manipulating pixels within a video frame or across the video frames, Figure 1.1(b) presents a spatially tampered video created from the actual footage of Figure 1.1 (a) Further, as presented in Figure 1.1(c), a forger can tamper source videos by disquieting the frame. Sequence through structures replacement frame adding, and by the A removal of video frames and thus creates temporally tampered sequence videos. Lastly, referring Figure 1.1 (d), a forger can tamper videos in a combination of both spatial and Temporal domain (i.e., spatiotemporal tampering) by altering pixels within a video frame or across the video frames (i.e., a set of adjacent structures) as well as disturb the frame sequence and thus create spatiotemporally tampered videos.

Over the last five years, significant contributions have been made for the detection of spatial video Tampering, whereas relatively little contributions in temporal tampering. Thus, our proposed Frame Correlation Coefficient algorithm aims to detect the temporal tampering (i.e., tampering with frame sequence) in temporally or spatiotemporally tampered videos.

Apply easily to video forensics. The temporal association between video frames to considered minimizing the complexity of video forensics. Thus we propose copy create video forgery detection techniques using frame correlation difference by SVM classifier.

2. Related Work

From the literature survey, it revealed that significant contributions identified on video forgery detection, and researchers have developed and proposed different video forensic approaches for video forgery detection using active and passive strategies a few prominent as described in the following section:

Copy-Move is the majority type of video forgery. Many researchers focus on clone based forgery detection [1] coarse detection using optical flow[2], frame duplication[3,6,8,9,10], Frame deletion[6] and region duplication[4,5] and commonly different statistical approaches such as mean frame comparison techniques [11]normalized cross-correlation factor[12], In similarity to the mentioned copy-move forensics approaches, video tamper detection is a difficult task. If we use the above forensics algorithms to identify video tampering, the computational cost is offensive. As a result,
the methods for photo forensics cannot be

3. Methodology

3.1 Data Set and Design Issues:

We created a dataset from standard data set supported for copy create video forgery using SULPA[3], REWIND[4], CVIP[5], and YTD[6] dataset supported for copy-move and copy-paste tampering operations.

A. Data Set Design:

Here we design and test our proposed work with the following standard video forensic dataset:

❖ SULFA [3]: contains unique as well as fake video files parsimoniously available through the University of Surrey's website. There are approximately 150 videos collected from different camera sources, which are Canon SX220, Nikon S3000, and Fujifilm S2800HD. Every video is about 10 seconds long, with a resolution of 320x240 and thirty frames per second. All videos have been considering both temporal and spatial video features.

❖ REWIND[4]: this dataset combination consists of 20 videos used in SULFA: 10 unique and 10 fake ones. Each track has a motion of 320x240 pixels, and a frame-rate of 30 fps. Unique sequences recorded using a low-end device. Thus they have all been compacted at the origin fake frames have been saved as an uncompressed format (RV24, 24 bit RGB). To consistent all the frame to the same standard, they have all converted into the uncompressed format to standard YUV (4:2:0) format file,

❖ CVIP[5] This Dataset includes 160 fake videos, from 6 different original videos. Fake videos are created by selecting an object in a frame of a video and tracking the object for a definite number of sequential frames. The copied object cloned into another part of the same video, after possible fundamental video transformations. And

- YTD[6]: The VTD, focused on video tampering detection on videos are composed of the YouTube channel, is composed of 33 videos, 16-s long, at 30 fps within high definition standard resolution. The original dataset divided into different segments containing unaltered videos, one with videos created with different copy moves and copy-paste operation. For manipulative and testing, From the above mentioned standard dataset, we use to create customized video dataset for testing our proposed algorithm be referring temporal tempering video transformations.

B. Proposed Algorithm and Framework

The indispensable idea of our method is that differences of correlation coefficients of gray values of original sequences are consistent, while disagreements of inter-frame forgeries have abnormal points. We first calculate the differences of correlation coefficients of gray values between sequential frames of videos and then use Support Vector Machine (SVM) to classify original videos and variant inter-frame forgeries.

3.1 Proposed Algorithm for implementing Frame Consistency Variance:

1. Convert video into a group of pictures (frameset)

2. Apply the image frame Transform technique to convert RGB colour image frame into a gray image using RGB to YUV mode with the formulae

$Y_{trani} = 0.2989\ _{Red} + 0.5870_{Green} + 0.1140\ _{Blue.}$

3. Apply computation to the inter-frame correlation coefficient between adjacent frames using the correlation coefficient

4. Apply computation to the difference between correlation coefficients of sequential contiguous frames

5. Use of the Chebyshev inequality to find out abnormal points that indicate where the tampered frames are present.

Digital video forgeries detection based on content continuity is efficient. Based on this method, we can detect which frames tampered in a video. However, cannot identify whether the same source of the video has tampered a video, look forward to attain whether tested video is tampered and identified the correlation difference between conjugative forged frame sequences.

3.2 Framework for SVM Classifier using the Correlation coefficient

The Proposed framework for identifying the forgery sequences can be extracted by considering the forged video from standard video gallery by executing the steps as shown in below figure 3.2

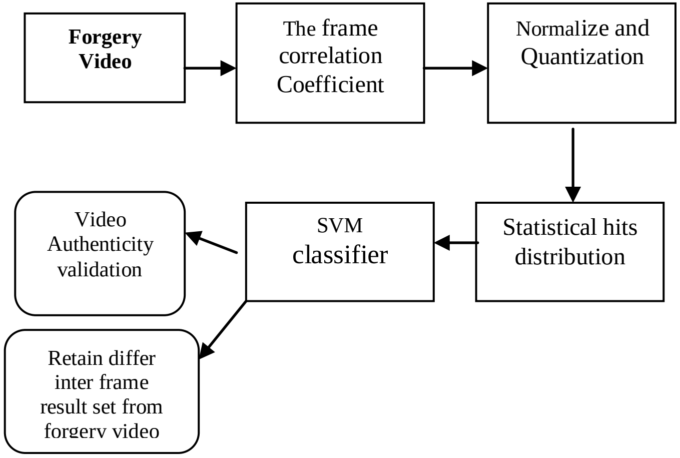

Forgery Video
The frame correlation Coefficient
Normalize and Quantization
Statistical hits distribution
SVM classifier
Video Authenticity validation
Retain differ inter frame result set from forgerv video

Fig 3.2 Framework for SVM Classifier using the Correlation coefficient

4. Results and Discussion

For the implementation of proposed work, make use of the polynomial kernel of support vector machine, which is much known as the classifier with a Matlab environment. To train the SVM classifier, about 4/5 of the 250 different video forgeries). The respite 1/5 form testing set (videos are arbitrarily select as the training set by referring standard dataset design as discussed in 3.1(A). The experiments are recurring for five times to secure reliable classification result

4.1 Video Selected From Standard Data Set and generated its sequence of the frameset.

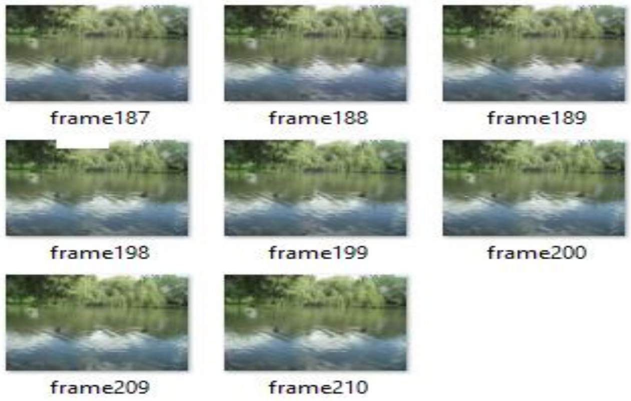


Fig 4.1 Converted sequence of frameset from forged video

4.2 Applied RGB colour Transformation and generated a series of Gray Frame Set.

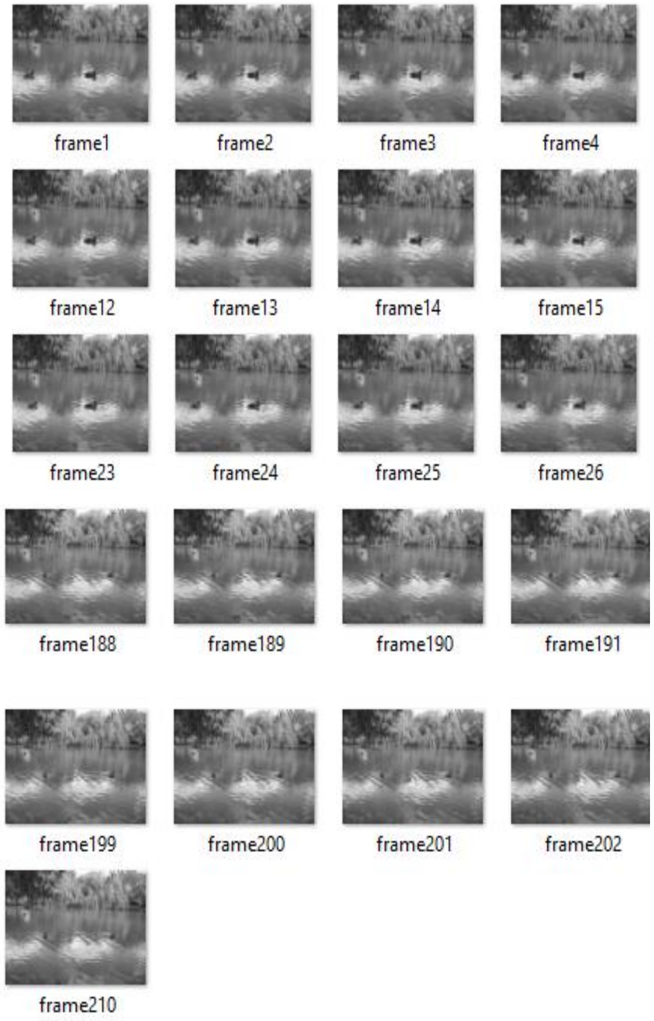


Fig 4.2 Gray Frameset for forgery video selected from the dataset

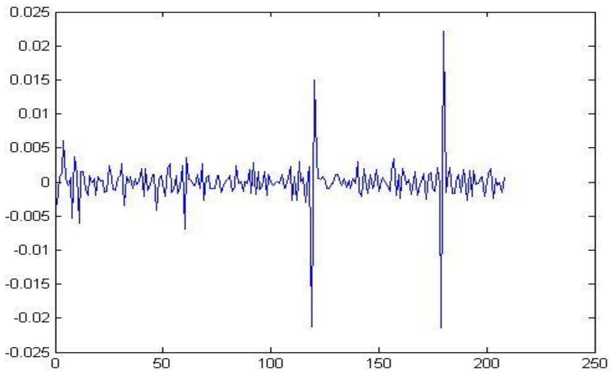


Fig 4.3 Resultant frame correlation differences with given forged frames

Identification of I-frame of forgery sequence from a given forged frames:

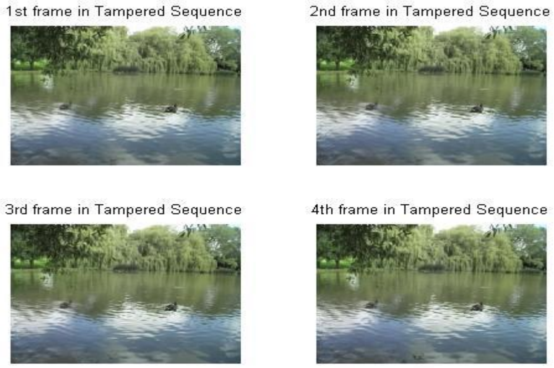

1st frame in Tampered Sequence
2nd frame in Tampered Sequence
3rd frame in Tampered Sequence
4th frame in Tampered Sequence

Fig 4.4(a) the first Interdependency forged an I- frame set of correlation difference set

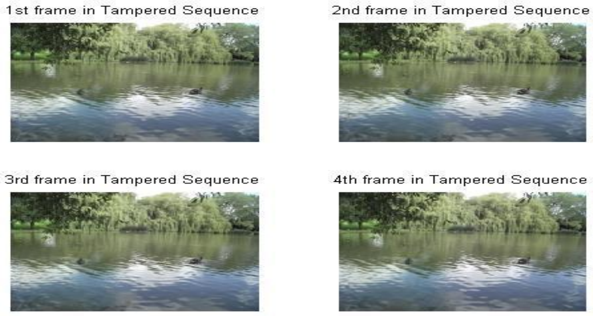

1st frame in Tampered Sequence
2nd frame in Tampered Sequence
3rd frame in Tampered Sequence
4th frame in Tampered Sequence

Fig 4.4(b) The second Interdependency forged an I-frame set of correlation difference set

From the above-obtained result, we get a forged sequence of interdependency frames from given forgery video.

5. Conclusion and Future Scope

We proposed an innovative method for the detection and identification of forged forgery inter-frame between conjugative forged sequences of copy create video forgery based on frame correlation difference by referring SVM classifier. Since the inter-frame forgery sequence of forgery identification is retaining as the best result among challenging issues, it exists in video forgery detection. With this approach, the central theme of complexity and redundancy is reduced in videos by their massive size by color transformation techniques between different frameset, to deal with this problem we resorted fast to identified the forgery region. The proposed a copy-create forensic technique used to verifies the inter-frame relationship among the sequence video frame set by referring the I-frame relation between two conjugative groups of a frameset. By considering the standard video forgery dataset like SULFA and Sysu-Obj-Forge dataset for evaluating the testing of forged and trained video sets obtained good accuracy and precession rate .success retain is above 90% depending on threshold value for training set.

6. References

1. O. I. Al-Sanjary, A. A. Ahmed, A. A. B. Jaharadak, M. A, M. Ali, and H. M. Zangana, "Detection clone an object movement using an optical flow approach," 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, 2018, pp. 388-394. doi: 10.1109/ISCAIE.2018.8405504
2. S. Jia, Z. Xu, H. Wang, C. Fan, and T. Wang, "Coarse-to-Fine Copy-Move Forgery Detection for Video Forensics," in IEEE Access, vol. 6, pp. 25323-25335, 2018. doi: 0.1109/ACCESS.2018.2819624
3. B. Üstübıoğlu, G. Ulutaş, V. V. Nabıyev, M. Ulutas, and A. Üstübıoğlu, "Using correlation matrix to detect frame duplication forgery in videos," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, 2018, pp. 1-4.doi: 10.1109/SIU.2018.840436 4
4. L. Su, C. Li, Y. Lai and J. Yang, "A Fast Forgery Detection Algorithm Based on Exponential-Fourier Moments for Video Region Duplication," in IEEE Transactions on Multimedia, vol. 20, no. 4, pp. 825-840, April 2018. doi: 10.1109/TMM.2017.2760098
5. . S. Verde, L. Bondi, P. Bestagini, S. Milani, G. Calcagno, and S. Tubaro, "Video Codec Forensics Based on Convolutional Neural Networks," 2018 25th IEEE International Conference on Image Processing (ICIP), Athens, Greece, 2018, pp. 530-534.doi: 10.1109/ICIP.2018.8451143
6. C. Feng, Z. Xu, S. Jia, W. Zhan, and Y. Xu, "Motion-Adaptive Frame Deletion Detection for Digital Video Forensics," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 27, no. 12, pp. 2543-2554, Dec. 2017. doi: 10.1109/TCSVT.2016.2593612 .
7. C. C. Huang, Y. Zhang and V. L. L. Thing, "Inter-frame video forgery detection based on multi-level subtraction approach for realistic video forensic applications," 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP), Singapore, 2017, pp. 20-24. doi: 10.1109/SIPROCESS.2017.8124498.
8. K. Sitara and B. M. Mehtre, "A comprehensive approach for exposing inter-frame video forgeries," 2017 IEEE **13th** International Colloquium on Signal Processing and Its Applications (CSPA), Batu Ferringhi, 2017, pp. 73-78. doi:1109/CSPA.2017.8064927.
9. S. Andy and A. Haikal, "Simple duplicate frame detection of MJPEG codec for video forensic," 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, 2017, pp. 321-324. doi: 10.1109/ICITISEE.2017.8285520
10. J. Xu, Y. Liang, X. Tian, and A. Xie, "A novel video inter-frame forgery detection method based on histogram intersection," 2016 IEEE/CIC International Conference on Communications in China (ICCC), Chengdu, 2016, pp. 1-6 doi: 10.1109/ICCChina.2016.7636851
11. Chittapur G.B., Murali S., Prabhakara H.S., Anami B.S. (2014) Exposing Digital Forgery in Video by Mean Frame Comparison Techniques. In: Sridhar V., Sheshadri H., Padma M. (eds) Emerging Research in Electronics, Computer Science and Technology. Lecture Notes in Electrical Engineering, vol 248. Springer, New Delhi
12. M. Mathai, D. Rajan, and S. Emmanuel, "Video forgery detection and localization using normalized cross-correlation of moment features," 2016 IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI), Santa Fe, NM, 2016, pp. 149-152.doi: 10.1109/SSIAI.2016.7459197.
13. Wang, Q. , Li, Z. , Zhang, Z. and Ma, Q. (2014) Video Inter-Frame Forgery Identification Based on Consistency of Correlation Coefficients of Gray Values. *Journal of Computer and Communications*, **2**, 51-57. doi: 10.4236/jcc.2014.24008.