






# A Simple Difference Based Inter Frame Video Forgery Detection and Localization

B. H. Shekar<sup>1</sup> , Wincy Abraham<sup>2</sup>  , and Bharathi Pilar<sup>3</sup> 

<sup>1</sup> Mangalore University, Mangalagangothri, Mangalore, India

<sup>2</sup> Assumption College, Changanacherry, Kottayam, India  
wincy@gmail.com

<sup>3</sup> University College, Mangalore, Mangalore, India

**Abstract.** A video becomes forged, if it is altered by changing the information contained within a frame or by changing the original sequencing of frames by deleting some frames or adding some frames in between, referred to as intra-frame forgery and inter-frame forgery respectively. This paper proposes an effective method for inter-frame video forgery detection which is capable of detecting duplication of frames, deletion of frames and also insertion of frames in the video. The method proposed is also capable of locating the forgery. There are many other existing methods which detect video forgery using features such as correlation coefficient between adjacent frames, optical flow, Zernike moment and so on. The proposed method detects forgery in a simple method compared to the existing ones. It consumes less computational power and time. The fact that manipulation done on the video alters the original sequencing of frames, which can be detected by examining the difference in pixel intensities of adjacent frames is made use of by this method. This method separates the frames of the video and uses the difference in pixel intensities of adjacent frames in two different ways to detect forgery. The original sequence of frames in the video follows a smooth pattern of adjacent frame differences, but any change occurring to the sequencing causes spikes. By checking the presence of these spikes, forgery along with the location of forgery can be detected. This method is found to have better accuracy compared to state-of-the-art methods and experimentation is done using the publicly available datasets.

**Keywords:** Video forgery · Pixel intensity · adjacent frames · outlier detection

## 1 Introduction

Nowadays video evidence plays a vital role in the detection of crimes, as video capturing of events is a common practice now due to the availability of surveillance cameras and other digital cameras for common use. Video forgery has become a common phenomenon as video manipulation tools are easily available and can be used even without much expertise. To hide evidence of crimes from

the video, it is modified by deleting some frames or removing some objects within the frame of the video. Sometimes video is altered by inserting some other frames into it or by doing any other type of forgery. This means that manipulation of the video is a common practice in every society. The detection of it is highly demanded especially by the court of law as it is used as evidence and also by the common man because people want to see what is real and not something fake. Many methods exist for video forgery detection but none is foolproof. So better methods are still in demand.

Video forgery can be classified as inter-frame forgery or intra-frame forgery. We know that a video is made up of a sequence of frames. In video compression, 3 types of frames are used, I-frame, P-frame and B-frame. I-frame(Intra coded picture) is the least compressed and is a complete image. P-frames(Predicted picture) contain only the difference from the previous I-frame to save space. B-frames(Bidirectional predicted picture) store the difference from both the previous and the following frames to specify its content, thus saving more space. In inter-frame forgery, the forgery takes place between the two adjacent frames of the video. It may be by inserting a new set of frames or by copy-pasting frames in between any two frames, or by deleting a set of frames from the video. Some video forgery detection algorithms use the changes happening to the different types of compressed frames of the video while others consider only the decompressed frames. In intra-frame video forgery, manipulation takes place within the frames of the video. Some objects in the frame may be removed or new objects added and so on. Various methods exist to detect inter-frame forgery and intra-frame forgery and forgery which is a combination of both types. They differ in the approach used, the data set considered and the level of detection accuracy.

This paper proposes a simple and efficient method for inter-frame video forgery detection which considers the intensity variations in the frames of the video and yields results better than some of the state-of-the-art methods. The following section discusses the works carried out by other researchers on this topic. Section 3 describes the methodology mean while Sect. 4 discusses various other methods we tried for forgery detection. Section 5 deals with the experimentation carried out and the results obtained for the various datasets and concluding remarks are expressed in Sect. 6.

## 2 Review of Related Literature

Video forgery occurs in various forms like object duplication, frame duplication, object deletion, frame deletion, object splicing, frame shuffling, frame insertion and so on. Various methods exist which perform the detection of these types of forgeries. Many of the detection methods which are capable of detecting one type of forgery do not work well for forgery of another type. A single technique which can detect video forgery irrespective of the type of forgery is highly demanded.

J. A. Aghamaleki et al. [1] detect inter frame video forgery by the analysis of quantization effect of DCT coefficients of I and P frames. Soumya et al. [2] in their method localizes inter-frame forgery due to frame replication and

the potential tampered frames are identified through frame similarity analysis. Statistical measures of entropy and contrast of residual frames along with similarity measures serve as the feature set for detection. They have done manipulation on surveillance video and self-captured smartphone video to create a dataset for the experimentation. Wang et al. [3] use correlation coefficient as a measure of similarity to find frame duplication. The similarity in the spatial and temporal correlations is used as an indication of frame duplication. Shanableh T et al. [4] use prediction residuals, percentage of intra-coded macroblocks, quantization scales and an estimate of the PSNR values using the I, P and B frames in the video for detecting frame deletion. K. Sitara et al. [5] proposes an inter-frame forgery detection algorithm based on tamper traces from spatiotemporal and compressed domains. They experimented using a dataset containing 23,586 videos which comprised inter-frame video forgeries like insertion, deletion, duplication, and shuffling. Evaluation results demonstrate that the model outperforms other methods, especially the inter-frame shuffling detection. Zhao et al. [6] propose a method which performs detection by HSV colour histogram difference between adjacent frames as a similarity measure and matching recheck based on tampering positions. The method is capable of detecting frame insertion, copying and deletion. Experimental results demonstrated that the model achieved precision, recall, and accuracy of 98.07%, 100%, and 99.01%, respectively. The model, therefore, outperformed the existing state-of-the-art methods of that time. Akumba et al. [7] use the mean and standard deviation of the correlation coefficient between adjacent frames as the feature to perform classification as authentic and forged. An accuracy of 100% is obtained for the VIFFD dataset and locally manipulated video dataset. In the method by Gurvinder Singh et al. [8] different algorithms are proposed to detect frame duplication and region duplication forgeries in videos. The authors claim higher detection accuracy and execution efficiency compared to the existing methods. The dataset used consists of some videos from SULFA [13] and some downloaded from the internet. In the method by Vinay Kumar et al. [9] the inter-frame correlation coefficient and correlation distance measure are used for the detection and localization of forgery and has 83% accuracy at the video level. They use the publicly available VIFFD [11] dataset for experimentation. In the work by Nitin et al. [10] entropy coded (DistrEn2D and MSE2D) frames are used for forgery detection using the correlation consistency between them. Two-dimensional distribution entropy (DistrEn2D) and bi-dimensional multiscale entropy (MSE2D), are used for the detection. Experimentation is done on original data collected from SULFA [13], REWIND [14], and VTL [18] and then applying various forgery operations. The overall detection accuracy is claimed to be 96.6%. Sondos et al. detect [16] inter-frame forgery operations like frame shuffling, frame insertion and deletion and are localized using the temporal average and the universal image quality index. The method was tested using 15 tampered videos which are made publicly available. In [17] the authors propose a two-stage inter-frame forgery detection technique with low computational cost for HEVC-coded videos. In the first stage, abnormal points are detected based on compression domain

features, and in the second stage, the abnormal points and their locations are validated. Li et al. [21] in their method use camera sensor pattern noise to detect inter-frame splicing forgery detection. The method first estimates reference SPN, and then calculates signed peak-to-correlation energy (SPCE) at the block level for classification. We concentrate our attention here on inter-frame forgery. The proposed method is capable of handling any kind of inter-frame forgeries like frame insertion, frame duplication and frame deletion.

### 3 Proposed Method

Frames of the video can be separated and each frame can be treated as an image. Each image is represented using the intensity at each pixel. The consecutive frames in the video will have small differences in some but not all of the corresponding pixel values. This fact is made use of in finding the inter-frame forgery. Our proposed method makes use of the difference in pixel intensities of the adjacent frames as the feature for the detection of forgery.

There are two differences considered in this approach for more accurate detection. Pixel-wise difference of adjacent frames and difference of adjacent frame averages. The video is first divided into constituent frames. Then frames are converted to gray scale. We then focus on the difference between the intensity values of adjacent frames for the clue for forgery as the difference will be high if any frame under consideration is a newly inserted one or which became adjacent due to the deletion of some frames in between. If there are scene changes in the video, it will result in frames with varying content. The variation of content in adjacent frames may be due to camera motion, movement of objects within the scene, noise and change in lighting [15]. In the case of videos captured using surveillance cameras, camera motion problems will not be present. The difference caused by noise and change in lighting can be neglected as it will be small compared to the difference caused by moving objects. Thus the main cause of scene change when the video is captured using surveillance cameras is the movement of objects. But in videos with high frame rate, the change in adjacent frame intensities due to forgery outweigh the change due to object motion.

The proposed method uses two difference arrays for video forgery detection each of which contains the difference between adjacent frames in two different ways. The presence of outliers in these arrays indicates forgery. They are computed as follows.

1. differenceArray DA is found by finding the difference in intensity of each pixel in the adjacent frames as

$$DA[i, j] = f_k[i, j] - f_{k+1}[i, j] \quad (1)$$

where  $k$  varies from 1 to one less than the total number of frames  $n$  of the video, and  $i, j$  take values as per the size of each frame.

DiffAvg, the average of differenceArray DA is found by

$$DiffAvg = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} DA(i, j)}{M \times N} \quad (2)$$

2. AvgDiff is found by finding the average intensity of each frame, as

$$AvgFrame_k = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f_k(i, j)}{M \times N} \quad (3)$$

and then taking the difference between adjacent frame averages.

$$AvgDiff = AvgFrame_k - AvgFrame_{k+1} \quad (4)$$

where  $k$  varies from 1 to one less than the total number of frames  $n$  of the video.

Both the differences hold the difference between the frame intensities and are found for the entire video. Thus there are two difference arrays created for each video. One to contain each DiffAvg corresponding to each adjacent frames as the element and the other to hold each AvgDiff as the element. These difference arrays are called differenceArray1 and differenceArray2 respectively. The location of the maximum element of the array is a suspected location of forgery. It is confirmed by checking whether the value found as the maximum of the array under consideration is a threshold time larger than the average value of its two neighbours at each side of the array. Otherwise, it is not a forgery location. It is formulated as

$$m > threshold \times \frac{differenceArrayx[n-1] + differenceArrayx[n+1]}{2} \quad (5)$$

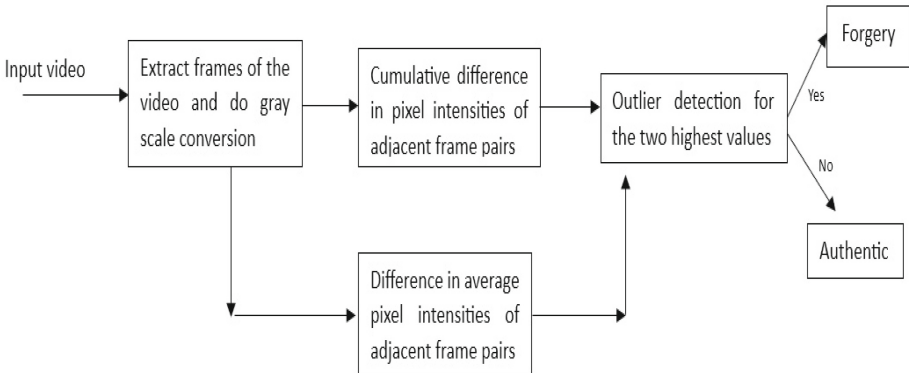
where  $m$  is the value at the location  $n$  of the *differenceArrayx*,  $x$  is either 1 or 2. The threshold is set as 20 for *differenceArray1* and 8 for *differenceArray2* empirically. If  $m$  is found to satisfy the above inequality,  $n$  is considered as a valid location of forgery and it is deleted from the array and the next maximum is found and the process is repeated. Thus if two such locations are found for a video it is considered as the location of insertion and copy forgeries while for deletion forgery only one value must appear as deviating from the normal values in the difference array. Since the inequality above checks for values which very much deviate from the normal values, many of them that come up during the process due to scene changes do not emerge as the locations of forgery.

The proposed method first checks differenceArray1 for outliers after which outlier detection is done on the differenceArray2 as well for which a threshold of 8 is chosen empirically instead of 20 used previously. Two types of arrays are used by the method since the forgery may remain undetected if only one array is used. Forgery undetected in one array is found to get detected in the other array. In case there is an outlier in any one of the arrays, the video is considered as forged. Otherwise, it is treated as authentic. It is seen that in most of the cases, the difference caused due to scene change or any other reason does not emerge as an outlier as the difference caused due to the manipulation of video is much larger compared to the differences due to the other reasons. The index of the outlier in the array is taken as the location of the forgery. The algorithm used in the proposed method is listed below.

Input: Video snippet  
 Output: Decision whether the video is forged or not  
 Method:

1. Separate all frames in the video.
2. Convert frames into gray colour format.
3. Calculate the cumulative difference in pixel intensities of adjacent pairs of frames.
4. Find the average intensity of each frame and then find the difference between adjacent frame pairs.
5. Use the difference array in step 3 for calculation and set threshold = 20.
6. From the difference array find the maximum value.
7. Confirm whether the maximum value is an outlier by checking whether it is more than threshold times the average of its neighbours at both sides in the array.
8. If any value emerges as an outlier in the above step keep it as a possible location of forgery, remove it from the array and repeat step 6 once more, go to step 10 otherwise.
9. If the threshold is not equal to 8, go to step 6 using the difference array of step 4 and by setting threshold = 8.
10. If forgery is detected in step 8 mark the video as forged and as authentic otherwise.
11. Exit

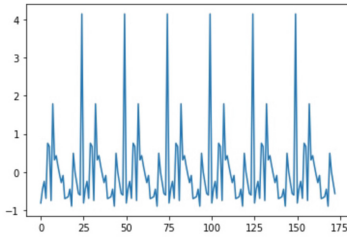
The block diagram depicting the method is shown in Fig. 1.



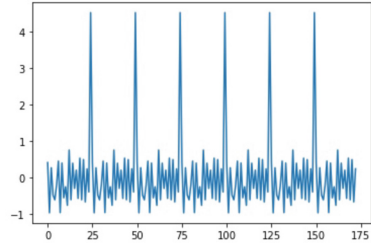
**Fig. 1.** Block diagram of the proposed classifier

The variation occurring to the frame content on forgery or scene change for various forged videos and original videos are illustrated in the following figures. Figures 2 and 3 depict the distribution of these differences for video forged by

frame duplication, the average value of adjacent frame differences (as mentioned in step 4 of the algorithm) and the difference of adjacent frame averages (as mentioned in step 6 of the algorithm) respectively. The spikes occur at the locations where the frame duplication occurs. It occurs at multiple places in this video. Both the differences indicate forgery.

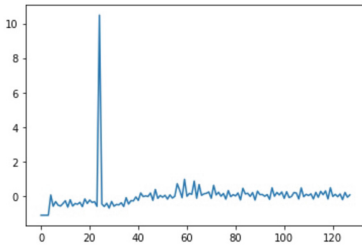


**Fig. 2.** Forgery due to frame duplication-Average of Pixel wise adjacent frame differences

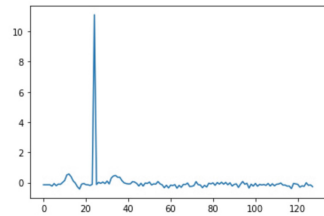


**Fig. 3.** Forgery due to frame duplication-Difference of averages of adjacent frames

Figures 4 and 5 illustrate the spike caused due to frame insertion at the beginning of the video. A set of frames have been inserted at the beginning. The spike occurs at the point of insertion and at the end of inserted frames. Here frames have been inserted at the beginning of the video. So the spike is seen only at one location. The difference graphs in Fig. 4 and Fig. 5 are shown in the same way as the above for a video forged due to frame insertion.

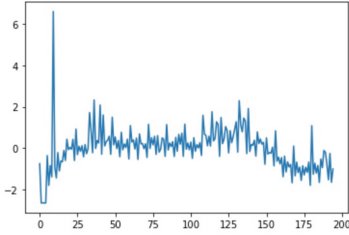


**Fig. 4.** Forgery due to frame insertion-Average of Pixel wise adjacent frame differences

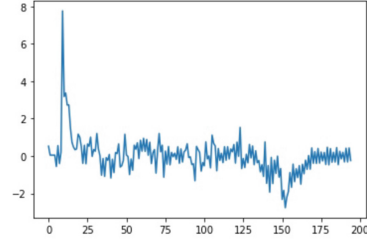


**Fig. 5.** Forgery due to frame insertion-Difference of averages of adjacent frames

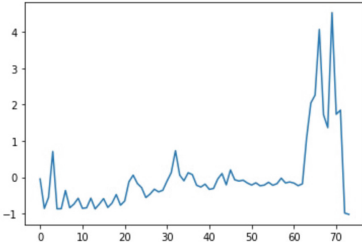
Figures 6 and 7 depicts the differences as before and the spikes occur at the locations where the frame deletion occurs. Since it is deletion forgery spike occurs only at one place if there is no sudden scene change. Figures 8 and 9 show the differences for video with no forgery and the graph appears not to have any spike indicating no forgery.



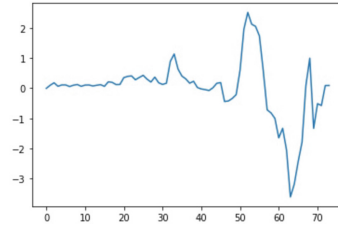
**Fig. 6.** Forgery due to frame deletion-Average of Pixel wise adjacent frame differences



**Fig. 7.** Forgery due to frame deletion-Difference of averages of adjacent frames



**Fig. 8.** Original Video-Average of Pixel wise adjacent frame differences



**Fig. 9.** Original video-Difference of averages of adjacent frames

## 4 Other Methods Considered

We borrowed some ideas from the state-of-the-art literature and tried various other methods for forgery detection. None of them could give satisfactory results, two of which are discussed below and a table is drawn to display the results of the comparison. One of them is the method by Qi Wang et al. [20] where they used the correlation coefficient between the adjacent frames of the video as the feature vector. We experimented the same using VIFFD as the dataset. For each video, the correlation coefficients obtained were analysed and the idea used was that if any value is below a certain lower limit, the video can be considered to be forged. Various lower limits were tried and the appropriate value to obtain the best result was found to be 0.95. However, it was found that only insert forgery it was able to identify well and in all other cases, it showed low performance. We ourselves considered another method which takes the standard deviation of the first 100 high-frequency coefficients of the DCT (Discrete Cosine Transform) of each frame of the video as the feature vector. Feature vectors extracted from all the videos in the dataset are supplied to SVM (Support Vector Machine) classifier for classification as authentic or forged. 80% of the feature vectors were used for training the classifier and the rest 20% were used for testing. However, the method could not achieve promising results. Table 1 shows the results obtained for both the methods considered in this section. The first method considered was



designed for forgery detection and localization while the second could do only forgery detection.

**Table 1.** Accuracy of the two other methods for VIFFD dataset

Method	Type of forgery	No of videos	Accuracy in %
Using	Copy	30	30
Correlation	Delete	30	43
Coefficient	insert	30	86.66
	Original	30	73.33
Using DCT	Forgery detection	120	77

## 5 Experiments

### 5.1 VIFFD Dataset

The proposed method is experimented on the VIFFD dataset [11] which has 120 videos out of which 30 are authentic and 90 videos are forged. Out of the 90 forged videos, 30 are forged due to frame duplication (copy), 30 videos are forged due to deletion and the rest are forged due to frame insertion. Experiments are carried out with this dataset and each video after processing is categorized into authentic or forged. For the VIFFD dataset this method works better than state-of-the-art methods. It gives 73.33% accuracy for frame deletion detection, 86.66% accuracy in frame duplication detection and 100% accuracy for frame insertion detection. Original video without forgery is identified with an accuracy of 70%. Thus the proposed system is found to have an overall accuracy of 82.5%. Table 2 shows the performance of this method for various types of forgery in terms of accuracy of classification.

The comparison of classification accuracy of the proposed method with some of the state-of-the-art methods is shown in Table 3.

**Table 2.** Accuracy of the proposed method for various types of forgery for VIFFD dataset

Type of forgery	No of videos	Accuracy in %
Copy	30	86.66
Delete	30	73.33
insert	30	100
No Forgery	30	70

**Table 3.** Performance Comparison of the proposed method with some of the existing methods using the VIFFD dataset

Method	forgeries	Accuracy in %
Vinay et al. [9]	Frame deletion, insertion	83
Proposed method	Frame deletion, insertion	86.66

## 5.2 Surveillance Video Dataset

A publicly available dataset was created by the authors of [16]. The dataset consists of 15 tampered videos. The forged videos are due to deletion, insertion and shuffling of frames. The proposed method is tested on this dataset, compared with the method proposed by the creators of the dataset and the result is shown in Table 4.

**Table 4.** Accuracy of the proposed method for various types of forgery for Surveillance video dataset

Method	Type of forgery	No of videos	Precision	Recall
Sondos et al. [16]	shuffling	5	.96	.97
	Delete	5	.98	.99
	insert	5	.99	.99
Proposed Method	shuffling	5	1	1
	Delete	5	1	1
	insert	5	1	1

## 5.3 TDTVD Dataset

In [18], the development TDTVD dataset containing total 210 videos for Temporal Domain Tampered Video Dataset using Frame Deletion, Frame Duplication and Frame Insertion is proposed. 120 videos in it are developed based on

Event/Object/Person (EOP) removal or modification, 40 each for frame deletion, frame insertion and frame duplication forgeries. The rest of the videos are created based on Smart Tampering (ST) or Multiple Tampering. They consist of videos with multiple tampering with frame deletion, frame insertion and frame duplication in three categories like 10 frames tampered, 20 frames tampered, and 30 frames tampered at 3 different locations in 10 videos each. The data set also contains 16 original videos from SULFA dataset [12]. The result of the experimentation is shown in Table 5.

**Table 5.** Accuracy of the proposed method for video forgery for TDTVD dataset

Type of forgery	No of videos	Accuracy in %
EOP Copy	40	90
EOPDelete	40	90
EOPInsert	40	100
Original	16	75
ST Copy-10	10	100
ST Copy-20	10	90
ST Copy-30	10	100
ST Delete-10	10	70
ST Delete-20	10	90
ST Delete-30	10	90
STInsert-10	10	100
STInsert-20	10	100
STInsert-30	10	100

#### 5.4 Inter-frame Forgery Data Set

Sondos et al. [19], made this data set publicly available, which they used for experimentation in their paper. Among the two folders with original and forged videos, the original video folder is copied as it is from the TDTVD data set. According to the authors their method has superiority in terms of execution time and precision and recall. The folder containing forged videos contains 32 videos forged due to insertion, copy, deletion and shuffling. Table 6 shows the details of the video and the result of experimentation using the proposed method.

**Table 6.** Accuracy of the proposed method for video forgery for inter-frame forgery dataset

Type of forgery	No of videos	Accuracy in %
Copy	10	90
Delete	5	100
Insert	5	100
Shuffling	9	77.77
Copy & Shuffling	3	100
Original	16	75

## 6 Conclusion

This paper presents an efficient and simple method for inter-frame video forgery detection which can detect frame insertion, deletion and frame duplication. The change happening to the sequence of adjacent frame differences, when the original sequencing is altered is found out by finding the arithmetic difference between adjacent frames of the video. The method may be modified by incorporating the detection of shot boundaries and then analysing each video segment by the proposed method for forgery detection as a future work. Thus the paper presents a simple difference-based method for inter-frame video forgery detection. It is found to work better than state-of-the-art methods.

## References

1. Aghamaleki, J.A., Behrad, A.: Malicious inter-frame video tampering detection in MPEG videos using time and spatial domain analysis of quantization effects. *Multimedia Tools Appl.* **76**(20), 20691–20717 (2017). <https://doi.org/10.1002/andp.19053221004>
2. Sowmya, K.N., Basavaraju, H.T., Lohitashva, B.H., Chennamma, H.R., Aradhya, V.N.M.: Similarity Analysis of Residual Frames for Inter Frame Forgery Detection in Video, ICICC 2019. *Advances in Intelligent Systems and Computing*, vol. 1034, p. 20. Springer, Cham (2019). <https://doi.org/10.1007/978-981-15-1084-7>
3. Wang, W., Farid, H.: Exposing digital forgeries in video by detecting duplication. In: *Proceedings of the 9th Workshop on Multimedia and Security - MM Sec 2007* (2007)
4. Shanableh, T.: Detection of frame deletion for digital video forensics. *Digit. Investig.* **10**(4), 350–360 (2013)
5. Sitara, K., Mehtre, B.M.: Detection of inter-frame forgeries in digital videos. *Forensic Sci. Int.* **289**, 186–206 (2007). <https://doi.org/10.1016/j.forsciint.2018.04.056>
6. Zhao, D.-N., Wang, R.-K., Lu, Z.-M.: Inter-frame passive-blind forgery detection for video shot based on similarity analysis. *Multimedia Tools Appl.* (2018). <https://doi.org/10.1007/s11042-018-5791-1>

7. Akumba, B.O., Iorliam, A., Agber, S., Okube, E.O., Kwaghtyo, K.D.: Authentication of video evidence for forensic investigation: a case of Nigeria. *J. Inf. Secur.* **12**, 163–176 (2021). <https://doi.org/10.4236/jis.2021.122008>
8. Singh, G.S.K.: Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation. *Multimedia Tools Appl.* (2018). <https://doi.org/10.1007/s11042-018-6585-1>
9. Gaur, V.K.M.: Multiple forgery detection in video using inter-frame correlation distance with dual-threshold. *Multimedia Tools Appl.* (2022). <https://doi.org/10.1007/s11042-022-13284-2>
10. Shelke, N.A., Kasana, S.S.: Multiple forgeries identification in digital video based on correlation consistency between entropy coded frames. *Multimedia Tools Appl.* **28**, 267–280 (2022). <https://doi.org/10.1007/s00530-021-00837-y>
11. Nguyen, X.H., Hu, J.: VIFFD - a dataset for detecting video inter-frame forgeries. *Mendeley Data 5*, *Multimedia Tools and Applications* (2020). <https://doi.org/10.17632/r3ss3v53sj.5>
12. Qadir, G., Yahaya, S., Ho, A.T.S.: Surrey university library for forensic analysis (sulfa) of video content. In: *IET Conference on Image Processing (IPR 2012)*, vol. 79(47), pp. 1–6 (2012). <http://sulfa.cs.surrey.ac.uk/>
13. Bestagini, P., Milani, S., Tagliasacchi, M., Tubaro, S.: Local tampering detection in video sequences. In: *2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP)* (2013)
14. Video Trace Library. <http://trace.eas.asu.edu/>
15. Hoose, N.: Computer vision as a traffic surveillance tool. In: *Control Computers Communications in Transportation*, pp. 57–64 (1990). <https://doi.org/10.1016/B978-0-08-037025-5.50014-1>
16. Fadl, S., Han, Q., Li, Q.: Surveillance video authentication using universal image quality index of temporal average. In: Yoo, C.D., Shi, Y.-Q., Kim, H.J., Piva, A., Kim, G. (eds.) *IWDW 2018*. LNCS, vol. 11378, pp. 337–350. Springer, Cham (2019). [https://doi.org/10.1007/978-3-030-11389-6\\_25](https://doi.org/10.1007/978-3-030-11389-6_25)
17. Singla, N., et al.: A two-stage forgery detection and localization framework based on feature classification and similarity metric. *Multimedia Syst.* **29**, 1173–1185 (2023)
18. Panchal, H.D., Shah, H.: Video tampering dataset development in temporal domain for video forgery authentication. *Multimedia Tools Appl.* **79**, 33–34 (2020). <https://doi.org/10.1007/s11042-020-09205-w>
19. Fadl, S., Han, Q., Qiong, L.: Exposing video inter-frame forgery via histogram of oriented gradients and motion energy image. *Multidimension. Syst. Signal Process.* **31**, 1365–1384 (2020). <https://doi.org/10.1007/s11045-020-00711-6>
20. Wang, Q., Li, Z., Zhang, Z., Ma, Q.: Video inter-frame forgery identification based on consistency of correlation coefficients of gray values. *J. Comput. Commun.* **2**, 51–57 (2014). <https://doi.org/10.4236/jcc.2014.24008>
21. Li, Q., Wang, R., Xu, D.: A video splicing forgery detection and localization algorithm based on sensor pattern noise. *Electronics* **12**(6), 1362 (2023). <https://doi.org/10.3390/electronics12061362>