https://dx.doi.org/10.4314/dujopas.v9i1a.3
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490

Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 9 No. 1a March 2023*

Scene Change aware Inter-Frame Forgeries Detection Technique for Surveillance Videos Based on Similarities Analysis

[1]Abdullahi Anas*, [2]Zaharadeen Yusuf Yeldu,
[3]Mustapha Aminu Bagiwa, [4]Muhammad Murtala Aliyu

[1]Department of Computer Science,
Faculty of Sciences
Sokoto State University,
Sokoto – Nigeria.

[2]Computer Science Unit,
Department of Mathematics
Usmanu Danfodiyo University
Sokoto–Nigeria

[3]Department of Computer Science,
Faculty of Physical Sciences,
Ahmadu Bello University,
Zaria – Nigeria.

[4]Department of Computer Science,
Collage of Sciences and Technology
Umaru Ali Shinkafi Polytechnic,
Sokoto – Nigeria.

Email: anas.abdullahi2@ssu.edu.ng

Abstract

Surveillance videos provide security and increases work efficiency in places of work and homes. as the most acceptable form of evidence, surveillance videos are now tampered to hide actions or convey wrong information. Researchers have proposed ways to mitigate the effect of activities of the attackers through checking the authenticity of the video. The proposed schemes suffer performance degradation in the presence of scene changes. Recently a scheme that addresses the effects of scene change on inter-frame forgery detection was developed where it detects scene changes and divides multiple scenes in to shots. The scheme improves the overall performance of the inter-frame forgery detection at the expense of high average computational time. In this research, a video scene change aware forgery detection scheme is proposed to mitigate the effect of scene change on inter-frame forgery detection with low average computational time. The proposed scheme utilizes the luminance level within frame region which is a more efficient feature to detect scene change. The experimental results show that the scheme has 57% decreases in computational average time and increased in accuracy to 99.03%.

Keywords: *Scene change, luminance level, Inter-frame forgery, Surveillance videos, Hue Saturation Value (HSV) colour histogram*

**Author for Correspondence*

INTRODUCTION

Nowadays video data has received great acceptability in the society. This is as a result of the way life and living changes after the global lockdown in the COVID-19 pandemic time. Videos are now widely used in conferences, calls, campaigns, preaching, seminars, class room and the court of law for evidences. Thus, there is development in the area of digital forensic and video forgery to be precise (Anas *et al.,* 2022). Video forgery is the tampering of video data to hide the occurrence of an event or item, delay the happening of an event or change the content of the video. This can be as simple as muting the sound of a video to as complex as showing an incumbent president campaigning for his opposition. Video forgery is made easy because of the free availability of the easy to use video editing softwares and websites that provide cracked copies of licensed softwares. Examples of these softwares include filmora, adobe photoshop, and coreldraw among others. To validate the authenticity of the video data, researchers developed techniques that detect tampered videos (Sitara, & Mehtre 2016).

Researchers classify video forgery detection into Active forgery detection and Passive forgery detection. The active forgery detection technique is an on the go technique that begins during the creation of the video data. This employs the use of specialized cameras with embedded features on the cameras. The passive forgery detection technique which does not rely on any embedded hardware feature explores the characteristics of the frame within the video for detection. Since video attacks can either be spatial, temporal and spacio-temporal, thus passive technique will also falls within one of these categories. Frame insertion, deletion and duplication are temporal forgeries in which frames are; removed from the video to conceal (deletion), inserted into the videos to convey or delay (insertion), and/or copied and pasted into the video to delay (duplication) by forgers (Anas *et al.,* 2022). To detect frame forgeries, numerous techniques have been employed by researchers Wang & Farid (2006, 2007 and 2009); Bestagini *et al.,* (2011); Feng *et al.,* (2011); Lin and Chan (2012); Yang *et al.,* (2016); Zhao *et al.,* (2018); and Anas *et al.,* (2022).

As mentioned earlier, a video forgery can be insertion, duplication and deletion, or combination of insertion/deletion or duplication, the developed techniques also exhibits same characteristics that is, one aspect which is insertion, duplication or deletion Wang and Farid (2006); Ling & Chang (2012) and Sharma *et al.,*(2021), combination of any two between insertion, duplication and deletion Feng *et al.,*(2011); Bestagini *et al.,* (2011); Wu, Jiang & Wang (2014); Yang *et al.,* (2016) and Bakas *et al* (2019) and all three aspects of frame forgery (Zhao *et al.,* 2020, Anas *et al.,* 2022). Zhao *et al.,* (2018) proposed a scheme which detects all the three aspect of frame forgeries by exploring the similarity analysis of the frame based on the correlation of statistical anomalies. The scheme achieved 98.07% precision rate, 100% recall rate and 99.01% detection accuracy. However, the accuracy of the scheme degrades in the presence of scene changes. Anas *et al.,* (2022) enhanced the performance of Zhao *et al.,* (2018) scheme in the presence of scene change by segmenting multi-scenes videos into shots, this increase the performance of the scheme with 99.1% accuracy in the presence of scene changes. Researchers had proposed several schemes to detect inter-frame forgeries. Wang and Farid (2006, 2007 and 2009), Bestagini *et al.,* (2011), Lin and Chan (2012), Lou *et al.,* (2014), Yang *et al.,* (2016), Zhao *et al.,* (2018), Anas *et al.,* (2022) among others. The proposed schemes can be broadly categorized in to single aspect, dual aspects and multiple aspects (Sitara, & Mehtre 2016). Single aspects are those schemes that detect either insertion/deletion or duplication of frames only. The dual aspect category is those schemes that detect combination of any of the two types of forgeries that is frame insertion & deletion insertion & duplication or duplication

& deletion. The final category is that which detects all the three aspects of insertion, deletion and duplication.

Zhao *et al.,* (2018) proposed Zhao *et al.,* (2018) proposed a technique which detects all the three aspects of frame forgery. However the accuracy of the scheme is affected by scene change. Shehnaz and Kaur (2022) and Anas *et al.,* (2022) improves the performance of Zhao *et al.,* (2018) by inserting the pre-check to detect the scene change and segments the multiple scene in to shots before checking for forgery. The scheme improves the overall performance of Zhao *et al.,* (2018) in the presence of scene change. However, it overall performance of the schemes solely depends on the incorporated scene change detection method. The scheme uses iteration method which results in computational overhead. A histogram based scene change detection algorithm was proposed Chon and Kang (2016) which extract and compute histogram distances; the scheme increases the detection accuracy. However, it is in effective in the presence of rapid movement.

Fuad *et al.,* (2021) utilizes DCT coefficient to capture the hidden locations as part of the scene change detection inputs. However, the used data set is too biased and also the scheme uses histogram shape difference only which is not efficient enough to reflect the features of regional shape and also computationally demanding. To mitigate this intrinsic flaw, Lee and Cho (2022) proposed a mechanism which uses histogram luminance level for every region within the given frame. The scheme outperforms Chandra and Dolley (2016) and other traditional schemes with 122.5% improvement and 87% reduction in complexity. The scheme proposed by Anas *et al.,* (2022) incorporates Chandra and dolley (2016) scene change detection mechanism. The scheme iteratively uses an automatic threshold to find the luminance difference of the preceding and the current frames which is simply termed as histogram shape difference. However, histogram shape difference only do not reflect the features of regional shape, it is also an iterative process which result in false detection and high computational intensity respectively. To increase the efficiency of Anas *et al.,* (2022) scheme and also to reduce its complexity, a robust and efficient scheme developed by Lee and Cho (2022) is proposed to replace the scene change detection scheme by Chandra and dolley (2016).

PROPOSED SCHEME

To enhance the performance of Anas *et al.,* (2022) scheme, Chandra and Dolley (2016) scene change detection mechanism will be replaced with a robust and efficient mechanism developed by Lee and Cho (2022). The newly incorporated scheme is chosen to reduce computational intensity of the overall scheme as well as increase the precision and accuracy. The figure 1 below shows the schematic view of the proposed scheme.

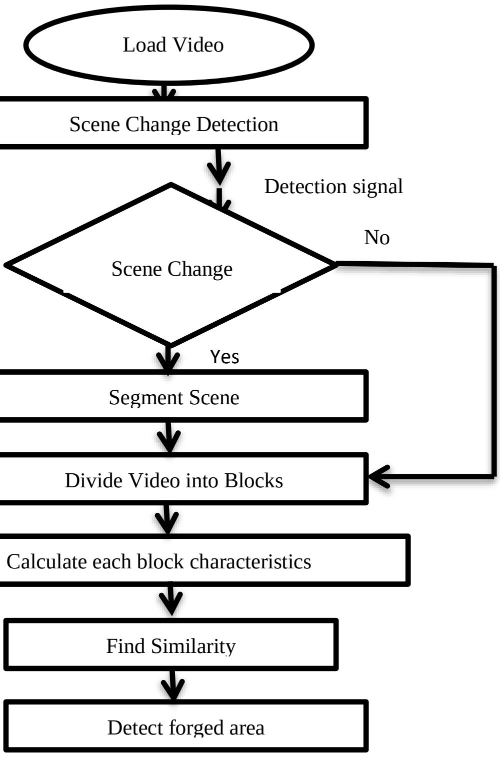

Figure 1: Proposed Scene Change Aware Inter-frame Forgery Detection Scheme (SCAIFD) Diagrammatic Description

DATA SET

Supporting the report of the proposed SCAIFD scheme, the performance of the scheme is evaluated using the same dataset used by Anas *et al*., (2022). The dataset consist of 2064 frame obtained from distinct test videos of (Casia 2 and Nc16). Table 1 shows summary of the data.

Table 1: Dataset Summary.

No	Names of Files	Arrangement	E&S	Resolution	Length
1	Yusuf bike.mp4	MP4	MP4V	1920x1080	253
2	Walking Mp.AVI	AVI	MJPG	640x480	111
3	Sajeed and Kayo. AVI	AVI	DIVX	320x240	266
4	Gwandu family.MP4	MP4	MP4V	720x404	273
5	Kofar ligi Street.MP4	MP4	MP4V	720x404	324
6	Sadiq table tennis. MP4	MP4	MJPG	320x240	304
7	Arif Ball.AVI	AVI	MJPG	1920x1080	294
8	Walking Ahmad deedat.AVI	AVI	DIVX	320x240	248
9	Baffa's Room.AVI	AVI	DIVX	640x480	119
10	Nawwal Riding Bike.AVI	MP4	MP4V	720x404	215

RESULTS

The performance of the scheme is evaluated and compared against the benchmark scheme (Anas *et al.* 2022). The implemented scheme also uses similarity analysis to detect forged videos. The Hue Saturation Value histogram (HSV) is used for the similarity analysis. In these histograms, frame insertion forgery is detected by searching for two abnormal peak values. This can be seen as shown in figure 2. Likewise frame deletion can be detected on the Saturation Value histogram (HSV) histogram when one abnormal peak value is detected as shown in figure 3. To detect the duplication on HSV histogram a solid straight depicting exact consecutive frame is searched for as frames of the same type have the same characteristics, this shown in figure 4.

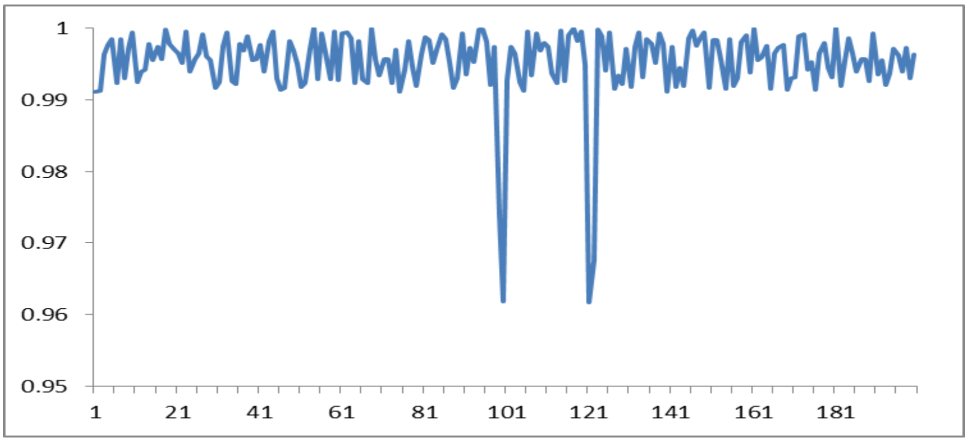

Figure 2: Frame insertion Detection sourced from HSV Histogram

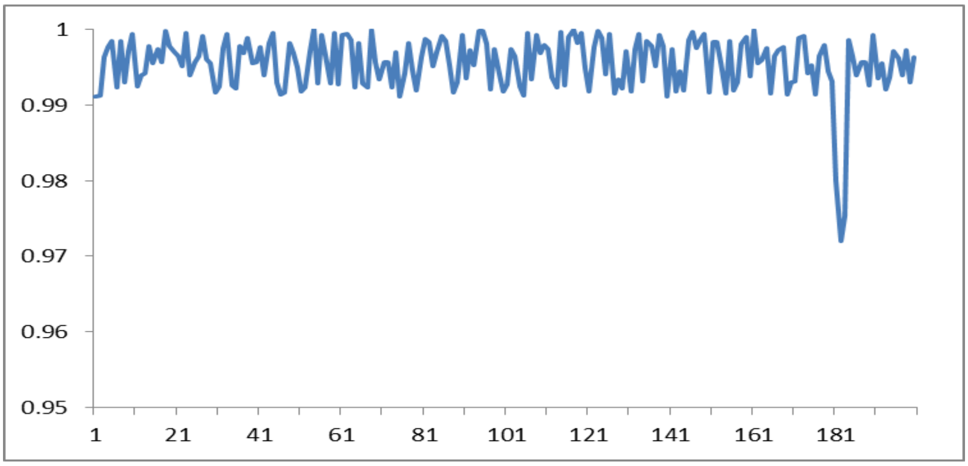

Figure 3: frame deletion Detection sourced from HSV Histogram

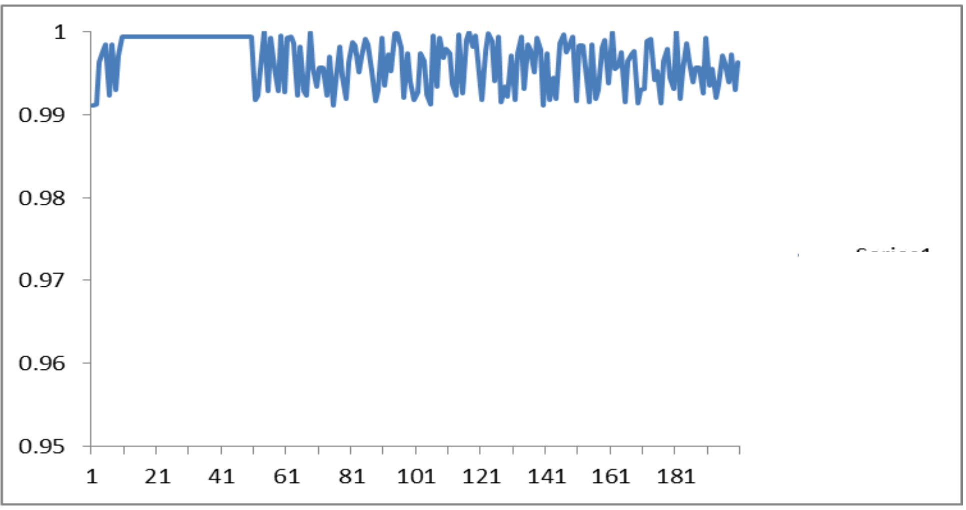

Figure 4: Frame duplication Detection sourced from HSV Histogram

DISCUSSION

To evaluate the overall performance of the implemented scheme, four robust metric which includes accuracy, precision, recall and average computational time were used in determining the efficiency of the scheme. The accuracy, precision and recall performance metrics are mathematically computed using the following equations.

$$\mathrm{P} = \frac{TP}{TP + FP}, R = \frac{TP}{TP + FN}, A = \frac{TP + TN}{TP + TN + FP + FN}$$

In the equations, TP denotes total frames detected correctly and TN denotes it opposite correctly detected forged frames. FP represent the number of incorrectly authentic frames detected as forged, FN is the opposite of FP. Figure 5 shows the performance of the implemented scheme against Anas *et al.,*(2022). As a scalar metric, the computational complexity of the scheme solely depends on the algorithm as shown in figure 6. The computational time complexity of Anas *et al.,* (2022) is approximately 104µs. in contrast the implemented scheme has uses approximate 13µs which is about 87% reduction. This is realized because Chandra and Dolly (2016) uses an iterative automatic threshold system which takes ample amount of time.

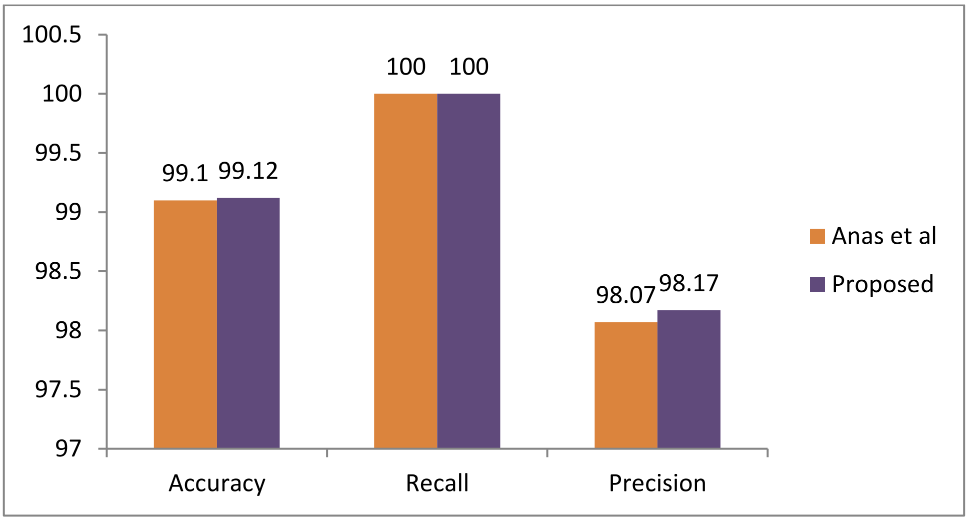

Figure 5: Performance scheme against bench mark scheme.

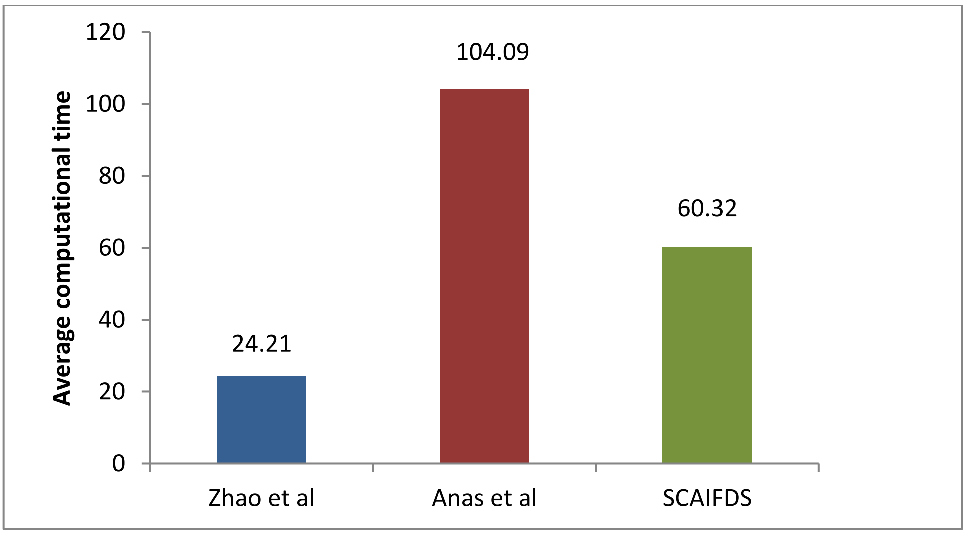

Figure 6: Average computational time

CONCLUSION

The experimental result of Scene Change Aware Inter-Frame Forgery Detection Scheme (SCAFDS) shows a significant improvement of the overall performance of Anas *et al.,* (2022) scheme. The computational average time has about 57% reduction and also the accuracy of the scheme increase by 0.02% which now reads 99.03%. The precision also realized on the increase 0.1% which is now 98.17%. With 0.02% increase in accuracy, 0.1% increase in precision and a whooping decreased of 57% in average computational time, this shows the robustness of SCAIFDS has an improved performance over the benchmarked schemes.

ACKNOWLEDGEMENT

This research is supported by Tertiary Education Trust Fund (*TetFund*) 2022, **No: TETF/DR&D/CE/UNI/SOKOTO/IBR/2022/VOL.I.**

REFERENCES

Anas, A., Bagiwa, M. A., Roko, A., Buda, S., Yaldu, Z. Y., Bello, A. M. & Ainu, H. A. (2022). An inter-frame forgery detection technique for surveillance videos based on analysis of similarities. *SLU journal of science and technology, 4(1&2), 15-26. doi.org/1056471/slujst.v4i.265.*

Bagiwa, A., Wahab, A., Idris, I., Khan, S., & Razak, Z. (2014). Passive Video Forgery Detection Techniques: A Survey. *IEEE International Conference on Information Assurance and Security,* 2(9), 29–34.

Bestagini, R, Milani, A., Tagaliassani, W., & Tubaro, F. (2011). Video forgery detection for detecting frame insertion and deletion based on structural similarity. *The Third International Conference on Multimedia Technology*, Guangzhou, pp 63–76

Chandra, M & Dolley S (2016). Detection of Scene Change in Video, *International Journal of Science and Research (IJSR),* pp. 2319-7064

Fuad M., Ernawan F & Hui L. J. (2021). Video scene change detection based on histogram analysis for hiding message. *Journal of Physics: Conference Series 9(4),* doi:10.1088/1742-6596/1918/4/042141.

Feng, C. X, Xu, Z. Y., Jia, S. W., Zhang, W. R. and Xu, Y. Y. (2016). Motion-Adaptive Frame Deletion Detection for Digital Video Forensics. *IEEE Trans on Circuits and Systems for Video Tech,* 25(9), pp. 123-139. https://doi.org/10.1109.

Kumar, V & Gaur, M (2022). Multiple forgery detection in video using inter-frame correlation distance with dual-threshold. *Multimed Tools Appl.* https://doi.org/10.1007/s11042-022-13284-2.

Lin, G. & Chang, J. (2012) Detection of frame duplication forgery in videos based on spatial and temporal analysis. *International Journal of Pattern Recognition and Artificial Intelligence,* 26(7): 1250017(1–18).

Lee & Cho (2022) Luminance Level of Histogram-Based Scene-Change Detection for Frame Rate Up-Conversion. *IEEE Trans. Consum. Electron.,* vol. 52(3), pp. 975_982, DOI:*10.1109/ACCESS.2022.314664*

Sitara, K., & Mehtre, M, (2016), Digital video tampering detection: An Overview of passive techniques, *Digital Investigation* doi: 10.1016/j.diin.2016.06.003.

Sharma H. M.and Kanwal N. K. (2021). Video inter-frame forgery detection: Classification, technique & new dataset Journal of Computer Security 29 (2021) 531–550 DOI 10.3233/JCS-200105.

Shehnaz, Kaur, M. (2022). Texture Feature Analysis for Inter-Frame Video Tampering Detection. In: Uddin, M.S., Jamwal, P.K., Bansal, J.C. (eds) Proceedings of International Joint Conference on Advances in Computational Intelligence. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-19-0332-8_22

Wang, W., & Farid, H., (2006). Exposing digital forgeries in video by detecting double MPEG compression. *In: Proceedings of the 8th Workshop on Multimedia and Security, Geneva, Switzerland, pp. 37–47.*

Wang, W., & Farid, H. (2007). Exposing digital forgeries in video by detecting duplication. *In: Proceedings of the 9th Workshop on Multimedia & Security, Dallas Texas USA, pp. 35–42.*

Wang, W., & Farid, H. (2009). Exposing digital forgeries in video by detecting double quantization. *In: Proceedings of the 11th ACM Workshop on Multimedia and Security, Princeton New Jersey USA, pp. 39–48.*

Wang, W., Jiang, X., Wang, S., Wan, M., & Sun, T. (2014). Identifying video forgery process using optical flow. *In: Digital-Forensics and Watermarking. Springer Berlin Heidelberg, pp. 244–257. http://dx.doi.org/10.1007/978-3-662-43886-2_18.*

Wu, Y., Jiang, X., Sun, T., & Wang, W. (2014). Exposing video inter-frame forgery based on velocity field consistency. *In: Proc. 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, Florence, Italy, http: //dx.doi.org/10.1109/icassp.2014.6854085.*

Yang, M., Huang, T., & Su, L. (2016) Using similarity analysis to detect frame duplication and deletion forgery in videos. *Multimedia Tools and Applications* 75(4):1793–1811.

Zhao D., Wang R., & Lu Z. (2018). Inter-frame passive-blind forgery detection for video shot based on similarity analysis. Springer Science+Business Media, https://doi.org/10.1007/s11042-018-5791-1.