Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 4501-4508

# Robust Video Authentication Mechanism Based On Statistical Local Feature

**[1]Mr. Avinash Wadhe, [2]Dr. Prof. Asha Ambhaikar**
[1]PhD Scholar, Kalinga University, Raipur, India
[2]Professor, Kalinga University, Raipur, India
aviwadhe@gmail.com, dr.asha.ambhaikar@gmail.com

**Abstract:** Advances in technology have made it easier to edit videos today, making it harder to maintain the reliability of video information. Videos can be created using many digital devices and such videos can be broadcast on any channel through high-speed internet. Video captured from CCTV can be used as evidence but must first be protected from tampering. Video authentication can be done using watermarking and digital signatures but this technique is used for copyright. It is difficult to monitor videos and authenticate videos captured by the user's cameras. In this study, we will develop a strong technique based on video local information for video authentication that can be used in real applications. The proposed technique processes the dataset of videos captured by the user's cameras using the statistical local information of the video. The results of the proposed technique show that the proposed technique for video authentication is reliable, faster and less expensive than other techniques.

**Keywords:**Video Information, Video Authentication, Video Sequences

## 1. Introduction

Information and technology have played an important role for many decades to this day. Today we can transmit information thousands of kilometers away in a few seconds. Therefore, it seems to have affected human life as well as development. Although technology has brought us to the threshold of a new era today, one of the serious challenges is video authentication.

In today's age of modern technology, it has become easier to share multiple videos using communication and compression techniques. Its reliability can also be compromised by making some changes to the video using multimedia tools and techniques. The increasing use of new multimedia and computer tools and techniques has made handling video sequences easier. So, it has not been easy to certify the reliability and integrity of the video.

Although Duffy and Hellman conducted research on the validation of multimedia data in 1976, new researchers are still working in this area. Although watermarking and digital signatures are used for video authentication, there are still limitations to this technique.

The disadvantage of watermarking and digital signatures is that they must be included when capturing video, [4] moreover, watermarking and digital signature-based techniques are helpless to have without any watermarks or in any raw video. Types of digital signatures, in this case, we cannot calculate and match any pre-embedded watermarks or prefabricated digital signatures and here

comes the importance of intelligent authentication techniques that can establish frames according to the frame relationship using local statistical features.

## 2. Related work

B. C. Hosler et. al. (2019) proposed the techniques for video authentication and camera recognition on video-ACID dataset using the deep learning approach. Hala Bahjat et. al. (2018) proposed the mechanism for digital video authentication on temporal attacks. In this mechanism, sender was generating the signature for video authentication based on video and private key and at the receiver end, also generate the signature for same video then both signatures were compared. if signature were match then video is not tempered otherwise tempered.

Fadl SM et. al. (2018) proposed the algorithm for duplicate frame detection in video based on standard deviation. In this approach used discrete cosine transform coefficients measured for selection of residual frame to remove the unnecessary feature and detect the video forgery.

Akumba, B et. al. (2021) proposed the model for detecting the forged videos from authentic videos based on the correlation coefficients implemented on MATLAB software. The proposed model achieves the good accuracy level and effectively detect the inter-frame forgeries.

## 3. Video Tampering Attacks

The main function of video authentication is to identify and show where and how the video was captured. Following are some video tempering techniques are given:

**Adding New Frames :**In this scheme, user can add one or more frames into the sequence of frames in video.

**Deleting Frames:**In this scheme, delete one or more frame is from the frame sequence.

**Frame shuffle:**In this scheme,user can change order of the sequence of frames.

**Transcoding:**In this scheme, video coding is translated into another coding.

**Frame rate:**In this scheme, user can change the frame rate at which frames are displayed.

**Spatial Tampering:**In this scheme, user can change the frame content according to need.

## 4. Proposed Methodology

### Video Statistical Local model and features

p is small piece of video segment. The sample video contains various video segments, $P^{(1)}, P^{(2)}, \dots\dots, P^{(n)}$. all the short segment are independent to each other. The Short segment can be obtained by dividing the complete video into small non-overlapping segments.

For, Video Segment P, related to graph $G = (V * T, E)$. The set V is related to the spatial location and the set T is related to temporal location in video segment. Each location, v belongs to V and time t belong T is related with a feature descriptor. While it is theoretically possible to consider all pixel locations and temporal instants, we quantize into $10 * 10 * 5$ non-overlapping blocks. We call these

blocks as atoms and we associate average values of features for each atom. Two atoms are connected if they are either temporal or spatial neighbors.

**Feature Descriptors:** We now describe local features that are associated with each node (atom) of our graph. During feature extraction we compute a feature value for each pixel. Then, the pixel-level features are condensed into a multi- dimensional vector for each atom by averaging each feature component over all the pixels within the atom. We use the following local features:

**Persistence:** Activity is detected using a basic back- ground subtraction method (as for instance in [5]). The initial background is estimated using median of several hundred frames. Then, the background is updated using the running average method. We flag each pixel as part of the background or foreground. Persistence, for an atom, is the percentage of foreground pixels in the atom.

**Algorithm for Video Anomaly Detection**

we are given training video samples and a test video sample. To reduce delay, we breakup the test video sample into test video segments, $P^{(1)}, P^{(2)}, \ldots\ldots, P^{(n)}$. Our task is to determine which of the test segment containan anomaly.

For convenience, we partition training videoin to segments$(x(1), \cdots, x(n))$ each of the same length as atest segments η , η(j). Our algorithm consists of three steps:

**Local Scores:** For any snippet y, which denotes either a test or training snippet, a local score at spatial location v, temporal instant, t, and at spatio-temporal scales, is computed (see Algorithm 1). We choose a uniform

Algorithm 1 Score for y at location (v, t), at scale s.

Input ; $\{x^{(j)}\}$ ; $KNN\ parameter\ K, Location\ (v,t);\ \ Scale\ s$

$Output d_{y,v,t}(s)$Filter at scale s:$x^{(j)} \leftarrow Filter_s(x^{(j)})$

Distance Computation:$d_j \leftarrow dist\big(yv,t,x^j v,\tau\big), \forall, j, \tau$

Compute $d_l$the $lth$ nearest neighbor distance by sorting$d_l$

Average: $d_{v,t} \leftarrow \frac{1}{k}\sum_{l=K+1}^{2K} d_{(l)}$

Normalized$d_{v,t}(S) \leftarrow \frac{d_{v,t}(s)}{D_v}; where\ D_v = max_t d_{v,t}$

spatio-temporal filter with support equal to s for simplicity.

**Segment Score:** Compute composite score for each segment-test and training segment—from local scores obtained

$$d_y(s) = \max_{v,t} d_{v,s,t(s)}$$

**Anomaly Detection:** Rank test snippet, η at scale s:

$$R_s(\eta) = \frac{1}{n}\sum_{j=1}^{n} I_{\{d_{x(j)}(s) > d_\eta(s)\}}$$

## 5. Experimental Results

First, an attempt was made to simulate real-life cases of digital video forensics by creating a dataset of videos captured by the user's mobile cameras. For this, a total of 220 videos of different geographical conditions were made in five months.

The proposed algorithm has been validated based on the created dataset, there is a total of 8 (Insertion, deletion, shuffle, frame rate, tempering, Transcoding, etc.) attacks were added to the video intentionally and analyze the histogram of a video frame that shows proposed algorithm detected the attack.

Figure 1 depicted a frame insertion attack on a video; figure 2 depicted how the proposed algorithm detect the attack well, note that the same video also suffered another 7 attacks at frames: 50, 100, 150, 200,300,350, and 400.

frame 199 New frame insert frame 201

Figure 1. Frame Insertion. A new frame is inserted within the 199 and 201 frame

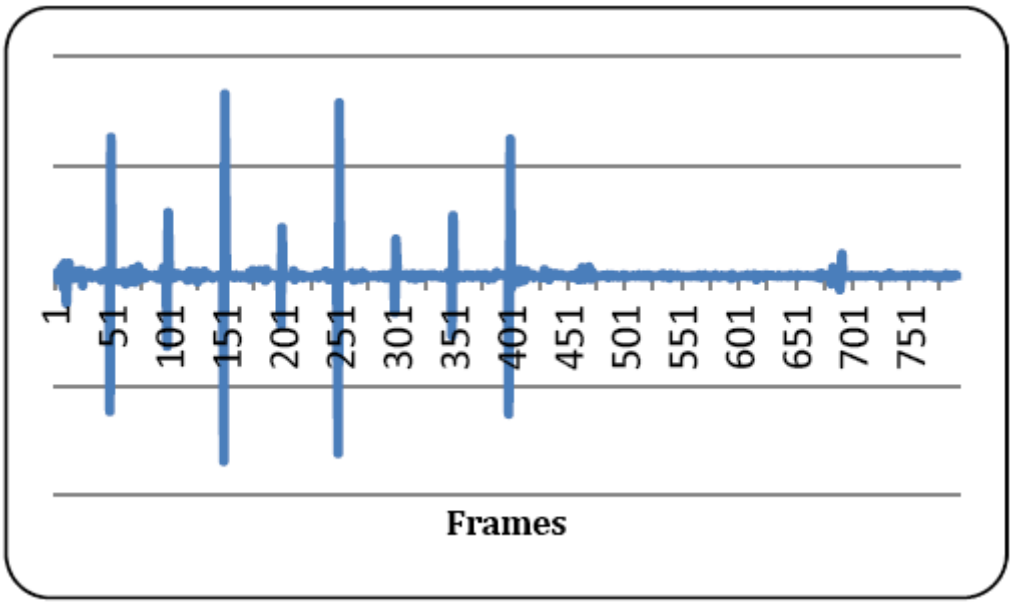


Figure 2 shows detecting frame insertion attacks at 250, other 7 created attacks at 50, 100, 150, 200,300,350, and 400 were also detected.

Figure 3 shows a twenty frames removal attack. Frames from 51 to frame 70 were removed; figure 4 shows how successfully the proposed algorithm detected this attack, note that the same video also suffered another 7 attacks.

frame 48 frame 51 frame 72

Figure 3. Frame removal. Frames from 51 to frame 72are deleted from the video sequence.

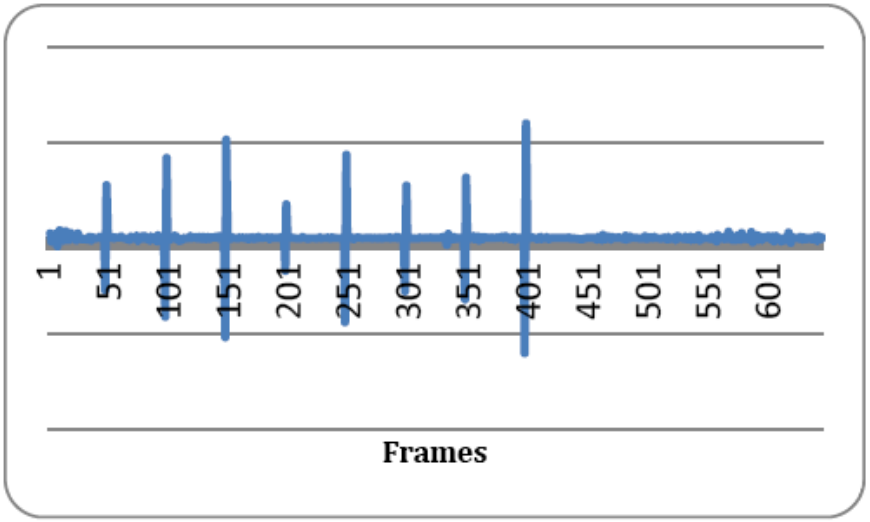


Figure 4. the proposed algorithm detecting frames removal attack at 50, other 7 created attacks at 100, 150, 200,250,300,350 and 400 were also successfully detected.

Figure 5 shows spatial tampering attack, the red car in the frame 100 was removed; figure 6 shows how successfully the proposed algorithm detected this attack, note that the same video also suffered another 7 attacks.

Figure 5. Spatial tampering. The red car in the frame 100 was removed.

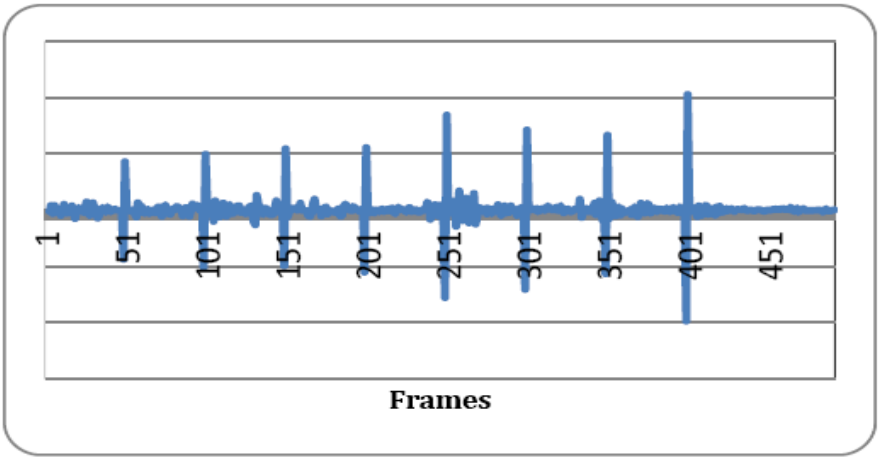


Figure 6. the proposed algorithm detecting spatial attack at frame 100, other 7 created attacks at 50, 150, 200,250,300,350 and 400 were also successfully detected.

Table 1: attack classification

| Name of Attack | No. of Video frames | No. of frame classify | Accuracy % |
|---|---|---|---|
| Non-Tempering | 6692 | 6691 | 99% |
| Frame Insertion | 61 | 59 | 96% |
| Frame Deletion | 45 | 43 | 95% |
| Tempering | 42 | 40 | 95% |

Table.1 shows the performance analysis of proposed algorithm for video authentication based on 22 videos, total 8 different attacks were added to each video intentionally. The classification accuracy for non-tempered video gives the 99%. For frame insertion and deletion of attack, a classification accuracy is 96% and 95% are obtained respectively. Only 2 frames are misclassified in tempered attack due to small region of spatial tempering. Overall classification accuracy level of proposed techniques is 96.25%

Table 2: Comparative analysis of proposed method with existing methods

| Name of Attack | Hala Bahjat et. al. [3] | Fadl SM et. al. [5] | Proposed Method |
|---|---|---|---|
| Frame Insertion | 80% | NA | 96% |
| Frame Deletion | 85% | 90% | 95% |
| Tempering | 90% | NA | 95% |

## 6. Conclusion

Digital signature and watermarking techniques are used in many applications and have some advantages and disadvantages. In this technique, additional information is inserted and removed from a video for video authentication. But this can only be done after video capture. It is not possible to implement watermark and digital signature techniques when capturing video.We have proposed a

robust technique for digital video authentication, which tests the user's usage on different videos captured from 3 cameras and 2 mobile phones. This technique has developed a reliable technique for video authentication using local video information and the results have been proven to be good. The accuracy of the proposed algorithm is shown to be 96.25%.

## References


1) B. C. Hosler, X. Zhao, O. Mayer, C. Chen, J. A. Shackleford and M. C. Stamm, "The Video Authentication and Camera Identification Database: A New Database for Video Forensics," in IEEE Access, vol. 7, pp. 76937-76948, 2019, doi: 10.1109/ACCESS.2019.2922145.
2) W. Diffie and M. E. Hellman, “New Directions in cryptography”, IEEE Trans. On Information Theory, Vol. 22, No. 6, pp.644-654, Nov 1976.
3) Hala Bahjat Abdulwahab, Khaldoun L. Hameed and Nawaf Hazim Barnouti, “Video Authentication using PLEXUS Method” International Journal of Advanced Computer Science and Applications(IJACSA), 9(11), 2018. http://dx.doi.org/10.14569/IJACSA.2018.0911104.
4) M. S. Zareen, A. Waqar and B. Aslam, "Digital forensics: Latest challenges and response," Information Assurance (NCIA), 2013 2nd National Conference on, Rawalpindi, pp. 21-29, 2013.
5) Fadl SM, Han Q, Li Q. Authentication of Surveillance Videos: Detecting Frame Duplication Based on Residual Frame. J Forensic Sci. 2018 Jul;63(4):1099-1109. doi: 10.1111/1556-4029.13658. Epub 2017 Oct 16. PMID: 29044501.
6) Akumba, B. , Iorliam, A. , Agber, S. , Okube, E. and Kwaghtyo, K. (2021) Authentication of Video Evidence for Forensic Investigation: A Case of Nigeria. Journal of Information Security, 12, 163-176. doi: 10.4236/jis.2021.122008.
7) A. Gupta, S. Gupta and A. Mehra, "Video authentication in digital forensic," Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference on, Noida, pp. 659-663, 2015.
8) S. Upadhyay and S. K. Singh, "Learning based video authentication using statistical local information," Image Information Processing (ICIIP), 2011 International Conference on, Himachal Pradesh, pp. 1-6 , 2011.
9) A. Gironi, M. Fontani, T. Bianchi, A. Piva and M. Barni, "A video forensic technique for detecting frame deletion and insertion," 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, pp. 6226-6230, 2014.
10) Chhaya S Gosavi and Suresh N Mali. Article: Video Authentication and Copyright Protection using Unique Watermark Generation Technique and Singular Value Decomposition. International Journal of Computer Applications 123(3):1-5, August 2015.
11) Jian Liu and Xiangjian He, "A Review Study on Digital Watermarking," 2005 International Conference on Information and Communication Technologies, pp. 337-341. 2005.
12) S. Upadhyay and S. K. Singh, “Video Authentication- An Overview”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.
13) Y. J. Ren, L. O'Gorman, L. J. Wu, F. Chang, T. L. Wood and J. R. Zhang, "Authenticating Lossy Surveillance Video," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 10, pp. 1678-1687, Oct. 2013, doi: 10.1109/TIFS.2013.2279542.
14) Mahbuba Begum, Mohammad Shorif Uddin, "Analysis of Digital Image Watermarking Techniques through Hybrid Methods", Advances in Multimedia, vol. 2020, Article ID 7912690, 12 pages, 2020. https://doi.org/10.1155/2020/7912690
15) J. A. Bloom, I. J. Cox, T. Kalker, J. P. M. G. Linnartz, M. L. Miller, and C. B. S. Traw, “Copy protection of DVD video”, Proceeding of the IEEE, vol. 87, pp. 1267-1276, (1999).
16) T. Kalker, G. Depovere, J. Haitsma, M. Maes, “A video watermarking system for broadcast monitoring”, proceedings of the SPIE, vol. 3657, pp. 103-112, (1999).
17) Digimarc Company Website: http://www.digimarc.com
18) H. Zhi-yu and T. Xiang-hong, "Integrity authentication scheme of color video based on the fragile watermarking," 2011 International Conference on Electronics, Communications and Control (ICECC), Ningbo, 2011, pp. 4354-4358, doi: 10.1109/ICECC.2011.6067709.

19) Avinash P. Wadhe and Dr. Asha Ambhaikar, "Critical Analysis Of Digital Video Authentication Based On Various Techniques" 2021 International E- Conference on computing and data science ,IPEM Ghaziabad India, ISSN: 0011-9342, Issue: 8, Pages: 1619- 1629

**Author Profile 1:**

Prof. Avinash P. Wadhe: Received the B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently Pursuing full time PhD (CSE) at Kalinga University ,Raipur (Chattisgarh) India. His research interest include Digital Forensics, Network Security, Data mining and Cloud Computing .He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference.

**Author Profile 2:**

Dr. Prof. Asha Ambhaikar is B.E, M.Tech. & Ph.D. in Computer Science and Engineering. At present she is working as a Professor (CSE) & Dean Students Welfare, Kalinga University Naya Raipur. India. She has 28 years of Academic experience. She has published more than 105 research papers in reputed national and international Journals (Scopus Indexed & SCI), 434 Google citations and a patent. She is a member of Editorial Board and Reviewer of various international journals and conferences. She is also the member of various professional societies like life member of IAENG (International Association of Engineers, Hong Kong, IEEE, Indian Society of Technical Education (ISTE), Computer Society of India (CSI), IET, ASDF, Computer Science Teachers Association (CSTA), and Association for Computing Machinery (ACM), New York, USA, IACSIT (International Association of Computer Science and Information Technology, Singapore. Member of SDIWC (The Society of Digital Information and Wireless Communication, USA. She has also chaired various National and International Conferences around various countries as a keynote speaker. She has also published 06 books by Lambert Publication, Germany.