

Authentication of Video Evidence for Forensic Investigation: A Case of Nigeria

Beatrice O. Akumba*, Aamo Iorliam*, Selumun Agber,
Emmanuel Odeh Okube, Kenneth Dekera Kwaghtyo

Department of Mathematics & Computer Science, BSU, Makurdi, Nigeria

Email: *beatriceakumba@gmail.com, *aamoiorliam@gmail.com

How to cite this paper: Akumba, B.O., Iorliam, A., Agber, S., Okube, E.O. and Kwaghtyo, K.D. (2021) Authentication of Video Evidence for Forensic Investigation: A Case of Nigeria. *Journal of Information Security*, 12, 163-176.

<https://doi.org/10.4236/jis.2021.122008>

Received: March 12, 2021

Accepted: April 26, 2021

Published: April 29, 2021

Copyright © 2021 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

Video shreds of evidence are usually admissible in the court of law all over the world. However, individuals manipulate these videos to either defame or incriminate innocent people. Others indulge in video tampering to falsely escape the wrath of the law against misconducts. One way impostors can forge these videos is through inter-frame video forgery. Thus, the integrity of such videos is under threat. This is because these digital forgeries seriously debase the credibility of video contents as being definite records of events. This leads to an increasing concern about the trustworthiness of video contents. Hence, it continues to affect the social and legal system, forensic investigations, intelligence services, and security and surveillance systems as the case may be. The problem of inter-frame video forgery is increasingly spontaneous as more video-editing software continues to emerge. These video editing tools can easily manipulate videos without leaving obvious traces and these tampered videos become viral. Alarmingly, even the beginner users of these editing tools can alter the contents of digital videos in a manner that renders them practically indistinguishable from the original content by mere observations. This paper, however, leveraged on the concept of correlation coefficients to produce a more elaborate and reliable inter-frame video detection to aid forensic investigations, especially in Nigeria. The model employed the use of the idea of a threshold to efficiently distinguish forged videos from authentic videos. A benchmark and locally manipulated video datasets were used to evaluate the proposed model. Experimentally, our approach performed better than the existing methods. The overall accuracy for all the evaluation metrics such as accuracy, recall, precision and F1-score was 100%. The proposed method implemented in the MATLAB programming language has proven to effectively detect inter-frame forgeries.

Keywords

Inter-Frame, Video Forgery, Correlation Coefficients, Forensic Investigation,

Threshold

1. Introduction

Video forgeries continue to be a great challenge to the admissibility of video evidence in the court of law, especially in Nigeria.

Due to the rapid increase in highly sophisticated video-editing software and video tampering techniques, there are several kinds of tampering techniques such as splicing, resampling, adding and or removing a portion from a video clip to mention but a few [1]. Inter-frame video forgery is the removal or insertion of a set of frames from or into a video [2]. Such practices affect the sequence of frames in a video. But video editing tools such as Adobe Premiere and Pinnacle Studio make video forgeries easier. Thus, causing serious threats, defaming and reducing the credibility of digital contents. Considering that videos can be used as evidence in the court of law or as news items, there is a need for authentication of these videos. Therefore, it has become imperative to carry out more research in the exploration for better ways to avert the bothersome level of digital video content manipulations. With very few forensic experts in Nigeria tasked with the huge responsibility of authenticating videos for forensic purposes, there is a need to develop novel approaches to tackle video forgeries.

Thus, this paper proposes a novel inter-frame video forgery detection method based on adjacent frames and has effectively detected video forgeries for forensic purposes. The rest of the paper is organised as follows. Related works are described in Section 2. Section 3 explains the materials and methods. Results and discussion are presented and discussed in Section 4. Conclusion and future work are presented in Section 5.

2. Related Works

Considerably, many forensics techniques have been proposed. Chao, Jiang and Sun [3], developed an inter-frame video forgery detection model using Lucas Kanade optical flow. The model used window based and binary search based detection for frame inserted forgery detection. A double adaptive threshold was used to detect the differences in the optical flow. The model achieved 95% recall and 98% precision evaluation results. Frame deleted forgery detection achieved 85% and 89% recall and precision, respectively.

Wang, Li, Zhang and Ma [4], leveraged on the concept of the consistency of correlation coefficients to classify inter-frame video tampered videos from original videos. The model employed the use of a support vector machine (SVM) in the classification process. The experimental setting used five datasets: one original and four tampered video datasets. The results of the experimenting model returned an overall accuracy of 98.79% for classifying both inserted and deleted frames.

Wu, Jiang, Sun and Wang [2], proposed a model using the consistency of velocity field for detecting frame deletion and duplication forgeries. The model adopted the use of the Extreme Studentized Deviate (ESD) test to extract the peaks or locate tampered regions in a given video and then determine the forgery type. The experimental results only considered when a video was manipulated or not and the model achieved an overall accuracy of 96.3%. But the accuracy dropped to 90%, 85% and 80% for detecting original, frame deleted and frame duplicated videos, respectively when been specific.

Zheng, Sun, and Shi [5], proposed the Block-wise Brightness Variance Descriptor (BBVD) method for inter-frame video detection. The method was evaluated using a dataset that constitutes 240 original and manipulated videos. From the experimental results, the frame inserted forgery achieved a recall value of 98.67% and 94.09% precision. To locate the actual region manipulated, the model achieved 89.23% and 79.45% for recall and precision.

Li, Zhang, Guo and Wang [6], leveraged on the consistency of Quotient of Mean Structural Similarity (QoMSSIM) for video forgery detection. The framework used the SVM technique to classify videos into original and inter-frame tampered videos. The model was evaluated using the Shanghai Jiao Tong University dataset containing: 25 frames-inserted videos, 25 frames-deleted videos, 100 frames-inserted videos and 100 frames-deleted videos. Results of the experiment showed that the framework yielded high accuracy of the classification and low computation complexity features.

Kingra, Aggarwal and Singh [7], proposed a framework for inter-frame forgery detection in videos. The inconsistencies of residual and optical flow detected frame insertion, removal and duplication in video datasets. Experimental results demonstrated that the model detected and located forgery with an accuracy of 83% and 80%, respectively.

Liu and Huang [8], implemented a novel inter-frame video forgery detection algorithm using Zernike opponent chromaticity moments and coarseness feature analysis. The model was tested using Surrey University Library for Forensic Analysis (SULFA), and manually captured videos using Canon IXUS 220HS and SONY DSC-P10 digital cameras. Results showed that the algorithm can detect all kinds of inter-frame forgeries with high accuracy and efficiency.

Aghamaleki and Behrad [9], leveraged on the spatial and time-domain analysis of quantization effect and developed a novel framework for forgery detection in MPEG videos. The model distinguished video segments into single compressed videos, double compressed videos without malicious tampering and double compressed videos with malicious tampering using a decision fusion algorithm. The algorithm when tested with a large dataset produced an accuracy of 83.39% and 88.6% on a reduced dataset.

Fadl, Han and Li [10], developed a framework for detecting three kinds of inter-frame forgeries. The SULFA, LASIESTA, and IVY LAB datasets were used to evaluate the model. The datasets comprised of 150 original, 132 duplicated, 53

inserted frames, and 125 deleted frames of videos. Results from the experiments showed that the model achieved a promising performance of 0.97 F1-score (that is 97% accuracy).

Leveraging on similarity analysis, Zhao, Wang and Lu [11], developed the passive-blind model for inter-frame forgery detection. 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 at that time.

Bakas, Bashaboina and Naskar [12], proposed a forensic approach to tackle double compression detection and localization. The algorithm used a convolutional neural network (CNN) approach for the detection process. The model was tested on 20 YUV sequences in CIF of size 352×288 format from the video TRACE library. From the experimental results, the method achieved 90% and 70% average accuracy for detecting manipulations and localization accuracy, respectively.

Sitara and Mehtre [13], proposed an inter-frame forgery detection algorithm based on tamper traces from Spatio-temporal and compressed domains. The evaluation was done using a dataset containing 23,586 videos which comprised of inter-frame video forgeries like insertion, deletion, duplication, and shuffling. Evaluation results demonstrated that the model outperforms other methods especially the inter-frame shuffling detection at that time.

Selected Cases of Video Evidence/Manipulations in Nigeria

In 2013, a video of a lecturer at Delta State University, Abraka, went viral. In the clip, the female student tactically captured the lecturer naked. Sources revealed that the lecturer had failed the female student in the second year for rejecting his sexual request. Until in the final year, the lecturer insisted on having sex with her first, so she cajoled him to her apartment, and captured him naked to serve as evidence [14].

A video went viral in 2018, indicating a scenario where a governor was receiving what was tagged a “kickback” meaning a return bribe from a contractor. The video showed that the governor received bundles of dollars from the contractor. In the video, the governor had requested 5 million US dollars from the contractor who recorded the video while handing in part of the payment. Most evidently, the uploaded version of the video was without audio content. Seemingly to conceal some details [15].

Again, Mwai [16], confirmed another misleading video clip during the End SARS protest in Nigeria where a video clip circulated on the Internet showing one of the President’s advisers, Femi Adesina, apparently describing the protest as a mere “child’s play”. Interpretations indicated that the adviser was abusing the protesters. But the video was an old one and was edited out of context having nothing to do with the End SARS protest.

Even though the Nigerian Constitution Section 84 (1) of the Evidence Act

2011, provides room for admissibility of computer-generated evidence in the court of law, such evidence must satisfy subsection (2).

This calls for forensic experts to devise techniques or means of authenticating digital contents to restore the lost trust in digitally generated contents [17].

3. Materials and Methods

Two datasets are used in this experiment. The first dataset is from VIFFD [18]. The dataset contains a total of 120 videos. The dataset has 30 original videos, 30 duplicated forgery, 30 deletion forgery, and 30 insertion forgery videos. For this experiment, we tested our algorithm on 30 original videos, 30 deletion forgery and 30 insertion forgery videos. The second dataset used for this study was locally developed and can be accessed at <http://bit.ly/3v6o1ZS>. The data consists of 10 original or authentic videos and 10 tampered videos by insertion, and 10 tampered videos by deletion.

The proposed method is achieved by applying the algorithm as shown below:

- 1) Read video input (tampered and original);
- 2) Extract frames from the original and tampered video;
- 3) Convert the frames to grayscale;
- 4) Calculate the inter-frame correlation coefficients between adjacent frames;
- 5) Calculate the mean of correlation difference;
- 6) Calculate the standard deviation of correlation difference;
- 7) Calculate the three-sigma rule to achieve the upper bound and lower bound in the distribution;
- 7) Classify videos based on the correlations of inter-frame coefficients using the threshold explained in Equation (1).

$$f(l) \begin{cases} M, & \text{if } \text{no}(\{f(l_i)\}) = M \\ & i = 1, 2, \dots, n \\ & \geq tdb \\ & \# \\ N, & \text{otherwise} \end{cases} \quad (1)$$

where: $f(l)$ = frame label;

M = Manipulation due to deletion/insertion;

N = Normal or original video;

$\text{no}(\{f(l)\})$ = number of deleted/inserted frames;

tdb = threshold to determine insertion/deletion vs normal frames. In our case, the tdb is set to 3.4.

4. Results and Discussion

The benchmark tests/results are carried out using VIFFD—A dataset for detecting video inter-frame forgeries (Nguyen, and Hu, 2020). This serves as a benchmark/standard upon which the locally manipulated videos were measured. Our source code was written in MATLAB and can be downloaded from

<https://github.com/OkubeEmmanuel/Video-forgery-detection>.

4.1. Evaluation Metrics Used

This study adopts the use of Recall, Precision, Accuracy, F₁-score and Confusion Matrix for evaluation. This is necessary to ascertain the effectiveness and efficiency of the proposed approach over other existing state-of-the-art approaches. The formulae for each of the evaluation measures are given as follows:

$$\text{Recall: } R = \frac{TP}{TP + FN};$$

$$\text{Precision: } P = \frac{TP}{TP + FP};$$

$$\text{Accuracy: } A = \frac{TP + TN}{TP + FP + FN + TN};$$

$$\text{F}_1\text{-Score: } = 2 \times \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}}.$$

where:

- 1) TP (True Positive) is the test result that defines a given condition exists, when it does;
- 2) TN (True Negative) defines that a condition does not take place when it does not;
- 3) FP (False Positive) is a test result that a given condition exists, when it does not;
- 4) FN (False Negative) defines that a condition does not take place when it does.

4.2. Detection Performance of Original, Frame Inserted and Frame Deleted Videos Using the Benchmark Datasets

Figure 1 shows the frames extracted from the benchmark original video.

The correlation coefficients of the benchmark original videos in **Figure 1** are as shown in **Figure 2**.

We observe that the differences in the frames are stable, hence the correlation coefficients of the benchmark original frames are consistent as shown in **Figure 2**.

4.2.1. Frame Inserted—Benchmark Result

Figure 3 and **Figure 4** depict the benchmark results for insertion forgery.

The inconsistency in the frames based on frame insertion are detected and



Figure 1. Frames from the benchmark original video.

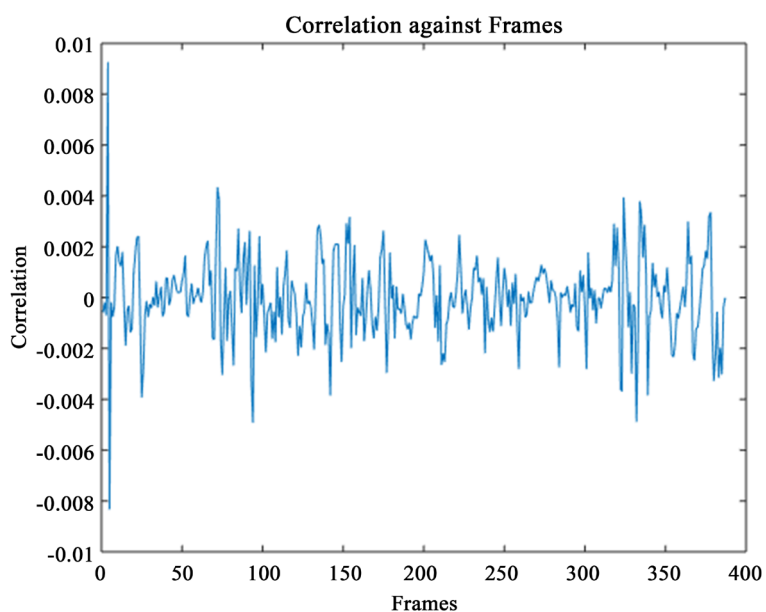


Figure 2. Correlation coefficients of the benchmark original video result.

1st Frame in Tampered Sequence 2nd Frame in Tampered Sequence



3rd Frame in Tampered Sequence 4th Frame in Tampered Sequence



Figure 3. Frames from the frame inserted video-benchmark result.

shown in **Figure 3**. Its correlation coefficients is shown in **Figure 4**.

Figure 4 validates the claim that a frame was inserted at a location around frames 70 and 80 as detected in **Figure 3**.

4.2.2. Frame Deleted—Benchmark Result

Figure 5 and **Figure 6** shows the benchmark results for deletion forgery.

In **Figure 5**, the inconsistency occurred in the first frame. The frame containing the picture of a person was removed.

Figure 6 shows spikes between frames 20 and 40, indicating the deletion of the frame.

The confusion matrix for the original video and insertion/deletion video is as shown in **Figure 7**.

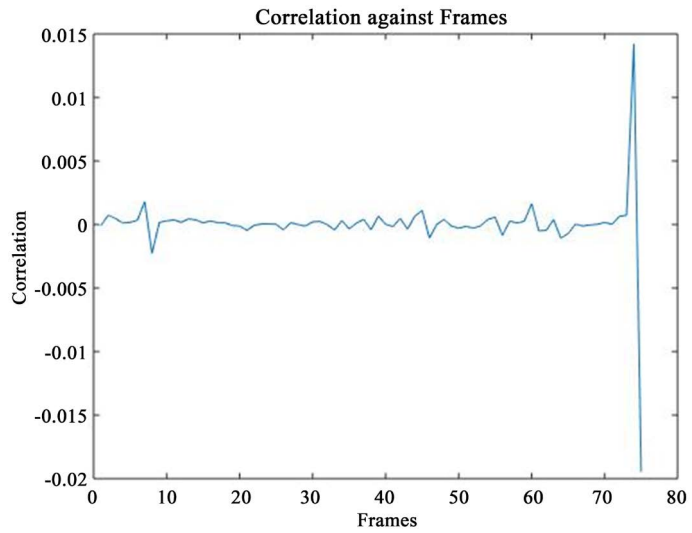


Figure 4. Correlation coefficients of the frame insertion-benchmark result.

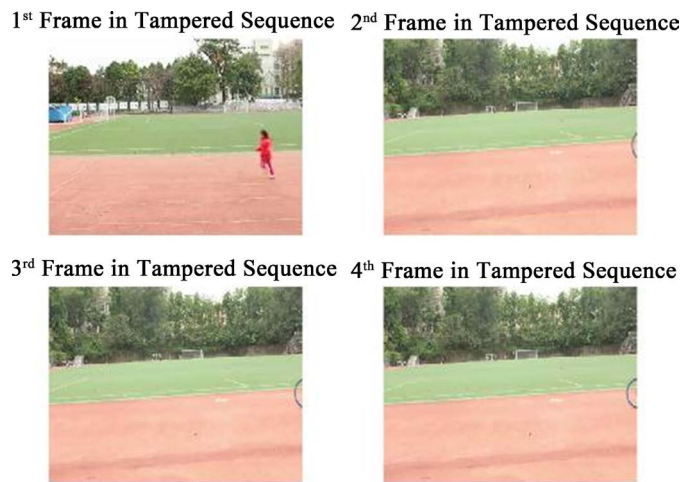


Figure 5. Frames from the frame deleted video-benchmark result.

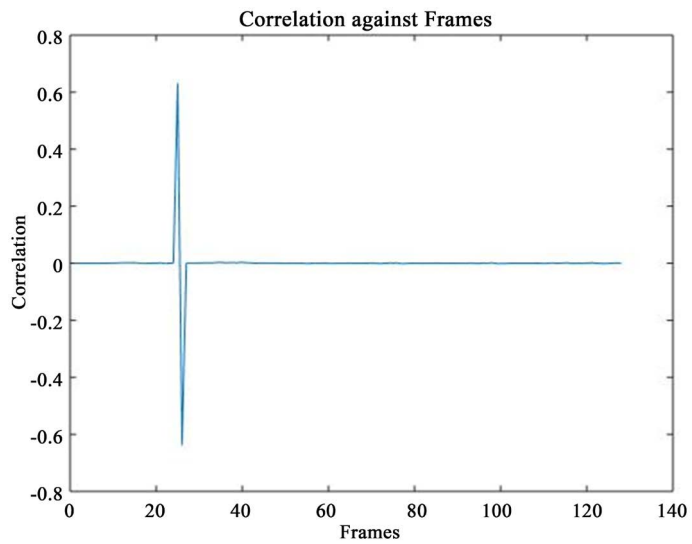


Figure 6. Correlation coefficients of the frame deleted-benchmark result.

Confusion Matrix

Output Class	0	1	0	1	0	1
	0	1	0	1	0	1
	0	1	0	1	0	1
			0	1	Target Class	

Detailed description of Figure 7: A 3x3 confusion matrix. The top two rows represent Output Class 0 and 1. The bottom row represents Target Class 0 and 1. The columns represent Target Class 0 and 1. The cells contain counts and percentages. The top-left cell (0,0) has a count of 1 (50.0%) and is green. The top-middle cell (0,1) has a count of 0 (0.0%) and is red. The middle-left cell (1,0) has a count of 0 (0.0%) and is red. The middle-right cell (1,1) has a count of 1 (50.0%) and is green. The bottom-left cell (2,0) has 100% (0.0%) in green and red. The bottom-middle cell (2,1) has 100% (0.0%) in green and red. The bottom-right cell (2,2) has 100% (0.0%) in green and red.

Figure 7. Confusion matrix for the original vs insertion/deletion video.

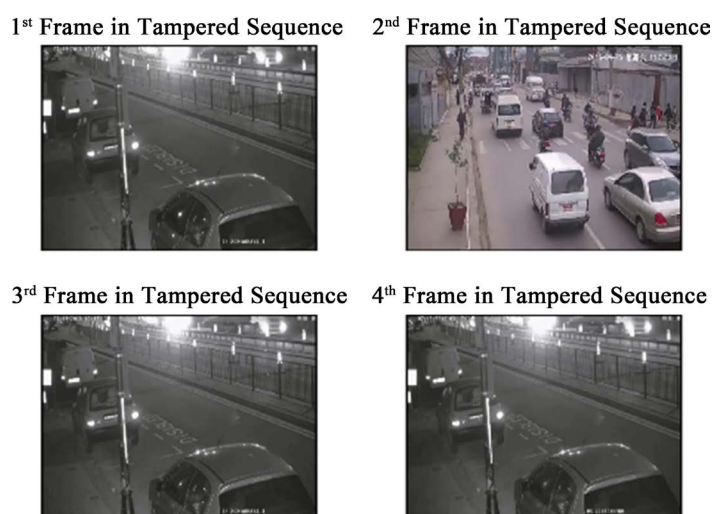


Figure 8. Discontinuous frames from frame inserted video.

The above results all achieved 100% accuracy as shown in **Figure 7**.

4.3. Detection Performance of Frame Inserted and Frame Deleted Videos Using the Locally Made Datasets

4.3.1. Frame Inserted Results—Locally Made Datasets

Usually, the frame inserted videos are discontinuous and inconsistent. The following four frames in **Figure 8** depict this scenario.

From **Figure 8**, the second frame which is at the top right corner shows the discontinuity/inconsistency of a frame inserted in the video.

The correlation coefficients of the detected frame inserted video are shown in **Figure 9**.

In **Figure 9**, the differences in the frames are noticeably unstable and inconsistent. The region between frames 80 and 100 indicates the point at which a frame was introduced, added or inserted into the original video data. Thus, the changes in the correlation coefficients suddenly rise to the peak at the point a frame was inserted.

4.3.2. Frame Deleted Results—Locally Made Datasets

In the frame deleted video data as shown in **Figure 10**, the changes in the frames are not as obvious as in the frame inserted video forgery. However, the inconsistency in the correlation coefficients of the frame deleted video data detects and

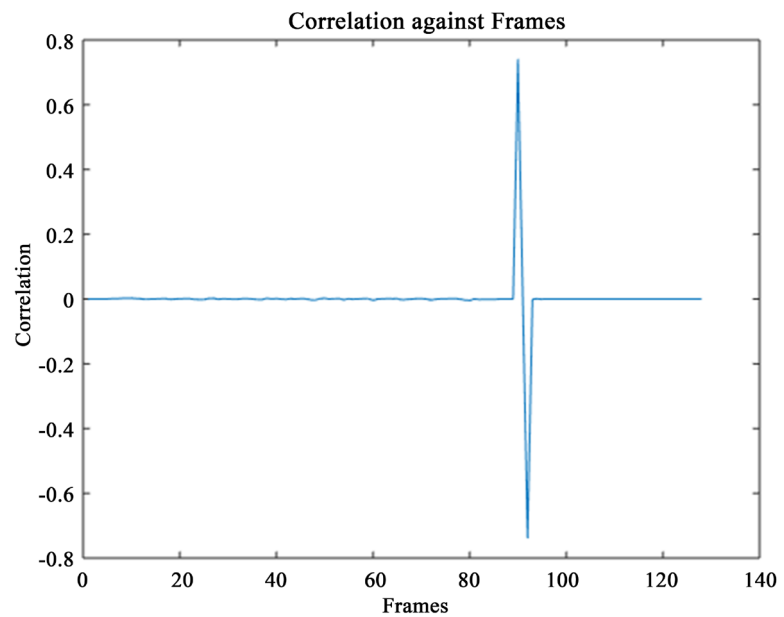


Figure 9. Correlation coefficients of a frame inserted video.

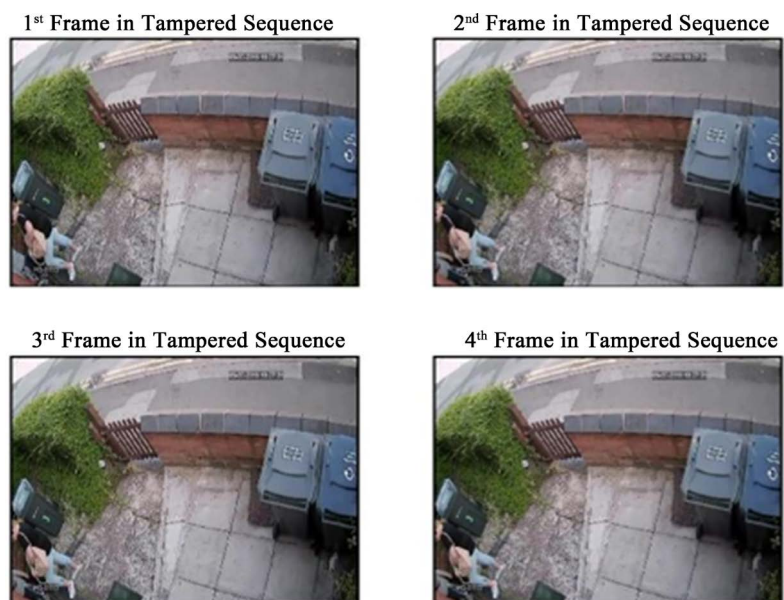


Figure 10. Discontinuous frames from frame deleted video.

indicates frame deleted forgery.

The correlation coefficients of the frame deleted video are as shown in **Figure 11**.

From **Figure 11**, the inconsistency became obvious at a point between frames 200 and 300. The spikes at this point became very high. Hence, this indicates the point at which a frame was deleted or cut off from the original video data.

4.4. Detection Performance for Deletion Forgery

The confusion matrix in **Figure 12** shows the result for 3 original videos and 3

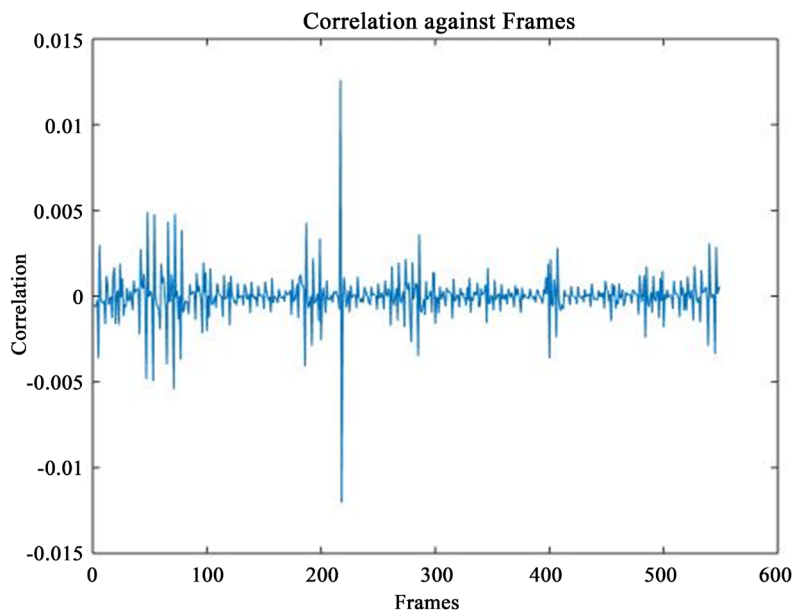


Figure 11. Correlation coefficients of a frame deleted video.

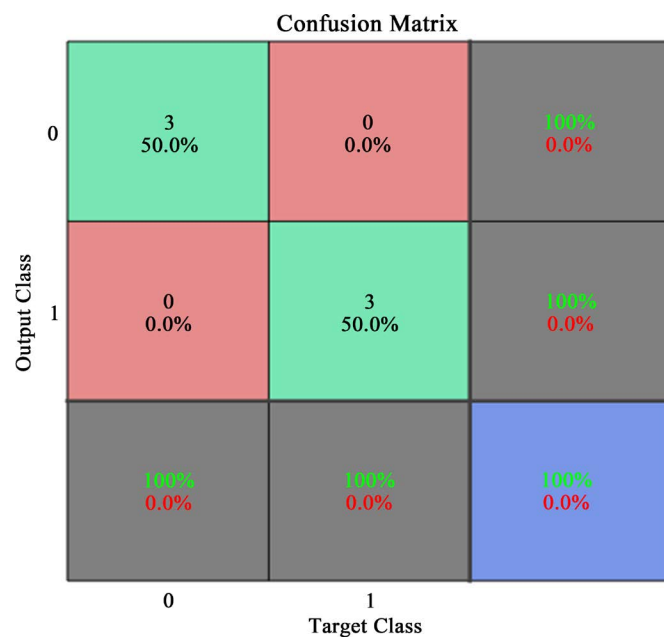


Figure 12. Confusion matrix for original vs deletion forgery.

deletion videos detection performance.

From the confusion matrix in **Figure 12**, all the deleted frames are detected with an overall accuracy of 100%.

Table 1 compares our proposed model with other similar research works based on recall, precision, accuracy and F1-score for deletion detection.

From the comparison, we observed that our proposed model outperformed the previous closely related deletion detection methods.

This means that our proposed method can effectively assist law enforcement agencies in Nigeria to investigate and authenticate videos that could be presented and used in the court of law especially when checking for deletion forgeries detection.

4.5. Detection Performance for Insertion Forgery

For insertion forgery detection, the confusion matrix is shown in **Figure 13** for 3 original videos and 4 insertion videos.

From **Figure 13**, it can be observed that the overall accuracy of the model returned 100% accuracy.

Table 1. Comparative analysis for detection performance of deletion forgery.

Method	Recall	Precision	Accuracy	F1-score
Wang <i>et al.</i> [4]	-	-	97.27% (0.9729)	-
Chao <i>et al.</i> [3]	85.67% (0.8567)	89.39% (0.8939)	-	-
Liu, and Huang [8]	0.95 (95%)	0.93 (93%)	-	0.94 (94%)
Our proposed method	1.00 (100%)	1.00 (100%)	100.00 (100%)	1.00 (100%)

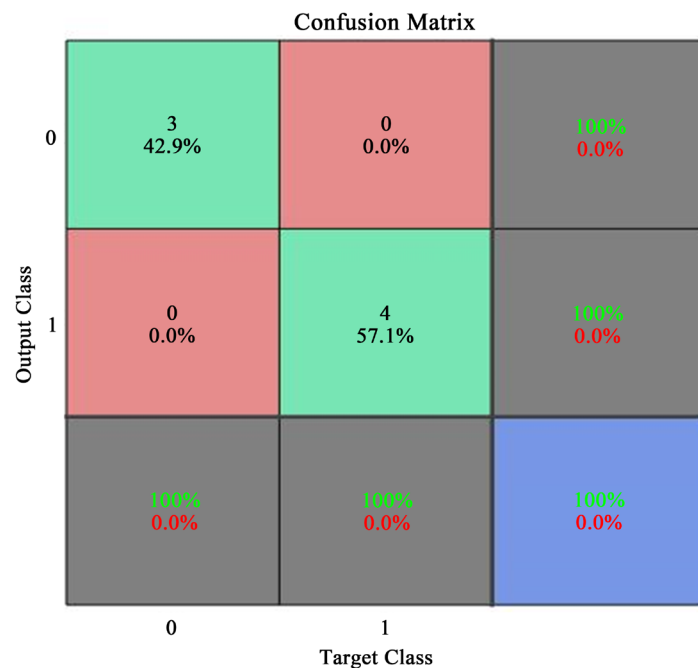


Figure 13. Confusion matrix for original vs insertion forgery.

Table 2 compares our results with the existing works based on insertion forgery detection. For comparison, it is shown that our proposed method outperformed the existing methods. Therefore, our proposed method can assist law enforcement agencies in Nigeria to authenticate videos for forensic purposes especially when checking for insertion forgeries.

Table 2. Comparative analysis for detection performance of insertion forgery.

Method	Recall	Precision	Accuracy	F1-score
Wang <i>et al.</i> [4]	-	-	99.34% (0.9934)	-
Chao <i>et al.</i> [3]	95% (0.9500)	98% (0.9800)	-	-
Liu, and Huang [8]	0.97 (97%)	0.96 (96%)	-	0.96 (96%)
Our proposed method	1.00 (100%)	1.00 (100%)	100.00 (100%)	1.00 (100%)

5. Conclusion and Future Work

This study leveraged on the consistency of correlation coefficients. Hence, classified original videos and tampered videos. The model adopts the use of the threshold technique for effective detection. The model demonstrates a simple but powerful process of verifying the authenticity of inter-frame video forgeries.

With this approach, digital contents associated with frame insertion or deletion in situations like the recent End SARS protest in Nigeria can be detected to ascertain their originality. That is, the model can detect whether a digital video on social media is genuine or not without prior knowledge of the original video data. Experimental results using the VIFFD and our locally manipulated video data indicate that the proposed model performed better than the existing methods. The overall accuracy for all the evaluation metrics such as recall, precision and F1-score achieved 100% accuracy.

In our future work, we plan to investigate the detection of more video forgeries using our proposed model. Additionally, machine learning techniques will be adopted to detect more video forgeries.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

- [1] Iorliam, A. (2016) Application of Power Laws to Biometrics, Forensics and Network Traffic Analysis. Doctoral Dissertation, University of Surrey, Guildford.
- [2] Wu, Y., Jiang, X., Sun, T. and Wang, W. (2014) Exposing Video Inter-Frame Forgery Based on Velocity Field Consistency. 2014 *IEEE International Conference on Acoustics, Speech and Signal Processing*, Florence, 4-9 May 2014, 2674-2678. <https://doi.org/10.1109/ICASSP.2014.6854085>
- [3] Chao, J., Jiang, X. and Sun, T. (2012) A Novel Video Inter-Frame Forgery Model Detection Scheme Based on Optical Flow Consistency. *International Workshop on*

- Digital Watermarking*, Shanghai, 31 October-3 November 2012, 267-281.
https://doi.org/10.1007/978-3-642-40099-5_22
- [4] Wang, Q., Li, Z., Zhang, Z. and Ma, Q. (2014) Video Inter-Frame Forgery Identification Based on the Consistency of Correlation Coefficients of Grey Values. *Journal of Computer and Communications*, **2**, 51-57. <https://doi.org/10.4236/jcc.2014.24008>
- [5] Zheng, L., Sun, T. and Shi, Y.Q. (2014) Inter-Frame Video Forgery Detection Based on Block-Wise Brightness Variance Descriptor. *International Workshop on Digital Watermarking*, Taipei, 1-4 October, 18-30.
https://doi.org/10.1007/978-3-319-19321-2_2
- [6] Li, Z., Zhang, Z., Guo, S. and Wang, J. (2016) Video Inter-Frame Forgery Identification Based on the Consistency of Quotient of MSSIM. *Security and Communication Networks*, **9**, 4548-4556. <https://doi.org/10.1002/sec.1648>
- [7] Kingra, S., Aggarwal, N. and Singh, R.D. (2017) Inter-Frame Forgery Detection in H. 264 Videos Using Motion and Brightness Gradients. *Multimedia Tools and Applications*, **76**, 25767-25786. <https://doi.org/10.1007/s11042-017-4762-2>
- [8] Liu, Y. and Huang, T. (2017) Exposing Video Inter-Frame Forgery by Zernike Opponent Chromaticity Moments and Coarseness Analysis. *Multimedia Systems*, **23**, 223-238. <https://doi.org/10.1007/s00530-015-0478-1>
- [9] Aghamaleki, J.A. and Behrad, A. (2017) Malicious Inter-Frame Video Tampering Detection in MPEG Videos Using Time and Spatial Domain Analysis of Quantization Effects. *Multimedia Tools and Applications*, **76**, 20691-20717.
<https://doi.org/10.1007/s11042-016-4004-z>
- [10] Fadl, S.M., Han, Q. and Li, Q. (2018) Inter-Frame Forgery Detection Based on Differential Energy of Residue. *IET Image Processing*, **13**, 522-528.
<https://doi.org/10.1049/iet-ipr.2018.5068>
- [11] Zhao, D.N., Wang, R.K. and Lu, Z.M. (2018) Inter-Frame Passive-Blind Forgery Detection for Video Shot Based on Similarity Analysis. *Multimedia Tools and Applications*, **77**, 25389-25408. <https://doi.org/10.1007/s11042-018-5791-1>
- [12] Bakas, J., Bashaboina, A.K. and Naskar, R. (2018) MPEG Double Compression Based Intra-Frame Video Forgery Detection using CNN. 2018 *International Conference on Information Technology*, Bhubaneswar, 19-21 December 2018, 221-226.
<https://doi.org/10.1109/ICIT.2018.00053>
- [13] Sitara, K. and Mehtre, B.M. (2018) Detection of Inter-Frame Forgeries in Digital Videos. *Forensic Science International*, **289**, 186-206.
<https://doi.org/10.1016/j.forsciint.2018.04.056>
- [14] Edafioka, L. (2016) An Unspoken Menace: Sexual Harassment in Nigerian Universities.
<https://wildaf-ao.org/index.php/en/woman-news/news/312-an-unspoken-menace-sexual-harassment-in-nigerian-universities>
- [15] Abdulaziz, A. (2019) Kano Govt Revokes Contracts of the Contractor Who Filmed Ganduje Bribe Videos.
<https://www.premiumtimesng.com/news/headlines/306538-kano-govt-revokes-contracts-of-contractor-who-filmed-ganduje-bribe-videos.html>
- [16] Mwai, P. (2020) Nigeria Sars Protest: The Misinformation Circulating Online. BBC Reality Check. <https://www.bbc.com/news/world-africa-54628292>
- [17] Anyebe, P.A. (2019) Appraisal of Admissibility of Electronic Evidence in Legal Proceedings in Nigeria. *Journal of Law, Policy and Globalization*, **92**, 1-12.
- [18] Nguyen, X.H. and Hu, Y. (2020) VIFFD—A Dataset for Detecting Video Inter-Frame Forgeries. Vision 6, Mendeley Data.