International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

Video Forgery Detection: A Comprehensive Study of Inter and Intra Frame Forgery With Comparison of State-Of-Art

Sumaiya Shaikh[1], Sathish Kumar Kannaiah[2]
[1]Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram, Vijayawada, AP, India
sumiyashaikh@gmail.com
[2]Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram, Vijayawada, AP, India.
Sathish1980@gmail.com

Abstract— Availability of sophisticated and low-cost smart phones, digital cameras, camcorders, surveillance CCTV cameras are extensively used to create videos in our daily life. The prevalence of video sharing techniques presently available in the market are: YouTube, Facebook, Instagram, snapchat and many more are in utilization to share the information related to videos. Besides this, there are many software which can edit the content of video: Window Movie Maker, Video Editor, Adobe Photoshop etc., with this available software anyone can edit the video content which is called as "Forgery" if edited content is harmful. Usually, videos play a vital role in terms of proof in crime scene. The Victim is judged by the proof submitted by the lawyer to the court. Many such cases have evidenced that the video being submitted as proof is been forged. Checking the authentication of the video is most important before submitting as proof. There has been a rapid development in deep learning techniques which have created deepfake videos where faces are replaced with other faces which strongly made a belief of saying "Seeing is no longer believing". The available software which can morph the faces are FakeApp, FaceSwap etc., the increased technology really made the Authentication of proofs very doubtful and un-trusty which are not accepted as proof without proper validation of the video. The survey gives the methods that are capable of accurately computing the videos and analyses to detect different kinds of forgeries. It has revealed that most of the existing methods are relying on number of tampered frames. The proposed techniques are with compression, double compression codec videos where research is being carried out from 2016 to present. This paper gives the comprehensive study of techniques, algorithms and applications designed and developed to detect forgery in videos.

Keywords- Digital Forensic, Inter Frame Forgery, Intra Frame Forgery, Video Forgery Detection, Video Surveillance, Intra Frame Forgery.

I. INTRODUCTION

Everyday millions of videos are uploaded in the internet. Among them many are manipulated by using the techniques which change the video content. From the last few years, continuous research is carried out to detect the video content which contain face tampering. Moreover nowadays, digital image forensic techniques enable to determine: whether the image or part of the image is authentic or artificial, whether the image is being processed with the history of the image. Abundant research is carried out in image forensics, despite of the significant literature survey in image forensics, researchers are more interested into video forensics to explore the issues of research peculiarity [1]. The word forensics comes from the term forensic. Without forensic reports, law enforcement agencies are not accepting the videos as the matter of proof. Every single instance of the video is named as "footprints" which are very important in the videos to prove their Authenticity. Providing video as evidence is important for news reporting, Crime branch investigation, Intelligence agencies, etc., analysing the video for evidence purpose is called Forensic analysis. This is most trending and recent study of researchers to ensure the authenticity of the multimedia data [2][87].

The investigation process from Figure 1 takes from collecting the evidences. If it is a generic crime scene then, the proofs will be the weapons and materials here in this Forensic investigation the evidences are the gadgets where the media is involved. The gathering of evidences is called "Acquisition". After gathering the information of the type of evidence identifying the type of context. This internally divides into three types: Physical context, Logical Context, and Physical Context which leads to the next step of the process i.e., "Evaluation". In evaluation the technology and tools are required to evaluate the type of the information in the evidence and finally it will admit as evidence after evaluating the information.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

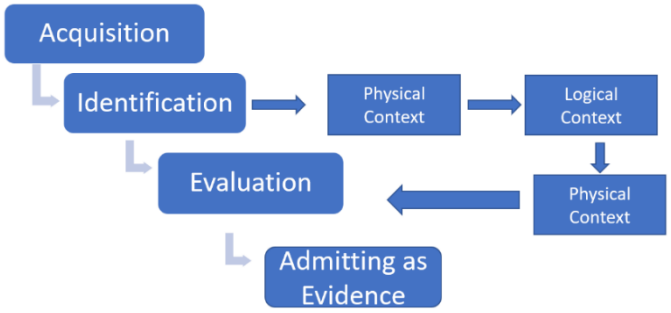

Figure 1. Video Investigation Process

Digital forensics are classified into many types. Particular type is classified depending on the particular application. Here in this paper mainly focus on the computer forensics that depends on the digital data. Multimedia forensics also comes under this category when we classify the type of the data.

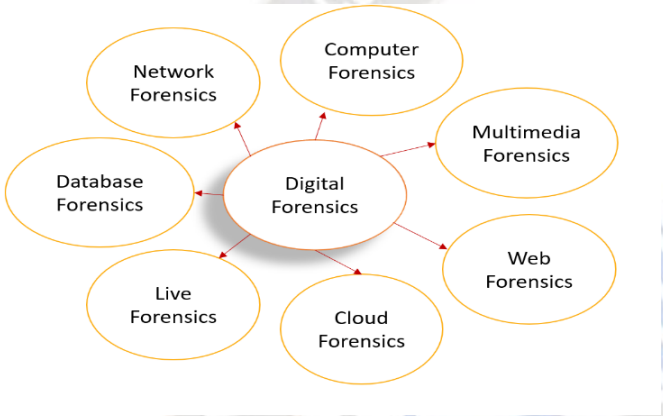

Figure 2. Types of Forensics

As presented in Figure 2, different kinds of digital forensics exist. In essence, digital forensics includes the retrieval and the investigation of information from digital devices.

II. LITERATURE SURVEY

Video forensics became an important research area due to its vast applications in the contemporary era. This section throws light on various existing techniques for video forensics. As discussed in [3] it was difficult to detect forged contents in a compressed video sample. The rationale behind his is that compression might erase footprints of forgery. In [4] there was focused study on forensics in terms of content authentication and detection of a variety of forgeries with possible classification of video tamper techniques. Singh R D [5] published his paper in reputed journal focused on one of the approaches of video tampering detection techniques. The studies show the types of tampering techniques and its description. Tao. J [6] in his paper described about video forgery using localization issues and discussed about the tampering techniques focusing more on image forgery tampering detection rather than video tampering. Rodriguez-Ortega et al. [7] this author presented forgery detection techniques which came across the generalization problems in dataset. These techniques are developed using deep learning where alsakar et al., [8] puts his focus on analysing and identifying the forgery in videos depending on the low complexity tensor representation. After this slowly the researchers showed interest in digging the concepts of forgery and its types. At first only two types famously registered as a puzzle in terms of static and dynamic video. Where insertion and deletion are the two techniques used to forge the video. Ferreria. S [9] in the paper presented by Amerini. I [10] which was published by MDPI in the year 2021 presented that ML techniques are used to detect and identify the fake and real multimedia files where it also gives the information about the presence of the content. Where this idea leads to the digital forensic application called Autospy which includes transformation techniques for the first time where the amalgamation of transformation technique is merged with multimedia data. Discrete Fourier Transform (DFT) technique is used in the application of digital video frames.

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

Large group of sequential images consisted of digital videos where in turn converted into frames by frame rate conversion where it can capture the illusion of motion and displays with rapid success rate [11]. From here any malicious content that violates the information or visual content of the video is considered as video forgery. As [4] presents the types in video forgery depends on the frame separation the insertion the content is called frame insertion and removing the content from the transformed frames from video is called frame deletion. The very first type is within the frame called copy move attack, where the author in [8] presented that certain frames are copied from region to the other region within the frame is inter frame forgery.

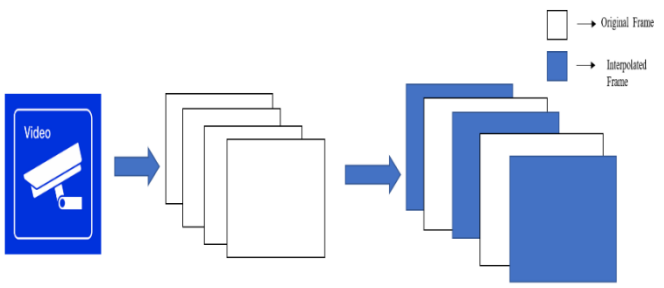

Figure 3. Video to Frame Conversion

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

According to author [8], frames are derived from given video, which are images of some fixed size, to which frame conversion bit rate is applied to identify the frame conversion rate. Depending upon the frame rate of each frame insertion and deletion is done. By [10], the author presented FRUC technique that generate higher frame to a lower frame rate where interpolated frame is inserted to lower the FRUC rate. The other type is presented by Mehta. V et, al., [12] as second type of domain forgery where spatiotemporal domain comes into state of art where this category is listed under active approach of video forgery. This author has introduced some common attacks where region splicing attack is registered as external objects are injected into existing frames. From here frame duplication concept come into picture where yang et, al., [13] presented a two staged effective model which calculates the correlation coefficient similarities between frames using SVD feature extraction.

Liu et, al., [14] has presented his work in duplication and deletion of frame (refer Figure 3) by two concepts where time and frequency are considered as domain features which measure the periodicity of sequence and at high points of frequency DTFT which is Discrete -Time Fourier Transform is calculated with the measures of F1-score, Mean Square Error, Accuracy and prediction rate. Wang et, al. [15] presented his perspective on calculating the correlation coefficient of Gray Values (CoGV's) by machine learning technique Support Vector Machine (SVM). Zhang [16], Aghamaleki [17] and Zhao [18] presented their research on frame insertion and deletion where three different techniques like HSV, SURF and FLANN were used. But the drawback of these techniques it can be only applicable in the case of blind forensic shots of video.

TABLE I. DETECTION METHODS OF VIDEO FORGERY

Reference	Type of Forgery	Used Feature	Limitation
[10]	Duplication of frame	Separation of each frame and finding the similarity using singular value decomposition	This method failed in detecting the other detections like frame re-ordering.
[11]	Frame Deletion	Using sequencing in frames with domain forgery	This method is fixed to certain range of frequency and time
[12]	Frame Insertion and Deletion	CGoVs	Applicable to fixed datasets
[13]	Frame insertion, deletion and duplication	Rather than correlation quotients of correlation is used in between frames	Forgery detection can be done but the other two techniques failed to identify
[14]	Frame Duplication	Histogram color comparison is done with SURF	Limited to some shots of frames
[15]	Frame Insertion, deletion and duplication	CNN – 3D to detect video forgery	Localization is failed to incorporate
[16]	Double compression	Double compression statistics	Localization is failed
[20]	Tampering	Motion residual	Forgery localization is failed
[22]	Upscale crop	Matches the inner dimension of the frame	This method drawback is the video will be enlarged.
[25]	Spatio Temporal forgery	Motion based SVM	The drawback of this method is obtained accuracy is less

Long et al. [19] could find forged frames in videos using a convolution neural network (CNN) with ResNet network where a network is created to identify the frame insertion, deletion and duplication. The limitation of this paper is this cannot be applicable to the continuous videos of long shot frames. To overcome the limitation of discontinuity in the long shot videos the concept of tampering introduced by chan et, al., [20] where this occurs by copy-paste of a small parts of the frame to another frame which attracts the researcher at first sight. The main challenge faced by researchers is manipulation of large size of videos. For this purpose, tensor structure is introduced where data decomposition and dimension reduction techniques are discussed in researcher paper by Kountchev et, al. [21].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

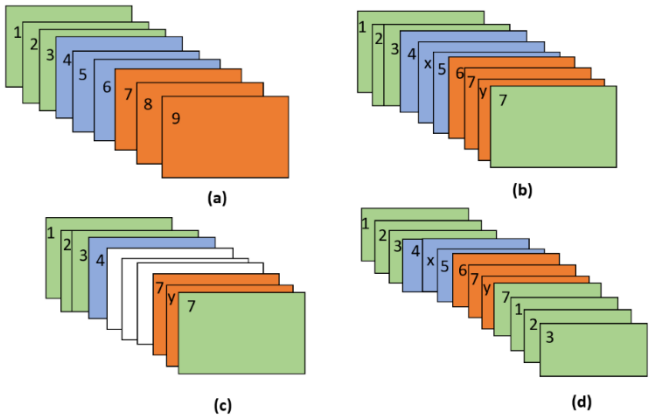

Figure 4. Illustrates inter-frame kind of video forgery reflecting original sequence of frames

Birajdar et al. (2013) and Pandey (2016) investigated on different categories of forensics to deal with videos and images. Chen (2017) was the first to identify video camera linked to forgery. His research was significant due to the notice of noise patterns and possible compression techniques used in videos. DFT transform was proposed to know the forged areas and their investigation was both on low quality and high quality videos. With low-quality videos, they found difficulty in forensics. Later on research focused on different video cameras and identification of forged contents. In [32], their study resulted in identification of forged contents in videos with an algorithm known as PRNU which exploits 3D patch-match to detect forged contents. Their method also uses feature extraction that leverages accuracy in forgery detection.

The studies say that, if we compare the research bar since 1990 in this research domain initially there is very less research in this area as the attacks increases researchers showed their interest more in this domain which will help the Law and government and many cyber forensics gets benefited with the resultant applications. Now, in 2023 [31] if we take the scale of 3-4 months there are more than 15% of research papers. The Figure 5 gives a visual pie chart of researches done in a tenure from 1990 to 2023.

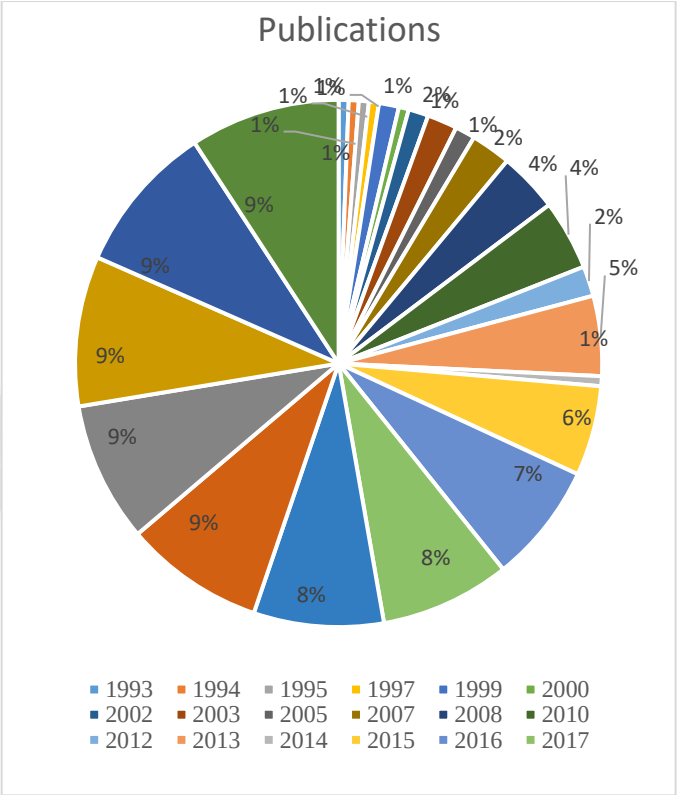

Figure 5. Pie chart of Research from 1990 to 2023

From Figure 5, as there are many types of digital forensics, the researchers classified into many types where the concentration is more on videos and networks. The network part of detection of forgery is called Intrusion [30]. Network intrusion in videos is the next trending research area where the forged videos are transmitted through a channel where intrusion is the forged part of detecting and identifying the breech in the network.

A. Network Forensics

Network Forensic being a branch of Digital Forensic is used to capture many crimes involving the videos in the network where digital data is captured over a computerised network environment with the help of NFT's and NFP's where data is being examined over a network with normal and abnormal traffic data is analysed over the network with incident detection and reaction analysis is provided to the court for evidence purpose [23]. The digital media transferred over the network will have the transmission channel which leaves the foot prints of the data in the network while searching through the search engine where the digital videos transmission is the dataset where detection of intrusion is identified model. As shown in below Figure 6, explains the process of data generation and examination of the evidence. After the detection of suspicious data, the log files are generated and sent to the network forensic analysis. Later the recovery process has

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

divided into four steps of process including collecting the data to reporting the data to the court as evidence [24].

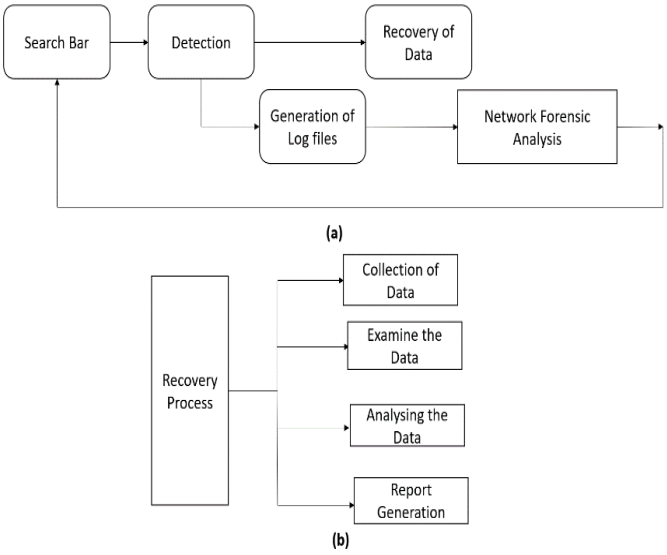

Figure 6. Network Forensic Process

From the above Figure 6 is the process of steps collecting the information of type data where report is generated that is to be sent to the bureau team. There are some tools which is used for testing the data and generating the report.

TABLE II. DESCRIPTION OF DIFFERENT DATASETS

Dataset	Types of Forgery	Feature
SULFA	Frame duplication with shuffling	GLCM
LASIESTA	Frame duplication	GLCM
TRACE	Duplicate region localization	Haralick PRG and OFG
REWIND	DWT, SIFT	CNN
VTL	Video based motion	CNN
TREC	Swapping-frames	GLCM
SYSU-OBJFORG	Spatial and Temporal Domain	TPFC
NTHU	Frame duplication, Frame shuffling	YouTube Video
GRIP	Copy-move, splicing, Deepfake	SIFT
CVAP	Homogenous background	Nimble challenge in house
DFDC	Deepfake	DERF collections
FaceForensics ++	Deepfakes	Neural textures
BOSS	Steganalysis	CNN and SIFT
IMDB	CM	GLCM
CASIA v2.0	CP and CM	OFG

With the recent survey, these datasets consist of original and forged videos which is designed by the University of Surrey and from many of the internet resources. SULFA, REWIND, GRIP are the datasets with the formats MJPEG, H.264 codecs. They are captured from real time Surveillance cameras and YouTube with different test sets 119, 154, 4000, 5000 and 10,000 video clips of less than 10 seconds in length [26]. Among the mentioned datasets and its features some commonly used datasets and its features extracted are from the above Table 2. A comparison graph plot is drawn to understand clearly in which year which type of dataset is used more frequently. Copy-move, splicing, inter frame and intra frame are the type of forgeries plotted in the chart.

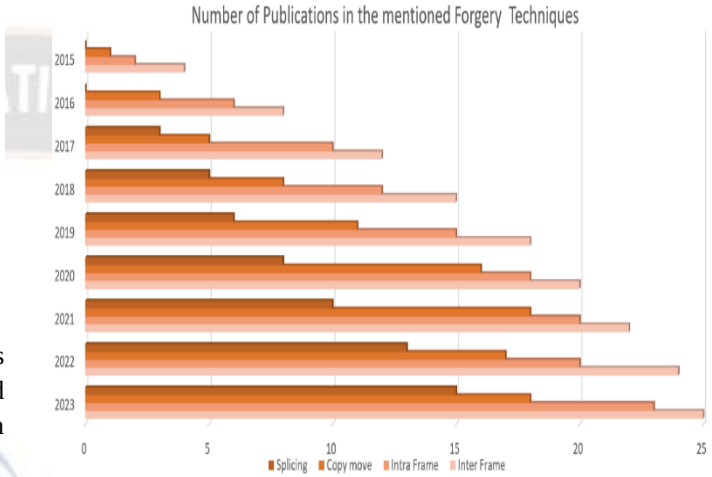

Figure 7. A bar chart of number of publication year wise with forgery techniques as categories

B. Summary of Video Forgery Detection Techniques

TABLE III. VIDEO FORGERY DETECTION BASED ON INTER AND INTRA FRAME TECHNIQUES

Reference	Approach	Technique	Algorithm	Dataset	Limitations
[33]	Passive approach	Inter-frame	Forgery detection	Internet Streamed Video	Vulnerable to attacks
[34]	Search based approach	Inter-frame	Block-based algorithm	Custom videos	Difficult to detect near duplicate areas
[35]	Active and passive search	Inter-frame	Fast rule identification algorithm	Live videos taken from camera	To be improved with more cases of forgery
[36]	Copy-move forgery detection	Inter-frame	Forgery detection and localization	REWIND	Time consuming

[37]	The active and the passive approach	Inter-frame	Forgery detection algorithm	REWIND	Not suitable for high motion videos
[38]	Normalized cross-correlation	Inter-frame	Video forgery detection	REWIND	High FPR
[39]	Bottom-up approach	Intra-frame	Expectation-Maximization	Custom dataset	Works for only fine quality sequences
[40]	Non-Subsampled Contourlet (NSCT)	Intra-frame	Feature selection algorithm	Dataset from mine.tku.edu	Relies on training samples
[41]	Digital forensics	Intra-frame	Video tampering detection	MPEG-2	Accuracy 87%. To be improved by checking effect of B-frame to P-frame's MCEAs
[42]	HMRF	Intra-frame	state of the art detection algorithms.	Derf's and YUV	Accuracy 88.95% and to be improved with localization
[43]	Digital forensics	Intra-frame	Automaton algorithm	KTH	Forgery localization is yet to be done.
[44]	Block-Wise Brightness Variance Descriptor	Inter-frame	Block-wise descriptor based algorithm	SYSU-OBJFORG	Accuracy 83.37% and to be improved to handle double compressed samples

As presented in Table 3, summary of forgery detection methods based on inter and intra-frame techniques are provided along with limitations in the existing works.

TABLE IV. SUMMARY OF VIDEO FORGERY DETECTION TECHNIQUES LIKED TO DEEPFAKE AND PIXEL MOTION DETECTION

Reference	Technique	Features Selected	Dataset	Limitations
[45]	Deepfake	Eye Blinking	Custom dataset	Needs to be evaluated with more video samples
[46]	Deepfake	Head Pose	UADFV and DARPA GAN	Not good in detection of puppet-master and lip-sync forgeries
[47]	Deepfake	Color Artifacts	LSUN and ImageNet	Localization is not yet effectively done
[48]	Deepfake	Classification	Self, FaceForensics	Suffers from overfitting problem
[49]	Pixel Motion Detection	Velocity Field Consistency	TRECVID	Could not identify manipulated regions
[50]	Pixel Motion Detection	Optical Flow	TRECVID	Expensive in computations
[51]	Pixel Motion Detection	Motion Vector Pyramid and Variation factor	TRECVID	Works with videos containing static backgrounds
[52]	Pixel Motion Detection	Coarse to fine Optical Flow	VTL, SULFA, DERF	Misdetection issue as it is sensitive to coarse detection
[53]	Key-Frame Extraction	Reference frame	Self	Relies on reference frame for accuracy
[54]	Key-Frame Extraction	Delaunay graph clustering	Self	Expensive in computations
[55]	Key-Frame Extraction	Cluster classification	Self	Suffers from loss of temporal order
[56]	Key-Frame Extraction	Abnormal events	Self	Suffers from loss of temporal order
[57]	Key-Frame Extraction	3D CNN	Self	Not accurate with different camera angles
[58]	Object Tracking and Detection	Motion Vectors and block types	SENSIAC	Tracking of modified patches is still desired
[59]	Object Tracking and Detection	Bayesian Approach	PETS-ECCV	Relies on colour information

[60]	Object Tracking and Detection	GMM	Self	Could not find long distance object
[61]	Object Tracking and Detection	Contrast Model	Custom dataset	Relies more on training samples
[62]	Feature extraction	Histogram Matching	Self	It is format-sensitive
[63]	Feature extraction	Convolutional LSTM	SULFA	Generalization was not accurate
[64]	Feature extraction	MLS	Self	Less detection accuracy
[65]	Feature extraction	Exponential Fourier Transforms	Self, SULFA	Detects only region duplication cases

As presented in Table 4, video forgery detection techniques liked to deepfake and pixel motion detection are provided.

III. RELATED WORK

Daily in our lives we find many doctored videos in media like WhatsApp, Instagram, TikTok, Snapchat, Facebook and many more. The purpose of sharing the information is different like fun or news, or community information, religious videos etc., are being shared fearlessly without having the knowledge that these videos can be morphed, forged or manipulated according to the conveniency of the manipulator [28]. As there is immense research in the field of video forensics there is no such method /technique /application is available which confirms the Genuity of the video.

In internet we came across many similar videos which have same content but they differ with the clarity of the video. This is because the resolution of the video is changed to different resolution using converter techniques. Even such videos are not reliable to view for 100% information, they are forged depending upon their requirements [26]. Hence here is a need for detection of forged videos. Definitely this will help the forensics as well to generate the report of the evidence which eventually wills top the spread of the fake videos. Malik et, al [27] in his previous research presented a paper on audio visual forensics where he carried work on detecting the audio manipulation with the sync to the video. The speech in the audio is manipulated with speech inconsistencies. Slowly, wide range of methods are used to learn the audio-video representation from videos. Variety of methods have recently use audio visual self-supervision for pertaining supervised models. In contrast to this another approach of learning is introduced the learning representation of audio visual which is leveraged to the natural semantic of separating the frames to audio track. Audio is separated from the video and only to the video part the combination of DWT and PCA analysis will give the early detection of the forgery in the content. This analysis can be done stages wise by operating first using the stationary wavelet transform and then the first step of DWT and at the end PCA (Principal Component Analysis) value id calculated which gives the entire accuracy and performance metric values like MSME, precision, recall and F1 score.

A. Summary of most recent work

TABLE V. SUMMARY OF VIDEO FORGERY DETECTION TECHNIQUES LIKED TO DEEPFAKE AND PIXEL MOTION DETECTION

Reference	**Approach**	**Technique**	**Algorithm**	**Data set**	**Limitation / Future Scope**
[66]	Deep learning	2D-CNN and SSIM fusion	Feature extraction algorithm	VIRAT, SULFA, LASIESTA, IVY LAB	In future, they intend to make the system detect multiple inter-frame forgeries
[67]	Deep learning	Adaptive-Taylor-rider optimization algorithm based DCNN	Dual adaptive-Taylor-rider optimization algorithm (DA-TROA)	Real dataset	In future, they intend to exploit hybrid optimizations for training the classifier
[68]	Deep learning	CNN, Compression and Video tampering detection	Video tampering detection	Dataset from xiph.org	In future, they intend to work on a better method to combine the features into a video manipulation localiser
[69]	Sequential and Patch Analyses	Object removal forgery detection	Object Removal Forgery Detection and Localization	Lin's video set	In the future, they intend to investigate non-additive change models

[70]	Deep learning	VGG-16	Digital image forgery detection using supervised learning method	GRIP, DVMM, CMFD, and BSDS300	In future different forgery attacks such as JPEG compression
[71]	Machine Learning and Deep Learning	CNN, KNN and AI	Deep fake video detection	Deep fake detection challenge datasets	Their future research is to focus on deepfake detection in other media like National IDs.
[72]	Deep Learning	Pixel-Region Relation Network (PRRNet)	Relation encoder and region feature extractor	FaceForensics++, celeb-DF and DFDC	Inter-frame inconsistencies in fake videos are yet to be explored
[73]	Deep Learning	Inconsistency-aware wavelet dual-branch network	Face forgery detection	FaceForensics++, Celeb-DF and UADFV	Intra-image and inter-image inconsistencies are yet to be explored.
[74]	Deep Learning	3D-CNN	Face forgery detection	FaceForensics++ and VidTIMIT	Detecting different types of facial reenactments is yet to be done
[75]	Machine Learning	ML models	Digital video post processing detection	VISION and Video-ACID	Their method needs improvement using deep learning techniques.

As presented in Table 5, most recent video forgery detection methods are summarized. There are significant research gaps found in the recent works.

B. Significant Research Gaps

Vinolin et al. [2] proposed research focuses on establishing the 3D model of the video frame to generate light coefficients in order to detect the forgeries in the video. Their method has limitations in detecting small correction in videos and need improvement of CNN model with optimizations for efficiency. Fadl et al. [1] propose inter-frame forgeries (frame deletion, frame insertion, and frame duplication) detection system using 2D convolution neural network (2D-CNN) of spatiotemporal information and fusion for deep automatically feature extraction. However, it lacks detection of detect multiple inter-frame forgeries present in a single video. Shang et al. [7] proposed a novel network, called Pixel-Region Relation Network (PRRNet), to capture pixel-wise and region wise relations respectively for face forgery detection. However, for efficient inter-frame forgeries detection efficiently, it needs improvement in terms of detecting Region of Interest (ROI) for improving detection accuracy and convergence.

IV. CONCLUSION

In this survey article many issues related to video forgery has been concentrated and their limitations also discussed. From the past few years whatever the work researchers has been carried out in this domain has been put up this survey article. The methods, study, techniques all these are very important for the video forgery detection because as he data is not constant it is been updated at every usage similarly the techniques need to be upgraded depending upon the requirements. At active approach of video forgery ample of research is done. Researchers should now bring out their studies at passive approach to detect the forgery depending upon on the advancement of the industry. The features like copy-move frame detection, frame duplication, frame deletion, frame insertion are the most common issues identified. Though there has been active research in this area but solution to this problem is yet to achieve. There is no universal tool/ algorithm to identify the tampering in videos. The solution is provided in this article which may solve this problem of tampering in videos with the compression of videos.

While compressing the videos, compression techniques are used. Which lead to loss of data by leaving the footprints of watermark which leads to the problem in generating reports. No compression should be done on videos and techniques should be applied on the video to detect the forgery. Important research gaps found in this research include need for better CNN variants, detection of multiple inter-frame forgeries present in a single video and region of interest awareness.

REFERENCES

[1] Simone Milani, Marco Fontani, Paolo Bestagini, Mauro Barni, Alessandro Piva, Marco Tagliasacchi and Stefano Tubaro (2012), "An overview on video forensics", APSIPA Transactions on Signal and Information Processing, 1, e2 doi:10.1017/ ATSIP.2012.

[2] Akhtar, N.; Saddique, M.; Asghar, K.; Bajwa, U.I.; Hussain, M.; Habib, Z. "Digital Video Tampering Detection and Localization: Review, Representations, Challenges and Algorithm",

Mathematics 2022, 10, 168. https://doi.org/10.3390/ math10020168.

[3] Staffy Kingra, Naveen Aggarwal and Raahat Devender Singh, "Video Inter-frame Forgery Detection: A Survey", Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105142, November 2016.

[4] Raahat Devender Singh, Naveen Aggarwal, "Video content authentication techniques: a comprehensive survey", Multimedia Systems (2018) 24:211–240 DOI 10.1007/s00530-017-0538-9.

[5] Singh, R.D.; Aggarwal, N. Video content authentication techniques: A comprehensive survey. Multimed. Syst. 2018, 24, 211–240.

[6] Tao, J.; Jia, L.; You, Y. Review of passive-blind detection in digital video forgery based on sensing and imaging techniques. In Proceedings of the International Conference on Optoelectronics and Microelectronics Technology and Application. International Society for Optics and Photonics, Shanghai, China, 5 January 2017.

[7] Rodriguez-Ortega, Y.; Ballesteros, D.; Renza, D. Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics. J. Imaging 2021, 7, 59. [CrossRef]

[8] Alsakar, Y.; Mekky, N.; Hikal, N. Detecting and Locating Passive Video Forgery Based on Low Computational Complexity Third-Order Tensor Representation. J. Imaging 2021, 7, 47. [CrossRef] [PubMed]

[9] Ferreira, S.; Antunes, M.; Correia, M. Exposing Manipulated Photos and Videos in Digital Forensics Analysis. J. Imaging 2021, 7, 102. [CrossRef]

[10] Amerini, I.; Baldini, G.; Leotta, F. Image and Video Forensics. J. Imaging 2021, 7, 242. https:// doi.org/10.3390/jimaging7110242

[11] Abdulhussain, S.H.; Al-Haddad, S.A.R.; Saripan, M.I.; Mahmmod, B.M.; Hussien, A.J.I.A. Fast Temporal Video Segmentation Based on Krawtchouk-Tchebichef Moments. IEEE Access 2020, 8, 72347–72359. [CrossRef]

[12] Mehta, V.; Jaiswal, A.K.; Srivastava, R. Copy-Move Image Forgery Detection Using DCT and ORB Feature Set. In Proceedings of the International Conference on Futuristic Trends in Networks and Computing Technologies, Chandigarh, India, 22–23 November 2013; Springer: Singapore, 2019; pp. 532–544.

[13] Yang, J.; Huang, T.; Su, L. Using similarity analysis to detect frame duplication forgery in videos. Multimed. Tools Appl. 2016, 75, 1793–1811. [CrossRef]

[14] Liu, H.; Li, S.; Bian, S. Detecting frame deletion in H. 264 video. In Proceedings of the International Conference on Information Security Practice and Experience, Fuzhou, China, 5–8 May 2014; Springer: Cham, Switzerland, 2014; pp. 262–270.

[15] Wang, Q.; Li, Z.; Zhang, Z.; Ma, Q.J. Video inter-frame forgery identification based on consistency of correlation coefficients of gray values. J. Comput. Commun. 2014, 2, 51. [CrossRef]

[16] Zhang, Z.; Hou, J.; Ma, Q.; Li, Z. Efficient video frame insertion and deletion detection based on inconsistency of correlations between local binary pattern coded frames. Secur. Commun. Netw. 2015, 8, 311–320. [CrossRef]

[17] Aghamaleki, J.A.; Behrad, A. Inter-frame video forgery detection and localization using intrinsic effects of double compression on quantization errors of video coding. Signal Process. Image Commun. 2016, 47, 289–302. [CrossRef]

[18] Zhao, D.-N.; Wang, R.-K.; Lu, Z.-M. Inter-frame passive-blind forgery detection for video shot based on similarity analysis. Multimed. Tools Appl. 2018, 77, 25389–25408. [CrossRef]

[19] Long, C.; Basharat, A.; Hoogs, A. A Coarse-to-fine Deep Convolutional Neural Network Framework for Frame Duplication Detection and Localization in Video Forgery. CVPR Workshops 2019. pp. 1–10. Available online: http://www.chengjianglong. com/publications/CopyPaste.pdf (accessed on 10 February 2021).

[20] Chen, S.; Tan, S.; Li, B.; Huang, J. Automatic detection of object-based forgery in advanced video. IEEE Trans. Circuits Syst. Video Technol. 2015, 26, 2138–2151. [CrossRef].

[21] Kountchev, R.K.; Iantovics, B.L.; Kountcheva, R.A. Hierarchical third-order tensor decomposition through inverse difference pyramid based on the three-dimensional Walsh–Hadamard transform with applications in data mining. Data Min. Knowl. Discov. 2020, 10, e1314.

[22] Harpreet Kaur, Neeru Jindal, "Image and Video Forensics: A Critical Survey', Springer Science Business Media, LLC, part of Springer Nature 2020.

[23] Damir Delija, Ivan Mohenski, Goran Sirovatka, "Comparative Analysis of Network Forensic Tools and Network Forensics Processes", International Conference on Smart Computing and Electronic Enterprise. (ICSCEE2021) ©2021 IEEE.

[24] Sirajuddin Qureshi, Jianqiang Li, Faheem Akhtar, Saima Tunio, Zahid Hussain Khand, "Analysis of challenges in Modern Network Forensic Framework", Hindawi Security and Communication Networks Volume 2021, Article ID 8871230, 13 pages https://doi.org/10.1155/2021/8871230.

[25] Kancherla K, Mukkamala S (2012) Novel blind video forgery detection using markov models on motion residue. In: Asian Conference on Intelligent Information and Database Systems. Springer, pp 308–315.

[26] Sk Mohiuddin, Samir Malakar, Munish Kumar, Ram Sarkar, "A comprehensive survey on state-of-the-art video forgery detection techniques", Multimedia Tools and Applications https://doi.org/10.1007/s11042-023-14870-8.

[27] Hafiz Malik and Hany Farid. Audio forensics from acoustic reverberation. In 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, 2010

[28] Chao Feng Ziyang Chen Andrew Owens, "Self-Supervised Video Forensics by Audio-Visual Anomaly Detection", arXiv:2301.01767v2 [cs.CV] 27 Mar 2023.

[29] Akhtar, N.; Saddique, M.; Asghar, K.; Bajwa, U.I.; Hussain, M.; Habib, Z. Digital Video Tampering Detection and Localization: Review, Representations, Challenges and Algorithm. Mathematics 2022, 10, 168. https://doi.org/10.3390/ math10020168

[30] Sowmya K.N, H.R. Chennamma, "A SURVEY ON VIDEO FORGERY DETECTION", International Journal of Computer Engineering and Applications, Volume IX, Issue II, February 2015 www.ijcea.com ISSN 2321-3469.

[31] Ferrag, Mohamed Amine & Maglaras, Leandros & Moschoyiannis, Sotiris & Janicke, Helge. (2019). Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study. Journal of Information Security and Applications. 50. 10.1016/j.jisa.2019.102419.

[32] Fahad M Ghabban, Ibrahim Alfadli, Omair Ameerbakhsh, Amer Nizar AbuAli, Arafat Al-Dhaqm, Mahmoud Ahmad Al-Khasawneh, "Mahmoud Ahmad Al-Khasawneh", International Conference on Smart Computing and Electronic Enterprise. (ICSCEE2021) ©2021 IEEE.

[33] Chetty, G., Biswas, M., Singh, R., 2010. Digital video tamper detection based on multimodal fusion of residue features. In: 2010 Fourth International Conference on Network and System Security. IEEE, Melbourne, VIC, Australia, pp. 606–613.

[34] LIN, GUO-SHIANG; CHANG, JIE-FAN (2012). detection of frame duplication forgery in videos based on spatial and temporal analysis. international journal of pattern recognition and artificial intelligence, 26(7), doi:10.1142/s0218001412500176

[35] Tralic, Dijana; Grgic, Sonja; Zovko-Cihlar, Branka (2014). [IEEE 2014 X International Symposium on Telecommunications (BIHTEL) - Sarajevo, Bosnia and Herzegovina (2014.10.27-2014.10.29)] 2014 X International Symposium on Telecommunications (BIHTEL) - Video frame copy-move forgery detection based on Cellular Automata and Local Binary Patterns. , pp.1–4. doi:10.1109/bihtel.2014.6987651

[36] D'Amiano, L.; Cozzolino, D.; Poggi, G.; Verdoliva, L. (2015). [IEEE 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) - Turin, Italy (2015.6.29-2015.7.3)] 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) - Video forgery detection and localization based on 3D patchmatch. , pp.1–6. doi:10.1109/icmew.2015.7169805

[37] Bidokhti, Amir; Ghaemmaghami, Shahrokh (2015). [IEEE 2015 International Symposium on Artificial Intelligence and Signal Processing (AISP) - Mashhad, Iran (2015.3.3-2015.3.5)] 2015 The International Symposium on Artificial Intelligence and Signal Processing (AISP) - Detection of regional copy/move forgery in MPEG videos using optical flow. , pp.13–17. doi:10.1109/AISP.2015.7123529

[38] Mathai, M.; Rajan, D.; Emmanuel, S. (2016). Video forgery detection and localization using normalized cross-correlation of moment features. , IEEE, pp.149–152. doi:10.1109/SSIAI.2016.7459197

[39] Hsu, C.-C., Hung, T.-Y., Lin, C.-W., Hsu, C.-T., 2008. Video forgery detection using correlation of noise residue. In: 2008 IEEE 10th Workshop on Multimedia Signal Processing. IEEE, Cairns, QLD, Australia, pp. 170–174.

[40] Chen, R., Dong, Q., Ren, H., Fu, J., 2012. Video forgery detection based on nonsubsampled contourlet transform and gradient information. Inform. Technol. J. 11 (10), 1456.

[41] Dong, Qiong; Yang, Gaobo; Zhu, Ningbo (2012). A MCEA based passive forensics scheme for detecting frame-based video tampering. Digital Investigation, 9(2), pp.151–159. doi:10.1016/j.diin.2012.07.002

[42] Ravi, Hareesh; Subramanyam, A. V.; Gupta, Gaurav; Kumar, B. Avinash (2014). Compression noise based video forgery detection. , IEEE, pp.5352–5356. doi:10.1109/ICIP.2014.7026083

[43] S. Chen; S. Tan; B. Li; J. Huang (2015). Automatic Detection of Object-based Forgery in Advanced Video. , pp.1-14. doi:10.1109/TCSVT.2015.2473436

[44] Zheng, L., Sun, T., Shi, Y.-Q., 2014. Inter-frame video forgery detection based on block-wise brightness variance descriptor. In: International Workshop on Digital Watermarking. Springer, Taipei, Taiwan, pp. 18–30.

[45] Li, Y., Chang, M.-C., Lyu, S., 2018. In ictu oculi: Exposing ai created fake videos by detecting eye blinking. In: 2018 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, Hong Kong, China, pp. 1–7.

[46] Yang, X., Li, Y., Lyu, S., 2019. Exposing deep fakes using inconsistent head poses. In: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, Brighton, UK, pp. 8261–8265.

[47] McCloskey, S., Albright, M., 2018. Detecting GAN-generated imagery using color cues. arXiv:arXiv:1812.08247.

[48] Afchar, D., Nozick, V., Yamagishi, J., Echizen, I., 2018. Mesonet: a compact facial video forgery detection network. In: Proc. 2018 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, pp. 1–7.

[49] 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.

[50] 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.

[51] Zhang, Z., Hou, J., Li, Z., Li, D., 2016. Inter-frame forgery detection for staticbackground video based on MVP consistency. In: Digital-Forensics and Watermarking. Springer International Publishing, pp. 94–106. http://dx.doi.org/10.1007/978- 3-319-31960-5_9.

[52] Jia, S., Xu, Z., Wang, H., Feng, C., Wang, T., 2018. Coarse-to-fine copy-move forgery detection for video forensics. IEEE Access 6, 25323–25335. http://dx.doi.org/10. 1109/access.2018.2819624.

[53] Sun, Z., Jia, K., Chen, H., 2008. Video key frame extraction based on spatial-temporal color distribution. In: Proc. of 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, Harbin, China, http: //dx.doi.org/10.1109/iih-msp.2008.245.

[54] Kuanar, S.K., Panda, R., Chowdhury, A.S., 2013. Video key frame extraction through dynamic delaunay clustering with a structural constraint. J. Vis. Commun. Image Represent. 24 (7), 1212–1227. http://dx.doi.org/10.1016/j.jvcir.2013.08.003.

[55] Bhatt, H.S., Singh, R., Vatsa, M., 2014. On recognizing faces in videos using clusteringbased re-ranking and fusion. IEEE Trans.

Inf. Forensics Secur. 9 (7), 1056–1068. http://dx.doi.org/10.1109/tifs.2014.2318433.

[56] Srinivas, M., Pai, M.M., Pai, R.M., 2016. An improved algorithm for video summarization–a rank based approach. Procedia Comput. Sci. 89, 812–819. http: //dx.doi.org/10.1016/j.procs.2016.06.065.

[57] Cai, X., Hu, F., Ding, L., 2016. Detecting abnormal behavior in examination surveillance video with 3D convolutional neural networks. In: 2016 6th International Conference on Digital Home (ICDH). IEEE, Guangzhou, http://dx.doi.org/10.1109/icdh.2016. 014.

[58] Demir, H.S., Adil, O.F., 2018. Part-based co-difference object tracking algorithm for infrared videos. In: Proc. 2018 25th IEEE International Conference on Image Processing (ICIP). IEEE, Athens, Greece, pp. 3723–3727.

[59] Besita Augustin, M., Juliet, S., Palanikumar, S., 2011. Motion and feature based person tracking in surveillance videos. In: Proc. 2011 International Conference on Emerging Trends in Electrical and Computer Technology, Nagercoil, India, pp. 605–609.

[60] Nazib, A., Oh, C., Lee, C., 2013. Object detection and tracking in night time video surveillance. In: 2013 10th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI), Jeju, Korea (South), pp. 629–632.

[61] Hong, K., Shim, J., Kang, B., Jung, I., 2012. Proc. of Homographic tracking algorithm of moving objects for multiple video surveillance system (ICCAS 2012). In: 2012 12th International Conference on Control, Automation and Systems, Jeju, Korea (South), pp. 462–465.

[62] Zhao, D.-N., Wang, R.-K., Lu, Z.-M., 2018. Inter-frame passive-blind forgery detection for video shot based on similarity analysis. Multimedia Tools Appl. 77 (19), 25389–25408. http://dx.doi.org/10.1007/s11042-018-5791-1.

[63] Kono, K., Yoshida, T., Ohshiro, S., Babaguchi, N., 2019. Passive video forgery detection considering spatio-temporal consistency. In: Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018). Springer International Publishing, pp. 381–391. http://dx.doi.org/10.1007/978-3-030-17065- 3_38.

[64] Huang, C.C., Zhang, Y., Thing, V.L.L., 2017. Inter-frame video forgery detection based on multi-level subtraction approach for realistic video forensic applications. In: Proc. 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP), Singapore, pp. 20–24.

[65] Su, L., Li, C., Lai, Y., Yang, J., 2018. A fast forgery detection algorithm based on exponential-Fourier moments for video region duplication. IEEE Trans. Multimed. 20 (4), 825–840.

[66] Fadl, Sondos; Han, Qi and Li, Qiong (2020). CNN spatiotemporal features and fusion for surveillance video forgery detection. Signal Processing: Image Communication, 116066–. http://doi:10.1016/j.image.2020.116066

[67] Vinolin, V. and Sucharitha, M. (2020). Dual adaptive deep convolutional neural network for video forgery detection in 3D lighting environment. The Visual Computer. http://doi:10.1007/s00371-020-01992-5

[68] Johnston, Pamela; Elyan, Eyad and Jayne, Chrisina (2019). Video tampering localisation using features learned from authentic content. Neural Computing and Applications. http://doi:10.1007/s00521-019-04272-z

[69] Aloraini, M., Sharifzadeh, M., & Schonfeld, D. (2020). Sequential and Patch Analyses for Object Removal Video Forgery Detection and Localization. IEEE Transactions on Circuits and Systems for Video Technology, 1–1. http://doi:10.1109/tcsvt.2020.2993004

[70] Abhishek and Jindal, Neeru (2020). Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation. Multimedia Tools and Applications. http://doi:10.1007/s11042-020-09816-3

[71] Alakananda Mitra; Saraju P. Mohanty; Peter Corcoran and Elias Kougianos; (2021). A Machine Learning Based Approach for Deepfake Detection in Social Media Through Key Video Frame Extraction. SN Computer Science. http://doi:10.1007/s42979-021-00495-x

[72] Zhihua Shang; Hongtao Xie; Zhengjun Zha; Lingyun Yu; Yan Li and Yongdong Zhang; (2021). PRRNet: Pixel-Region relation network for face forgery detection. Pattern Recognition. http://doi:10.1016/j.patcog.2021.107950

[73] Gengyun Jia; Meisong Zheng; Chuanrui Hu; Xin Ma; Yuting Xu; Luoqi Liu; Yafeng Deng and Ran He; (2021). Inconsistency-Aware Wavelet Dual-Branch Network for Face Forgery Detection. IEEE Transactions on Biometrics, Behavior, and Identity Science. http://doi:10.1109/TBIOM.2021.3086109.

[74] Xuan Hau Nguyen; Thai Son Tran; Van Thinh Le; Kim Duy Nguyen and Dinh-Tu Truong; (2021). Learning Spatio-temporal features to detect manipulated facial videos created by the Deepfake techniques. Forensic Science International: Digital Investigation. http://doi:10.1016/j.fsidi.2021.301108

[75] Sandoval Orozco, Ana Lucila; Quinto HuamÃ¡n, Carlos; Povedano Ã• lvarez, Daniel and GarcÃ-a Villalba, Luis Javier (2020). A machine learning forensics technique to detect post-processing in digital videos. Future Generation Computer Systems,111,199–212. http://doi:10.1016/j.future.2020.04.041.