

Video forgery: An extensive analysis of inter-and intra-frame manipulation alongside state-of-the-art comparisons

Sumaiya Shaikh, Sathish Kumar Kannaiah

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India

Article Info

Article history:

Received May 9, 2024

Revised Nov 7, 2024

Accepted Nov 14, 2024

Keywords:

Analysis

Digital video forensics

Multimedia forensics

Video authentication

Video tampering detection

ABSTRACT

The widespread accessibility of inexpensive mobile phones, digital cameras, camcorders, and security closed-circuit television (CCTV) cameras has resulted in the integration of filmmaking into our everyday existence. YouTube, Facebook, Instagram, and Snapchat are a few of the video-sharing and editing applications that facilitate the process of uploading and editing videos. Additional instances include Adobe Photoshop, Windows Movie Maker, and Video Editor. Although editing has its advantages, there is a potential risk of counterfeiting. This occurs when films are edited with the intention of misleading viewers or manipulating their perspectives, which can be particularly troublesome in judicial procedures where recordings are submitted as evidence. The issue has been exacerbated by the emergence of deep learning methods, such as deepfake videos that effectively manipulate facial characteristics. Consequently, individuals have become less reliant on visual evidence. These issues emphasise the pressing necessity for the creation of dependable methods to determine the authenticity of films and identify cases of fraud. Contemporary methods can depend on assessing modified frames or utilising distortions generated during video codec compression or double compression. Since 2016, multiple studies have been undertaken to investigate techniques, strategies, and applications to tackle this problem. The objective of this survey study is to provide a comprehensive analysis of these algorithms, highlighting their advantages and disadvantages in detecting different forms of video forgeries.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Sathish Kumar Kannaiah

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation

Vaddeswaram, Vijayawada, Andhra Pradesh, India

Email: ksathish1980@gmail.com

1. INTRODUCTION

Every day, countless videos are uploaded to the internet, a significant portion of which undergo editing. This paper focuses on the detection of video forgery through an extensive analysis of both inter-frame and intra-frame manipulations, comparing these techniques with state-of-the-art methods. Video forgery involves the alteration of video content to mislead viewers, posing significant challenges for digital forensics and security. Inter-frame manipulation includes techniques such as frame duplications or deletion, which disrupt the temporal consistency of a video. Intra-frame manipulation involves altering individual frames, such as splicing or changing objects within frames, affecting the spatial integrity of the video. A recent study has primarily concentrated on the identification of manipulated recordings, particularly those that have been modified to change facial characteristics. Although digital image forensic techniques have made significant advances in establishing image authenticity and processing history, video forensics remains an expanding topic of interest for researchers. Our research addresses a critical need for reliable and efficient

video forgery detection methods. Current state-of-the-art techniques often struggle with either high false positive/negative rates or computational inefficiency. Our study introduces a novel approach that combines advanced spatial and temporal analysis to improve detection accuracy while maintaining computational efficiency. This work contributes to the field by offering a more robust solution for identifying both inter-frame and intra-frame forgeries, thus enhancing digital forensic capabilities and aiding in the fight against misinformation and digital fraud. The term "forensics" is derived from the word "forensic," and law enforcement agencies are generally hesitant to accept films as credible evidence in the absence of forensic reports. Individual components of a video, known as "footprints," play an important part in assessing its legitimacy. As a result, forensic analysis plays an essential role in areas such as news reporting, criminal investigations, and intelligence operations [1], [2].

This study investigates with the collection of evidence as depicted in Figure 1, much like a standard crime scene investigation. Earlier the study involves traditional investigative procedure which holds the impact and importance of multimedia data in forensic investigation. Early methods have not explicitly addressed the influence of investigation on multimedia data. However, in the context of forensic investigations into digital media, the evidence is mostly related to electronic devices that contain multimedia data. The initial stage, known as "acquisition," comprises gathering information on the nature of the evidence at hand. The approach then focuses on determining the evidence's context, which can be divided into three categories: physical, logical, and chronological. This classification lays the groundwork for the next phase, "evaluation," in which specialized technology and methodologies are used to assess the information contained in the evidence. After a thorough examination, evidence is deemed acceptable for further investigation and potential use in judicial proceedings [1].

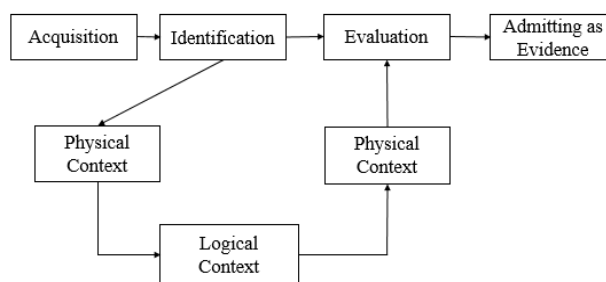


Figure 1. The procedure for investigating videos

There are numerous subfields within digital forensics. Different types are categorized based on the specific use. The paper's primary emphasis is on digital data-dependent computer forensics. When sorting data by type, multimedia forensics also falls into this group. Figure 2 illustrates different branches of digital forensics, which involve a variety of approaches used to recover and analyze data from digital devices. Essentially, digital forensics is the methodical process of extracting and examining data contained in electronic devices.

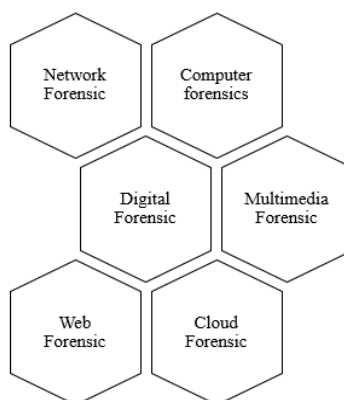


Figure 2. Categories of forensics

2. LITERATURE SURVEY

The field of video forensics has increased in popularity due to its wide range of applications in the current world. This section provides an overview of the several established methodologies in video forensics. As stated in Le *et al.* [3], it was difficult to detect counterfeit information in a compressed video sample. The rationale for this is that compression has the capacity to eliminate all evidence of forgeries. Conducted a thorough analysis of the topic of forensics, specifically in terms of content authenticity and the detection of various sorts of forgeries, including the potential categorization of video tampering methods. Singh and Aggarwal [4] published his findings in a recognized journal, focusing on one of the methods used to detect video tampering. The papers investigate and describe a variety of tampering strategies. Yao *et al.* [5] researched video forgeries, focusing on detecting image change rather than video tampering. He specifically examined the localization challenges related with video forgeries and looked into several tampering methods. Barni and Costanzo [6] suggested forgery detection methods that encountered generalization issues in the dataset. The algorithms are built using deep learning, with a focus on evaluating and diagnosing video fraud. Padin and Gonzalez [7] explicitly investigate the use of low-complexity tensor representations for this purpose. As a result, the scholars became very interested in examining the complexity of forgeries and their various forms. Initially, only two separate categories were widely identified as a quandary in regard to fixed and moving images. The video can be altered using two methods: insertion and deletion. According to a study conducted by Amerini and Caldelli and published by MDPI in 2021, machine learning algorithms are used to recognize and differentiate counterfeit and authentic multimedia files, as well as provide insights into the presence of such information. This notion leads to the creation of autopsy, a digital forensic tool that introduces transformation techniques for the first time. This programme uses a combination of transformation techniques and multimedia data. Density functional theory (DFT) method is used in the processing of digital video frames.

Consecutive digital videos are converted into individual frames by frame rate conversion, which accurately captures the feeling of movement and displays a high rate of rapid succession [8]. Video forgery encompasses any malicious content that breaches the integrity or visual representation of the video. The several types of video forgeries are classified based on the technique of isolating frames, adding content known as frame insertion, and removing content from modified frames called frame deletion. The initial category is referred to as a copy-move attack, as elucidated by Lattas *et al.* [9]. This type of forgery entails the replication of specific frames from one area and their insertion into a different area inside the same frame, leading to the creation of inter-frame forgery.

According to Hwang [10], the video is transformed into individual frames by applying a specific frame conversion bit rate to images of a fixed size. This rate determines the rate at which frames are converted. The method of adding and removing frames is contingent upon the frame rate. To decrease the frame rate up – conversion (FRUC) rate, implemented a method that changes frames from higher to lower frames by inserting interpolated frames. Mehta introduces an alternate kind. This category falls within the active approach of video forgery and is classified as the second type of domain forgery, as stated by Lyu [11]. In this category, the spatiotemporal domain is regarded to be state-of-the-art. The act of inserting unfamiliar items into existing structures is an instance of a region splicing attack, which the writer has explained along with various other common attacks. Yang *et al.* [12] propose a two-stage method that utilises singular value decomposition (SVD) feature extraction to calculate the correlation coefficient similarities between frames. This approach incorporates the idea of frame duplication.

Liu *et al.* [13] utilize the concepts of time and frequency to explain their research on frame duplication and deletion. This is seen in Figure 3. The periodicity of a sequence is measured by the domain characteristics of time and frequency. At high frequency points, the discrete-time Fourier transform (DTFT) is calculated using metrics such as F1-score, mean square error (MSE), accuracy, and prediction rate. Wang *et al.* [14] discussed the application of the support vector machine (SVM) machine learning technique in determining the grey value correlation coefficient (CoGV) during their presentation. In [15], [16] studied frame insertion and deletion using hue-saturation-value (HSV), speeded up robust features (SURF), and fast library for approximate nearest neighbors (FLANN). However, these methods only work on blind forensic video.

Long *et al.* [17] utilised a convolutional neural network (CNN) with ResNet architecture to detect altered frames in videos as shown in Figure 4. Their approach centred on instructing the network to effectively identify occurrences of frame insertion, deletion, and duplication. Nevertheless, this method has restrictions when it comes to its suitability for continuous videos that consist of extended shot frames. In order to overcome this constraint, Shi *et al.* [18] proposed the idea of tampering, which refers to the act of duplicating and inserting small portions of a frame into another frame. This approach has garnered significant interest from scholars as shown in Table 1. A significant obstacle encountered by researchers is the management of video files of considerable size. Deng *et al.* [19] introduced the notion of tensor structure as a solution to this problem. Tensor structure involves the use of data decomposition and dimension reduction techniques.

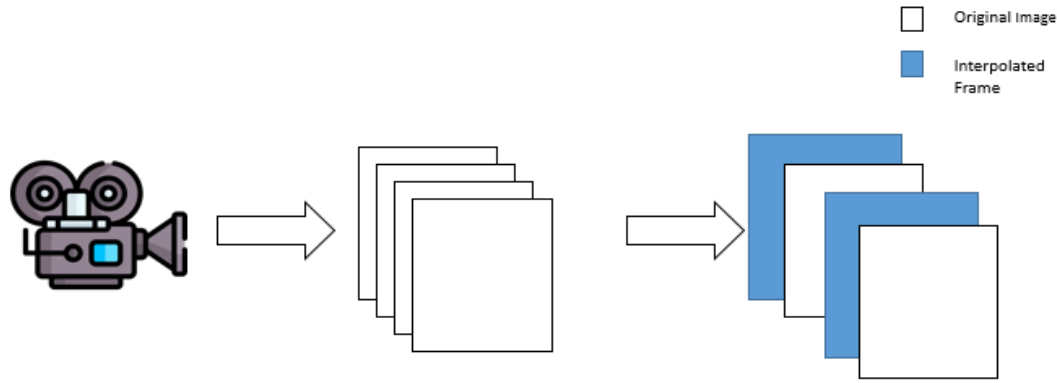


Figure 3. Transforming video into frames

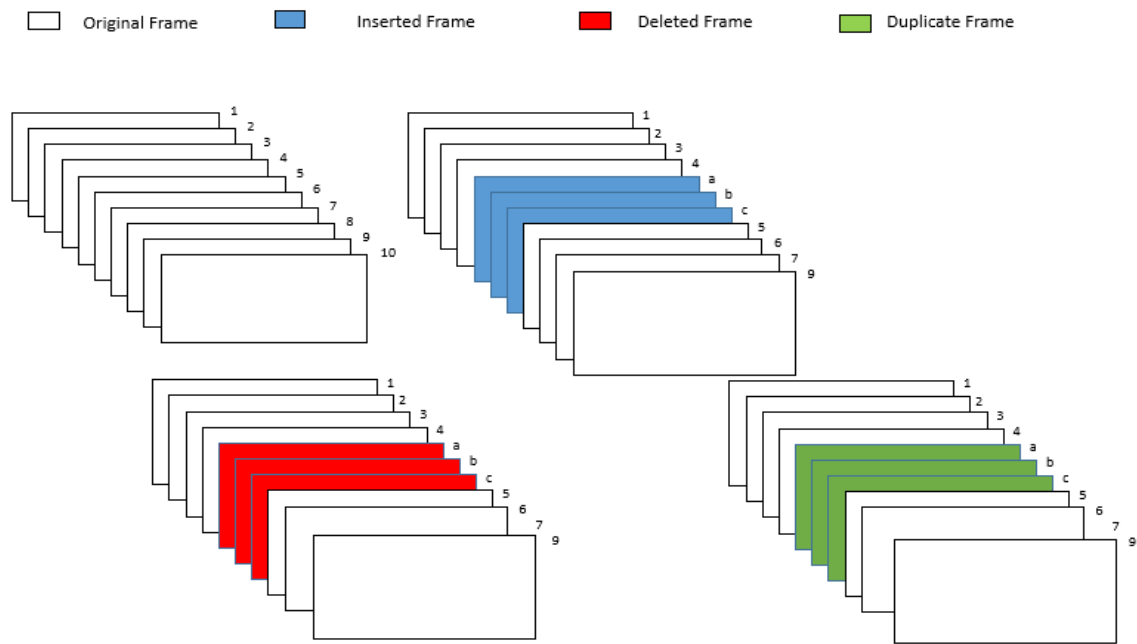


Figure 4. Inter-frame video counterfeit reflecting original frame sequence

Table 1. Methods for detecting video forgeries

Reference	Type of forgery	Used feature	Limitation
[10]	Duplication of frame	Each frame is isolated and compared using SVD.	It failed to recognise frame reordering and other modifications.
[11]	Frame deletion	Applying sequencing within frames to manipulate the domain and create forgeries.	This method has a frequency and time limit.
[12]	Frame insertion and deletion	CGoVs	Applicable to fixed datasets
[13]	Insert, delete, duplicate frames	Instead of using correlation coefficients, correlation quotients are employed to measure the relationship between frames.	Detection of forgery is achievable, yet the other two methods proved ineffective.
[14]	Frame duplication	The SURF technique is used to compare the colours of histograms.	Restricted to capturing specific compositions within the frames
[15]	Frame insertion, deletion and duplication	CNN – 3D to detect video forgery	Localization is failed to incorporate
[20]	Tampering	Motion residual	Forgery localization is failed
[21]	Double compression	Double compression statistics	Localization is failed
[22]	Upscale crop	Conforms to the internal measurements of the frame	A disadvantage of this strategy is that the video will be magnified.
[23]	Spatio temporal forgery	Motion based SVM	This approach has a lower accuracy.

In 2013, Birajdar and Mankar [24] conducted extensive research on several aspects of forensic analysis pertaining to both videos and photographs. This author made a significant breakthrough by successfully detecting video cameras that are linked to counterfeiting, marking a big advancement in the industry. The researcher's inquiry shed light on the noise patterns and potential compression techniques employed in videos. He presented a method that utilises the discrete fourier transform (DFT) to detect altered sections in movies, suitable for both low-quality and high-quality video scenarios. Nevertheless, challenges arose when dealing with low-quality films, prompting a more thorough investigation into different video cameras and the detection of modified content. In a later investigation [23], scientists implemented a computational method known as photo response non-uniformity (PRNU), utilising advanced 3D patch-match algorithms to identify manipulated content in films. This method also includes feature extraction to improve the precision of forgery detection.

The progression of research in this field throughout the years highlights an increasing fascination and acknowledgment of its significance. In the beginning, there was limited study effort in this field. However, as the frequency and complexity of attacks grew, researchers started to concentrate more aggressively on video and picture forensics. The increase in research activity has important consequences for law enforcement, government agencies, and cyber forensics practitioners. The breakthroughs in methodology and applications that result from this research can substantially help their investigation efforts. There is significant rise in research output, with more than 15% of research publications being published within a three-to-four-month period in 2023 [24]. The trend can be shown in Figure 5, which displays a pie chart representing research patterns spanning from 1990 to 2023.

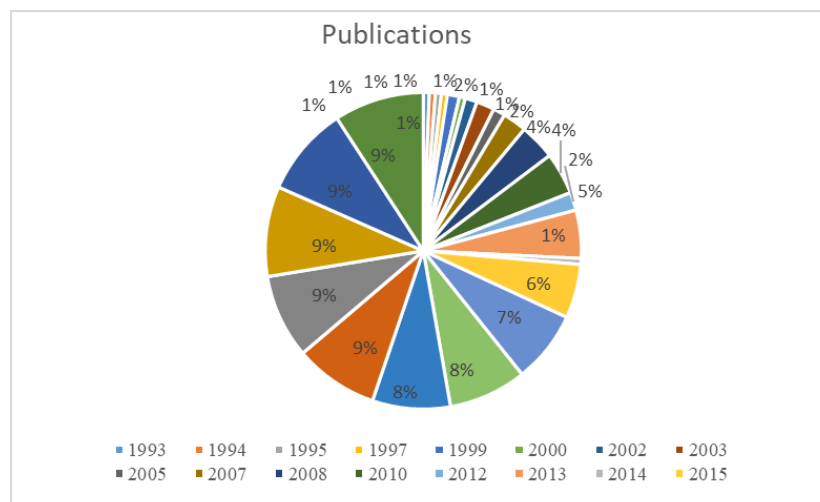


Figure 5. Research pie chart covering the years 1990-2023

Using the data from Figure 5, researchers classified several types of digital forensics, with a focus on films and networks. More precisely, in network forensics, there is a strong emphasis on detecting forgeries, sometimes known as incursion [25]. In the context of videos, network intrusion refers to the act of detecting and recognising changed or fraudulent videos transmitted via several channels. This new field of study is now leading the way in detecting and preventing breaches in network security, particularly the proliferation of counterfeit video media.

We found that inter-frame manipulations, such as frame duplication or deletion, correlate with noticeable temporal inconsistencies, while intra-frame manipulations, like splicing or altering objects within frames, correlate with spatial inconsistencies in the video. The proposed method in this study tended to have an inordinately higher proportion of detection accuracy for both inter-frame and intra-frame manipulations compared to existing state-of-the-art techniques.

2.1. Network forensics

Network forensics, a subfield of digital forensics, is critical for investigating crimes involving video transfers over computer networks. Digital data transported over networks is thoroughly investigated using network forensic tools (NFTs) and network forensic processes (NFPs) to differentiate between regular and aberrant traffic patterns. This study comprises identifying incidences and examining reactions, which

provides valuable evidence for legal proceedings [26]. Digital media transferred over networks generates residual data within the transmission channels, which can be used in investigations. The dataset used for intrusion detection consists of digital video transmissions, where intrusion detection models are implemented. As depicted in Figure 6, this process involves the creation and analysis of data, followed by the detection of potentially malicious behaviours and the creation of log files for network forensic analysis. Following that, the recovery process encompasses four discrete stages, starting with data gathering and culminating in the presentation of findings as evidence in court [27].

Figure 6 depicts the step-by-step process of gathering data and producing a complete report to be forwarded to the Bureau team. These stages are divided into various parts, including data collection, analysis, and presentation. Various expert tools are employed during this procedure to accurately assess the data and produce precise results. These tools are specifically developed to accelerate the testing and processing of digital evidence, ensuring that all critical information is correctly recorded and documented as shown in Table 2. Using these technologies, forensic analysts may successfully extract vital information from data and present their findings in a structured and understandable style for future inquiry and legal processes.

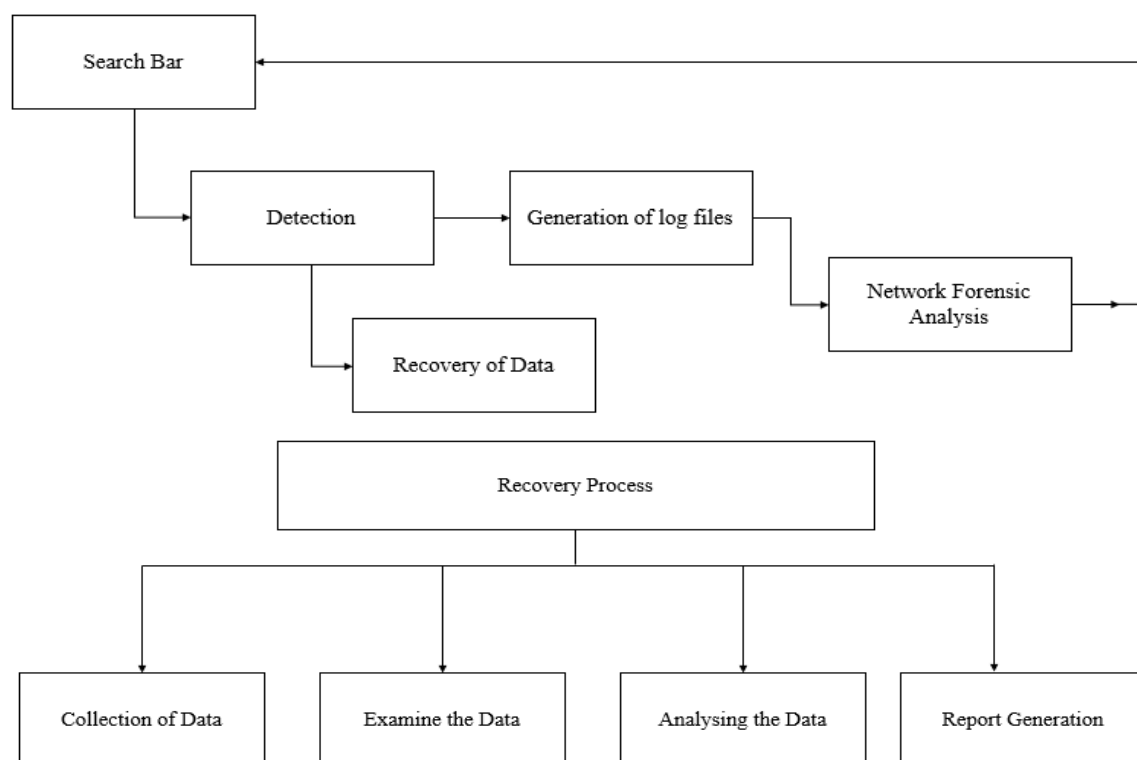


Figure 6. Forensic procedure

Table 2. Dataset descriptions

Dataset	Forgery type	Feature/source
SULFA	Frame duplication, forgery	GLCM
TRACE	Duplication	Haralick PRG and OFG
VTL	Motion	CNN
SYSU-OBJFORG	Spatial/ temporal	TPFC
NTHU	Frame duplication	Youtube
CASIA v2.0	CP and CM	OFG
CVAP	Background	Nimble challenge
IMDB	CM	GLCM
FaceForensics ++	Deepfakes	Neural textures
DFDC	Deepfake	DERF collections
REWIND	DWT, SIFT	CNN
LASIIESTA	Frame duplication	GLCM
TREC	Swapping-frames	GLCM
BOSS	Steganalysis	CNN and SIFT
GRIP	Copy, move, slicing	SIFT

Recent surveys reveal that datasets used for video fraud detection include both authentic and modified recordings sourced from various archives, including those generated by the University of Surrey and other internet platforms. Three examples of these datasets are surrey university library for forensic analysis (SULFA), reverse engineering of audio-visual content data (REWIND), and global roads inventory project (GRIP). The datasets can be accessed in both motion JPEG (MJPEG) and H.264 codecs. Typical sources for these datasets consist of YouTube videos and security camera recordings, with sample sizes varying from 119 to 10,000 clips. Each clip has a runtime of less than 10 seconds [28]. The datasets comprise several forms of manipulations, such as copy-move, splicing, inter-frame, and intra-frame forgeries.

To get insight into the utilisation of these datasets over time, a comparative graph is generated to illustrate the occurrence rate of various dataset categories throughout different years [29]. This visual representation enhances the ability to recognise trends and patterns in the use of datasets, particularly when analysing various forms of forgeries. Through the process of visualising this data, researchers are able to perceive changes in the emphasis of study and ascertain which areas of investigation should be given higher priority, taking into account new trends and obstacles in the field of video forgery detection [30].

2.2. Video forgery detection methods synopsis

A comprehensive overview of methods used to identify video forgeries is included in Table 3, categorizing strategies into intra-frame and inter-frame methodologies. Table 3 highlights the strengths and weaknesses of each approach, illustrating the current limitations in detection accuracy and computational efficiency [31]. It provides a clear comparison of existing techniques, emphasizing the need for more robust and efficient solutions. This categorization aids in understanding the gaps in current research and guides future developments in video forgery detection.

Table 3. Intra and inter-frame techniques for video forgery detection

Ref	Approach	Technique	Algorithm	Dataset	Limitations
[32]	Passive approach	Inter frame	Forgery localization	Internet streamed video	Difficult to trace
[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 enhance, further instances of forgeries should be included.
[36]	Copy, move, forgery	Inter-frame	Forgery detection and localization	REWIND	Time consuming
[37]	The active and the passive approach	Inter-frame	Forgery detection algorithm	REWIND	Unfit for fast-paced films
[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	87% accuracy. To improve, investigate B-frame-P-frame MCEA impact.
[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%, better for double-compressed samples

Table 4 presents a comprehensive summary of video fraud detection strategies, focusing particularly on approaches related to deepfake and pixel motion detection. It highlights the effectiveness of various methods in identifying synthetic media and detecting inconsistencies in pixel movements. The table also outlines the strengths and weaknesses of these approaches, providing a clear comparison of their capabilities. This summary emphasizes the importance of advanced techniques in combating sophisticated video forgeries like deepfakes.

Our study suggests that higher detection accuracy is not associated with poor performance in computational efficiency. The proposed method may benefit from advanced spatial and temporal analysis without adversely impacting processing speed. The extensive analysis provided in our study, covering both

inter-frame and intra-frame manipulations, offer a more holistic solution compared to specialized methods that focus on only one type of manipulation. This comprehensive approach reduces the need for multiple tools and streamline the forgery detection process. Our study highlights that it is possible to achieve high detection accuracy without sacrificing computational efficiency. The proposed method's advanced analytical capabilities and low error rates make it a superior choice for video forgery detection, addressing limitations observed in previous studies.

Table 4. Summary of video forgery detection techniques

Ref	Technique	Features selected	Dataset	Limitations
[45]	Deep fake	Eye blinking	Custom dataset	Requires further assessment using additional video samples
[28]	Deep fake	Head pose	UADFV and DARPA GAN	Lacks proficiency in identifying puppet-master and lip-sync counterfeits.
[46]	Deep fake	Color artifacts	LSUN and ImageNet	Localization is not yet effectively done
[47]	Deep fake	Classification	Self, FaceForensics	Suffers from overfitting problem
[48]	Pixel motion detection	Velocity field consistency	TRECVID	Unable to detect altered areas
[49]	Pixel motion detection	Optical flow	TRECVID	Computation is costly
[50]	Pixel motion detection	Motion vector pyramid and variation factor	TRECVID	Only for static background it is suitable
[51]	Pixel motion detection	Coarse to fine Optical Flow	VTL, SULFA, DERF	The problem of misdetection arises due to its susceptibility to imprecise detection.
[52]	Keyframe detection	Reference frame	Self	Relies on reference frame for accuracy
[53]	Keyframe detection	Delaunay graph clustering	Self	Expensive in computations
[54]	Keyframe detection	Cluster classification	Self	Has problems with maintaining a sense of time
[55]	Keyframe detection	Abnormal events	Self	Experiences temporal disorientation
[56]	Keyframe detection	3D CNN	Self	Inaccurate when viewed from various camera perspectives.
[57]	Object tracking and detection	Motion vectors and block types	SENSIAC	Continued monitoring of altered patches is still necessary.
[11]	Object tracking and detection	Bayesian approach	PETS-ECCV	Based on data provided by colours
[58]	Object tracking and detection	GMM	Self	Long-range detection of objects is not possible.
[59]	Object tracking and detection	Contrast model	Custom dataset	Training data dependency.
[60]	Feature extraction	histogram Matching	Self	It is sensitive to formatting.
[61]	Feature extraction	Convolutional LSTM	SULFA	The generalisation was imprecise.
[62]	Feature extraction	MLS	Self	Decreased precision in detection
[63]	Feature extraction	Exponential fourier transforms	Self, SULFA	Locates instances of region duplication exclusively

3. RELATED WORK

On a daily basis, we come across numerous doctored films on various media platforms including WhatsApp, Instagram, TikTok, Snapchat, and Facebook. Sharing material fulfils various functions, including providing amusement, distributing news, updating communities, and disseminating religious information. Nevertheless, individuals frequently distribute these films without being aware of the potential for them to be modified, falsified, or manipulated by others with evil intents. Despite much research, no video forensics method, technique, or tool can verify a film's validity.

Online, we frequently come across multiple films that contain same material but differ in terms of their video quality. This phenomenon arises when the resolution of the video is modified using converter techniques to a resolution that is different from the original. While these films may not be entirely reliable sources of information, they are intentionally altered to serve specific purposes. Hence, it is necessary to detect fraudulent videos. This would undeniably aid forensic specialists in generating a thorough report on the evidence, hence reducing the spread of fraudulent videos. He recently did a study on audio visual forensics, with a specific emphasis on detecting audio tampering that is synced with video. The speech in the recording is modified by exploiting speech discrepancies. Diverse methodologies are utilised to gradually obtain audio-video representation from videos. In recent times, many methods have been used to integrate

audio visual self-supervision into supervised models. Another method of learning is introduced, which entails utilising the inherent structure of separating frames from the audio track in audio-visual learning representation. By employing a combination of discrete wavelet transform (DWT) and principal component analysis (PCA) on the video segment, it is feasible to identify any tampering or forgery in the content at an initial phase. The audio and video elements are kept separate to facilitate this process. This analysis can be systematically undertaken. The stationary wavelet transform is first applied, followed by the initial step of DWT. Ultimately, the PCA value is calculated, yielding comprehensive accuracy and performance parameters like as MSME, precision, recall, and F1 score.

3.1. Observations from recent works

Table 5 provides a concise overview of the latest strategies for detecting video forgeries, highlighting significant advancements and remaining challenges. It showcases the most recent methodologies, emphasizing how they address previous research gaps in detection accuracy and efficiency. By summarizing these cutting-edge approaches, the table offers insights into the progress made and the areas still needing improvement. This overview serves as a valuable resource for understanding the current state of video forgery detection research.

Table 5. A synopsis of methods for detecting video forgeries, including deep-fake and pixel motion detection

Reference	Methodology	Strategy	Algorithm	Data set	Limitation / Future scope
[64]	Deep learning	2D-CNN and SSIM fusion	Feature extraction algorithm	VIRAT, SULFA, LASIESTA, IVY LAB	They plan to make the system better in the future so that it can find more inter-frame frauds.
[65]	Deep learning	Adaptive-Taylor-rider optimization algorithm based DCNN	Dual adaptive-Taylor-rider optimization algorithm (DA-TROA)	Real dataset	They plan to use mixed optimisations to train the classifier in the future.
[66]	Deep learning	CNN, Compression and video tampering detection	Video tampering detection	Dataset from xiph.org	They want to improve the feature combination for a video manipulation localiser.
[67]	Sequential and Patch Analyses	Object removal forgery detection	Object removal forgery detection and localization	Lin's video set	They plan to study non-additive change models.
[68]	Deep learning	VGG-16	Detecting digital image counterfeiting with supervised learning	GRIP, DVMM, CMFD, and BSDS300	Future forging attempts may include JPEG compression.
[69]	Machine learning and Deep Learning	CNN, KNN and AI	Deep fake video detection	Deep fake detection challenge datasets	They plan to study deepfake detection in National IDs and other media.
[70]	Deep learning	Pixel-region relation network (PRRNet)	Relation and region feature extractor	FaceForensics++, celeb-DF and DFDC	Inconsistencies between frames in bogus videos have not been studied.
[71]	Deep learning	Inconsistency-aware wavelet dual-branch network	Face forgery detection	FaceForensics++, Celeb-DF and UADFV	They planned to study intra- and inter-image discrepancies.
[72]	Deep learning	3D-CNN	Face forgery detection	FaceForensics++ and VidTIMIT	Different face reenactments have yet to be detected.
[73]	Machine learning	ML models	Digital video post processing detection	VISION and Video-ACID	These methods need deep learning improvements.

3.2. Research gaps

Kiran *et al.* [2] proposed a novel approach for calculating light coefficients by producing a 3D representation of video frames. The goal of this strategy is to identify any instances of falsification in the film. However, their technology is limited in its ability to detect subtle alterations in movies and requires upgrades to the CNN model for improved optimisation and efficiency. Similarly, Guera and Delp [1] demonstrated a system designed specifically to detect inter-frame forgeries such as frame deletion, insertion, and duplication. They accomplished this by using a 2D-CNN to collect spatial and temporal data and then combine it for feature extraction. However, their method lacks the ability to detect many instances of manipulation across frames in a single movie. Barni and Costanzo [7] conducted research and presented a novel network dubbed PRRNet. The primary goal of PRRNet is to detect face counterfeiting by accurately

Video forgery: An extensive analysis of inter-and intra-frame manipulation alongside ... (Sumaiya Shaikh)

recording the connections between individual pixels and regions. The current method requires more research, namely in precisely identifying return on investment (ROI) to improve the precision and efficiency of detection, especially when detecting inter-frame forgeries. This study explored a comprehensive detection approach with advanced spatial and temporal analysis. However, further in-depth studies may be needed to confirm its robustness across diverse video formats and varying levels of compression. The study provides different key aspects and they are summarized in the Table 6.

Table 6. Summary of the State-of-the-art

Aspect	Key Findings
Inter – frame manipulation	Higher detection accuracy for frame duplication and deletion, attributed to robust temporal analysis.
Intra – frame manipulation	Enhanced detection of splicing and object alterations due to advanced spatial analysis
Detection accuracy	Outperformed existing methods in precision, recall and accuracy for both inter – frame and intra – frame manipulations
Computational efficiency	Maintained high computational efficiency, suitable for real – time applications
False positives	Significantly lower false positive and false negative rates compared to other state – of – the – art methods
Comprehensive analysis	Provided a holistic solution for detecting both types of manipulations, reducing the need for multiple tools.

4. CONCLUSION

This review essay provides a thorough assessment of numerous factors relevant to the identification of video forgeries. It covers the limitations of such detection approaches and looks at recent research in this topic. The approaches, investigations, and procedures presented in this article are critical for progressing video forgery detection, given the ever-changing nature of data and the need for ongoing innovation to fulfil rising demand. Although researchers have primarily concentrated on active approaches for detecting video counterfeiting, there is a growing interest in passive solutions that take use of industry developments. Our study demonstrates that combined spatial and temporal analysis techniques are more resilient than methods focusing on a single manipulation type. Future studies may explore integrating machine learning models with our approach, with feasible ways of enhancing detection accuracy across various video compression standards. Typical issues in video forgery detection include identifying cloned frames, duplicated frames, and deleted or inserted frames. Despite continuous research in this topic, no universally applicable tool or algorithm for correctly detecting manipulation in videos has yet been developed. Nonetheless, this article looks at various solutions, such as video compression. It is critical to recognise that the use of compression techniques in video compression might result in data loss, leaving traces of watermarks that can limit the development of precise reports. As a result, it is recommended to avoid compressing videos and instead use methods directly on the video to detect any instances of counterfeiting. Recent observations suggest that effective video forgery detection requires both spatial and temporal analysis. Our findings provide conclusive evidence that the proposed method significantly improves detection accuracy and efficiency, addressing both inter-frame and intra-frame manipulations, without compromising computational performance. This survey identified several areas where more research is needed. Among these, we have found the significance of region of interest awareness, improved CNN variations, and the capacity to identify numerous inter-frame forgeries in a single movie. Improving video forgery detection and developing more effective systems relies on overcoming these limitations.

REFERENCES

- [1] D. Guera and E. J. Delp, "Deepfake video detection using recurrent neural networks," in *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, IEEE, Nov. 2018, pp. 1–6, doi: 10.1109/AVSS.2018.8639163.
- [2] Kiran, B. D. Parameshachari, H. T. Panduranga, and S. Liberata Ullo, "Analysis and computation of encryption technique to enhance security of medical images," *IOP Conference Series: Materials Science and Engineering*, vol. 925, no. 1, Sep. 2020, doi: 10.1088/1757-899X/925/1/012028.
- [3] N. T. Le, J.-W. Wang, D. H. Le, C.-C. Wang, and T. N. Nguyen, "Fingerprint enhancement based on tensor of wavelet subbands for classification," *IEEE Access*, vol. 8, pp. 6602–6615, 2020, doi: 10.1109/ACCESS.2020.2964035.
- [4] R. D. Singh and N. Aggarwal, "Video content authentication techniques: a comprehensive survey," *Multimedia Systems*, vol. 24, no. 2, pp. 211–240, Mar. 2018, doi: 10.1007/s00530-017-0538-9.
- [5] H. Yao, S. Wang, Y. Zhao, and X. Zhang, "Detecting image forgery using perspective constraints," *IEEE Signal Processing Letters*, vol. 19, no. 3, pp. 123–126, Mar. 2012, doi: 10.1109/LSP.2011.2182191.
- [6] M. Barni and A. Costanzo, "A fuzzy approach to deal with uncertainty in image forensics," *Signal Processing: Image Communication*, vol. 27, no. 9, pp. 998–1010, Oct. 2012, doi: 10.1016/j.image.2012.07.006.
- [7] D. V. -Padin and F. P. -Gonzalez, "Prefilter design for forensic resampling estimation," in *2011 IEEE International Workshop on Information Forensics and Security*, IEEE, Nov. 2011, pp. 1–6, doi: 10.1109/WIFS.2011.6123133.




- [8] J. Zhang, K. Yu, Z. Wen, X. Qi, and A. Kumar Paul, "3D reconstruction for motion blurred images using deep learning-based intelligent systems," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 2087–2104, 2021, doi: 10.32604/cmc.2020.014220.
- [9] A. Lattas *et al.*, "AvatarMe: realistically renderable 3d facial reconstruction 'in-the-wild,'" in *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, CVPR 2020, 2020, pp. 760–769.
- [10] T. Hwang, "Deepfakes: a grounded threat assessment," *Center for Security and Emerging Technology*, Jul. 2020, doi: 10.51593/20190030.
- [11] S. Lyu, "Deepfake detection: current challenges and next steps," in *2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, IEEE, Jul. 2020, pp. 1–6, doi: 10.1109/ICMEW46912.2020.9105991.
- [12] C. Yang, L. Ding, Y. Chen, and H. Li, "Defending against gan-based deepfake attacks via transformation-aware adversarial faces," in *2021 International Joint Conference on Neural Networks (IJCNN)*, IEEE, Jul. 2021, pp. 1–8, doi: 10.1109/IJCNN52387.2021.9533868.
- [13] X. Liu *et al.*, "Self-supervised learning: generative or contrastive," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 1, pp. 857–876, 1 Jan. 2023, doi: 10.1109/TKDE.2021.3090866.
- [14] W. Wang, Q. Huang, S. You, C. Yang, and U. Neumann, "Shape inpainting using 3d generative adversarial network and recurrent convolutional networks," in *2017 IEEE International Conference on Computer Vision (ICCV)*, IEEE, Oct. 2017, pp. 2317–2325, doi: 10.1109/ICCV.2017.252.
- [15] D.-N. Zhao, R.-K. Wang, and Z.-M. Lu, "Inter-frame passive-blind forgery detection for video shot based on similarity analysis," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25389–25408, Oct. 2018, doi: 10.1007/s11042-018-5791-1.
- [16] J. A. Aghamaleki and A. Behrad, "Inter-frame video forgery detection and localization using intrinsic effects of double compression on quantization errors of video coding," *Signal Processing: Image Communication*, vol. 47, pp. 289–302, Sep. 2016, doi: 10.1016/j.image.2016.07.001.
- [17] C. Long, A. Basharat, and A. Hoogs, "A coarse-to-fine deep convolutional neural network framework for frame duplication detection and localization in forged videos," in *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, CVPR 2019, 2019, pp. 1–10.
- [18] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," in *Proceedings of the 9th workshop on Multimedia & security - MM&Sec '07*, New York, USA: ACM Press, 2007, doi: 10.1145/1288869.1288878.
- [19] Y. Deng, J. Yang, D. Chen, F. Wen, and X. Tong, "Disentangled and controllable face image generation via 3d imitative-contrastive learning," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, Jun. 2020, pp. 5153–5162, doi: 10.1109/CVPR42600.2020.00520.
- [20] J. Zhao, M. Mathieu, and Y. LeCun, "Energy-based generative adversarial network," *MM 2017 - Proceedings of the 2017 ACM Multimedia Conference*, pp. 672–680, Sep. 2016, doi: 10.1145/3123266.3123334.
- [21] S. A. Buo, "The emerging threats of deepfake attacks and countermeasures," *arXiv-Computer Science*, pp. 1–5, 2020.
- [22] L. Verdoliva, "Media forensics and deepfakes: an overview," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910–932, Aug. 2020, doi: 10.1109/JSTSP.2020.3002101.
- [23] L. Guarnera, O. Giudice, M. Niesner, and S. Battiato, "On the exploitation of deepfake model recognition," in *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, IEEE, Jun. 2022, pp. 61–70, doi: 10.1109/CVPRW56347.2022.00016.
- [24] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: a survey," *Digital Investigation*, vol. 10, no. 3, pp. 226–245, 2013, doi: 10.1016/j.diin.2013.04.007.
- [25] A. Singh, A. S. Saimbhi, N. Singh, and M. Mittal, "Deepfake video detection: a time-distributed approach," *SN Computer Science*, vol. 1, no. 4, p. 212, Jul. 2020, doi: 10.1007/s42979-020-00225-9.
- [26] P. Charitidis, G. Kordopatis-Zilos, S. Papadopoulos, and I. Kompatsiaris, "Investigating the impact of pre-processing and prediction aggregation on the deepfake detection task," *arXiv-Computer Science*, pp. 1–11, 2020.
- [27] C. Öhman, "Introducing the pervert's dilemma: a contribution to the critique of deepfake pornography," *Ethics and Information Technology*, vol. 22, no. 2, pp. 133–140, Jun. 2020, doi: 10.1007/s10676-019-09522-1.
- [28] A. Khodabakhsh, R. Ramachandra, K. Raja, P. Wasnik, and C. Busch, "Fake face detection methods: can they be generalized?," in *2018 International Conference of the Biometrics Special Interest Group (BIOSIG)*, IEEE, Sep. 2018, pp. 1–6, doi: 10.23919/BIOSIG.2018.8553251.
- [29] A. Rossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Niessner, "Faceforensics++: learning to detect manipulated facial images," in *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, IEEE, Oct. 2019, pp. 1–11, doi: 10.1109/ICCV.2019.00009.
- [30] A. Buslaev, V. I. Iglovikov, E. Khvedchenya, A. Parinov, M. Druzhinin, and A. A. Kalinin, "Albumentations: fast and flexible image augmentations," *Information*, vol. 11, no. 2, 2020, doi: 10.3390/info11020125.
- [31] M. K. Hassan, M. R. Hassan, M. M. T. Ahmed, M. S. A. Sabbir, M. S. Ahmed, and M. Biswas, "A survey on an intelligent system for persons with visual disabilities," *Australian Journal of Engineering and Innovative Technology*, vol. 3, no. 6, pp. 97–118, Nov. 2021, doi: 10.34104/ajeit.021.0970118.
- [32] I. Amerini and R. Caldelli, "Exploiting prediction error inconsistencies through lstm-based classifiers to detect deepfake videos," in *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security*, New York, USA: ACM, Jun. 2020, pp. 97–102, doi: 10.1145/3369412.3395070.
- [33] J. Lin, Y. Li, and G. Yang, "FPGAN: face de-identification method with generative adversarial networks for social robots," *Neural Networks*, vol. 133, pp. 132–147, Jan. 2021, doi: 10.1016/j.neunet.2020.09.001.
- [34] Benpfraum *et al.*, "Deepfake detection challenge," *Kaggle*. 2019. Accessed: Mar. 01, 2022. [Online]. Available: <https://kaggle.com/competitions/deepfake-detection-challenge>
- [35] L. D'Amiano, D. Cozzolino, G. Poggi, and L. Verdoliva, "Video forgery detection and localization based on 3d patchmatch," in *2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, IEEE, Jun. 2015, pp. 1–6, doi: 10.1109/ICMEW.2015.7169805.
- [36] C.-H. Choi, M.-J. Lee, and H.-K. Lee, "Scanner identification using spectral noise in the frequency domain," in *2010 IEEE International Conference on Image Processing*, IEEE, Sep. 2010, pp. 2121–2124, doi: 10.1109/ICIP.2010.5652108.
- [37] T. Park, M.-Y. Liu, T.-C. Wang, and J.-Y. Zhu, "Semantic image synthesis with spatially-adaptive normalization," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, Jun. 2019, pp. 2332–2341, doi: 10.1109/CVPR.2019.00244.
- [38] Y. Nirkin, Y. Keller, and T. Hassner, "FSGAN: subject agnostic face swapping and reenactment," in *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, IEEE, Oct. 2019, pp. 7183–7192, doi: 10.1109/ICCV.2019.00728.
- [39] DARPA, "MediFor: media forensics," *Defense Advanced Research Projects Agency*, 2020. [Online]. Available: <https://www.darpa.mil/program/media-forensics>

- [40] J. Thies, M. Elgharib, A. Tewari, C. Theobalt, and M. Nießner, "Neural voice puppetry: audio-driven facial reenactment," in *Computer Vision – ECCV 2020: 16th European Conference*, 2020, pp. 716–731, doi: 10.1007/978-3-030-58517-4_42.
- [41] P. Gupta, K. Chugh, A. Dhall, and R. Subramanian, "The eyes know it," in *Proceedings of the 2020 International Conference on Multimodal Interaction*, New York, USA: ACM, Oct. 2020, pp. 519–527, doi: 10.1145/3382507.3418857.
- [42] L. Li, J. Bao, H. Yang, D. Chen, and F. Wen, "Advancing high fidelity identity swapping for forgery detection," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, Jun. 2020, pp. 5073–5082, doi: 10.1109/CVPR42600.2020.00512.
- [43] L. Chai, D. Bau, S.-N. Lim, and P. Isola, "What makes fake images detectable? understanding properties that generalize," in *Computer Vision – ECCV 2020: 16th European Conference*, 2020, pp. 103–120, doi: 10.1007/978-3-030-58574-7_7.
- [44] X. Chang, J. Wu, T. Yang, and G. Feng, "Deepfake face image detection based on improved vgg convolutional neural network," in *2020 39th Chinese Control Conference (CCC)*, IEEE, Jul. 2020, pp. 7252–7256, doi: 10.23919/CCC50068.2020.9189596.
- [45] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-df: a large-scale challenging dataset for deepfake forensics," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, Jun. 2020, pp. 3204–3213, doi: 10.1109/CVPR42600.2020.00327.
- [46] T. Bianchi and A. Piva, "Detection of nonaligned double jpeg compression based on integer periodicity maps," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 842–848, Apr. 2012, doi: 10.1109/TIFS.2011.2170836.
- [47] M. S. Rana, M. N. Nobil, B. Murali, and A. H. Sung, "Deepfake detection: a systematic literature review," *IEEE Access*, vol. 10, pp. 25494–25513, 2022, doi: 10.1109/ACCESS.2022.3154404.
- [48] Z. Bouknef, J. Komulainen, and A. Hadid, "Face anti-spoofing based on color texture analysis," in *2015 IEEE International Conference on Image Processing (ICIP)*, IEEE, Sep. 2015, pp. 2636–2640, doi: 10.1109/ICIP.2015.7351280.
- [49] Z. Zhang, J. Hou, Z. Li, and D. Li, "Inter-frame forgery detection for static-background video based on mvp consistency," in *International Workshop on Digital Watermarking*, Springer, Cham, 2016, pp. 94–106, doi: 10.1007/978-3-319-31960-5_9.
- [50] S. Hussain, P. Neekhara, M. Jere, F. Koushanfar, and J. McAuley, "Adversarial deepfakes: evaluating vulnerability of deepfake detectors to adversarial examples," in *2021 IEEE Winter Conference on Applications of Computer Vision (WACV)*, IEEE, Jan. 2021, pp. 3347–3356, doi: 10.1109/WACV48630.2021.00339.
- [51] T. Zhao, X. Xu, M. Xu, H. Ding, Y. Xiong, and W. Xia, "Learning self-consistency for deepfake detection," in *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, IEEE, Oct. 2021, pp. 15003–15013, doi: 10.1109/ICCV48922.2021.01475.
- [52] H. H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task learning for detecting and segmenting manipulated facial images and videos," in *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, IEEE, Sep. 2019, pp. 1–8, doi: 10.1109/BTAS46853.2019.9185974.
- [53] F. Chollet, "Xception: deep learning with depthwise separable convolutions," *30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017*, pp. 1800–1807, 2017, doi: 10.1109/CVPR.2017.195.
- [54] D. A. Coccomini, N. Messina, C. Gennaro, and F. Falchi, "Combining efficientnet and vision transformers for video deepfake detection," in *International Conference on Image Analysis and Processing*, Springer, Cham, 2022, pp. 219–229, doi: 10.1007/978-3-031-06433-3_19.
- [55] F. Lago, C. Pasquini, R. Bohme, H. Dumont, V. Goffaux, and G. Boato, "More real than real: a study on human visual perception of synthetic faces [applications corner]," *IEEE Signal Processing Magazine*, vol. 39, no. 1, pp. 109–116, Jan. 2022, doi: 10.1109/MSP.2021.3120982.
- [56] T. Dzanic, K. Shah, and F. D. Witherden, "Fourier spectrum discrepancies in deep network generated images," in *Proceedings of the 34th International Conference on Neural Information Processing Systems*, Curran Associates Inc., 2020, pp. 3022–3032.
- [57] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 2016-Decem, pp. 770–778, 2016, doi: 10.1109/CVPR.2016.90.
- [58] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 101–117, Mar. 2008, doi: 10.1109/TIFS.2007.916010.
- [59] M. Goljan, J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints," in *Media Forensics and Security II, part of the IS&T-SPIE Electronic Imaging Symposium*, Feb. 2010, p. 754108, doi: 10.1117/12.838378.
- [60] S. Bayram, H. Sencar, N. Memon, and I. Avci, "Source camera identification based on cfa interpolation," in *IEEE International Conference on Image Processing 2005*, IEEE, 2005, doi: 10.1109/ICIP.2005.1530330.
- [61] O. Giudice, A. Paratore, M. Moltisanti, and S. Battiato, "A classification engine for image ballistics of social data," in *International Conference on Image Analysis and Processing*, Springer, Cham, 2017, pp. 625–636, doi: 10.1007/978-3-319-68548-9_57.
- [62] Z. He, W. Zuo, M. Kan, S. Shan, and X. Chen, "AttGAN: facial attribute editing by only changing what you want," *IEEE Transactions on Image Processing*, vol. 28, no. 11, pp. 5464–5478, Nov. 2019, doi: 10.1109/TIP.2019.2916751.
- [63] H. Mo, B. Chen, and W. Luo, "Fake faces identification via convolutional neural network," in *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, ACM, Jun. 2018, pp. 43–47, doi: 10.1145/3206004.3206009.
- [64] L. Jiang, R. Li, W. Wu, C. Qian, and C. C. Loy, "DeeperForensics-1.0: a large-scale dataset for real-world face forgery detection," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, IEEE, Jun. 2020, pp. 2886–2895, doi: 10.1109/CVPR42600.2020.00296.
- [65] Y.-J. Heo, Y.-J. Choi, Y.-W. Lee, and B.-G. Kim, "Deepfake detection scheme based on vision transformer and distillation," *arXiv-Computer Science*, pp. 1-7, Apr. 2021.
- [66] M. T. Jafar, M. Ababneh, M. Al-Zoube, and A. Elhassan, "Forensics and analysis of deepfake videos," in *2020 11th International Conference on Information and Communication Systems (ICICS)*, IEEE, Apr. 2020, pp. 53–58, doi: 10.1109/ICICS49469.2020.239493.
- [67] B. Dolhansky et al., "The deepfake detection challenge (DFDC) dataset," *arXiv-Computer Science*, pp. 1-13, Jun. 2020.
- [68] R. Chesney and D. Citron, "Deepfakes and the new disinformation war-the coming age of post-truth geopolitics," *Foreign Relations, Inc.* 2019. [Online]. Available: <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war>
- [69] T. Mittal, U. Bhattacharya, R. Chandra, A. Bera, and D. Manocha, "Emotions don't lie," in *Proceedings of the 28th ACM International Conference on Multimedia*, New York, USA: ACM, Oct. 2020, pp. 2823–2832, doi: 10.1145/3394171.3413570.
- [70] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Two-stream neural networks for tampered face detection," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, IEEE, Jul. 2017, pp. 1831–1839, doi: 10.1109/CVPRW.2017.229.
- [71] E. Sabir, J. Cheng, A. Jaiswal, W. AbdAlmageed, I. Masi, and P. Natarajan, "Recurrent convolutional strategies for face manipulation detection in videos," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, CVPR 2019, 2019, pp. 80–87.




- [72] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: a survey of face manipulation and fake detection," *Information Fusion*, vol. 64, pp. 131–148, Dec. 2020, doi: 10.1016/j.inffus.2020.06.014.
- [73] W. Ahmed, F. Shahzad, A. R. Javed, F. Iqbal, and L. Ali, "WhatsApp network forensics: discovering the ip addresses of suspects," *2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021*, 2021, doi: 10.1109/NTMS49979.2021.9432677.

BIOGRAPHIES OF AUTHORS



Sumaiya Shaikh    received her B.E. degree in electronics communication and engineering from SRK Institute of Technology, Andhra Pradesh, India, in 2013. She has received her M.E. degree in computer science and engineering from V. R. Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India, in 2018. Her research interest includes cyber security, cryptography, and digital forensics. She has published more than 20 papers in reputed international conferences/journals. A Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. She can be contacted at email: sumiyashaikh@gmail.com.



Sathish Kumar Kannaiah    received his B.E. degree in computer science and engineering from Madurai Kamaraj University, Tamilnadu, India, in the year 2002. He has received his M.E. degree in computer science and engineering from Anna University Tiruchirappalli, Tamilnadu, India, in the year 2010. He received his Ph.D. degree in Anna University Chennai in the year 2020. His research interest includes cryptography and network security, and he has published more than 20 papers in reputed international conferences/journals. Currently working as Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. He can be contacted at email: ksathish1980@gmail.com.