International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 6, December 2023, pp. 6324~6334
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i6.pp6324-6334

A survey on passive digital video forgery detection techniques

Liba Manopriya Jegaveerapandian[1], Arockia Jansi Rani[1], Prakash Periyaswamy[2], Sakthivel Velusamy[2]
[1]Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India
[2]School of Computer Science Engineering, Vellore Institute of Technology, Chennai, India

Article Info

Article history:

Received Jul 7, 2022
Revised Sep 16, 2022
Accepted Jun 23, 2023

Keywords:

Active and passive techniques
Deep learning
Inter-frame forgery
Intra-frame forgery
Video forgery

ABSTRACT

Digital media devices such as smartphones, cameras, and notebooks are becoming increasingly popular. Through digital platforms such as Facebook, WhatsApp, Twitter, and others, people share digital images, videos, and audio in large quantities. Especially in a crime scene investigation, digital evidence plays a crucial role in a courtroom. Manipulating video content with high-quality software tools is easier, which helps fabricate video content more efficiently. It is therefore necessary to develop an authenticating method for detecting and verifying manipulated videos. The objective of this paper is to provide a comprehensive review of the passive methods for detecting video forgeries. This survey has the primary goal of studying and analyzing the existing passive techniques for detecting video forgeries. First, an overview of the basic information needed to understand video forgery detection is presented. Later, it provides an in-depth understanding of the techniques used in the spatial, temporal, and spatio-temporal domain analysis of videos, datasets used, and their limitations are reviewed. In the following sections, standard benchmark video forgery datasets and the generalized architecture for passive video forgery detection techniques are discussed in more depth. Finally, identifying loopholes in existing surveys so detecting forged videos much more effectively in the future are discussed.

Corresponding Author:

Liba Manopriya Jegaveerapandian
Department of Computer Science and Engineering, Manonmaniam Sundaranar University
Tirunelveli, Tamilnadu, India
Email: libamanopriya06@gmail.com

1. INTRODUCTION

In today's technology-driven world, multimedia data such as videos and images can be modified or forged maliciously through the use of editing tools such as Adobe Photoshop, Premiere Pro, Final Cut Pro X, and Filmora. Also, users can edit video content easily with today's digital devices, such as smartphones, laptops, and personal computers. Digital forgery is being used in digital cinema to create fake scenes in movies, and the rapidly rising trend is reflected in the negative use of such technology. Videos and images play a significant role in litigation, especially when used as evidence. Video surveillance has recently become indispensable for providing specific evidence of a crime [1]. In recent years, video surveillance has become important to social security. Additionally, courts use videos as evidence of a crime, though the originality of the video content cannot be verified by the naked eye. Attackers can forge recorded videos quickly using a slew of media editing tools, culminating in security issues [2]. Further, authorizing surveillance videos is a challenge for law enforcement, journalism, the military, and government agencies.

This paper is structured as follows: section 2 presents an overview of video forgery detection as it relates to forgery types. Section 3 reviews video forgery detection mechanisms or methods. Section 4 discusses the framework of the video forgery detection process and describes the datasets used to detect video forgeries, while section 5 discusses the limitations of the existing techniques. Finally, section 6 concludes the article with final observations.

2. THEORETICAL FRAMEWORK OF VIDEO FORGERY: AN OVERVIEW

A video is a collection of frames that displays images continuously and creates visible movement. Videos are represented in two dimensions, with rows and columns denoting the spatial, and time denoting the temporal dimension. Forgery or tampering or doctoring destroys the information in a video. Checking the authenticity and integrity of videos is a significant component of video forensics. Although traces of forgery cannot be seen with the naked eye, computational techniques can help detect if a video is forged. In this way, digital crimes may be reduced by ensuring that the video evidence available is entirely reliable.

2.1. Types of video forgery

Inter-frame and intra-frame forgery in digital video classify distinct manipulations within video frames. Inter-frame forgery involves modifications between frames, while intra-frame forgery pertains to alternations within individual frames.

a) Inter-frame video forgery: Inter-frame video forgery comprises the four operations of frame insertion, deletion, duplication, and shuffling, as shown in Figure 1. In particular, Figure 1(a) showcases an original video sequence.
   - Frame insertion: A single frame or a set of frames, from the same video or another, is inserted. The width and height of the inserted frame are the same, regardless of whether the frame comes from the same video or a different one. Figure 1(b) depicts frame insertion occurring between the F2 and F3 frames.
   - Frame deletion: Surveillance video systems are often subject to attacks of this type, where a particular video may be singled out to obliterate the presence of an intruder. This is done by deliberately effacing a single frame, or a set of frames, from a video sequence of a particular shot. In Figure 1(c), the deleted frames are located between F2 and F5.
   - Frame duplication: Duplication refers to the process of copying a set of frames in a video sequence and pasting it onto the same video in a different temporal location so the same scenario repeats itself. Figure 1(d) depicts frame duplication, where frames F2 is copied and placed between frames F3 and F4.
   - Frame shuffling: Frame shuffling changes the temporal location of the frame to reorder or interchange the frame sequence and generates misleading information as it pertains to a particular scenario. Figure 1(e) shows the order of the frames changed from F2 to F5.

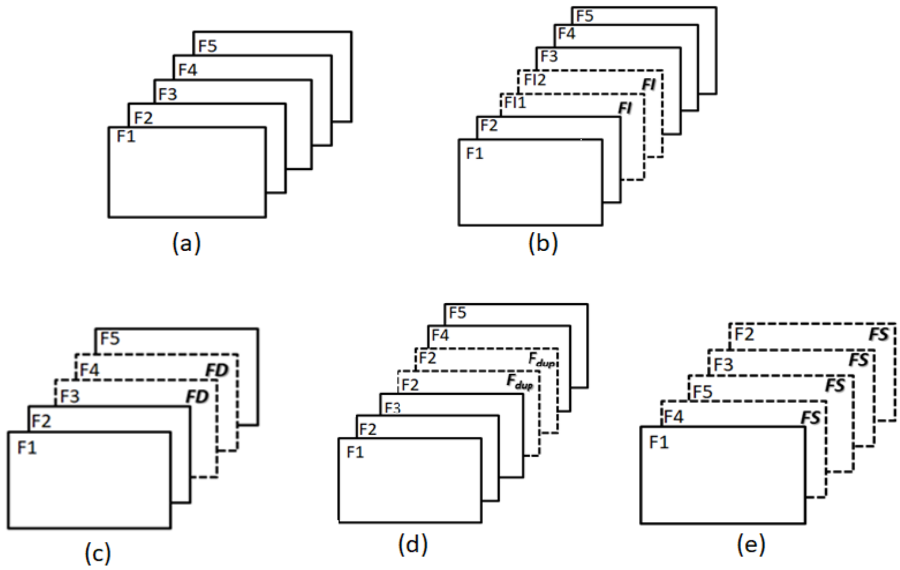

Figure 1. Inter-frame forgeries in a digital video (a) original video sequence, (b) frame insertion (*FI*), (c) frame deletion (*FD*), (d) frame duplication (F_{dup}), and (e) frame shuffling (*FS*)

b) Intra-frame video forgery: This type of forgery involves attacks at two levels, upscale crop and object addition/deletion.
   - Upscale-crop: With this type of forgery, a significant part of the frame is cropped and deleted from a particular scene, following which the frame is enlarged to match the dimensions.
   - Object addition or deletion: This kind of forgery involves copying an object or region from a particular place and positioning it elsewhere. Apart from creating a new video sequence, any object may be added to/removed from the video sequence. This is also known as partial manipulation, copy-paste, or copy-move video forgery. With such easy editing tools for frames (insertion, deletion, shuffling, and duplication) or objects, videos can be forged easily. Also, detection is much more difficult when complex processes like rotation, compression, and resizing occur.

3. VIDEO FORGERY DETECTION MECHANISMS/METHODS

Video forgery detection methods are classified into two, active and passive. The active approach uses a digital signature or a watermarking technique that is embedded in the information/data and is transferred to a frame either before being broadcast or during its creation, depending on the detailed information ascertained earlier in the video. In contrast, passive video forgery detection requires no previous details about the video and is, therefore, termed blind or passive. In the past, forged videos were detected using the active method. However, it is impossible to insert a pre-embedding watermark in every surveillance camera because it reduces the video quality. Further, de-watermarking software easily removes traces of watermarking evidence. Therefore, the passive method is applied to verify the authenticity of a video, using no pre-embedded information and only examining the intrinsic features.

3.1. Techniques used in video forgery detection

This section describes the techniques used in inter-and intra-frame video forgery detection. Statistics-based methods are commonly used to analyze inter-frame forgeries such as frame insertion, deletion, duplication, and shuffling. Spatial, temporal, and spatio-temporal forgery detection techniques are discussed in detail in the following sections.

3.2. Spatial domain forgery detection

This procedure detects forgery in which objects are added or deleted to/from a video scene. Saddique *et al.* [3] developed a new texture descriptor called the chrominance value of consecutive frame difference (CCD), coupled with the discriminative robust local binary pattern (DRLBP), to ascertain inconsistencies in forged videos and the support vector machine (SVM) to detect a forgery. The drawback of the scheme is that a pasted object cannot be determined accurately if it is part of the same frame. Chittapur *et al.* [4] proposed an approach called frame similarity. Based on the backtracking method, frames are partitioned into blocks and the similarity between them is calculated. To detect a forgery, the approach maps the block comparison technique to identify differences in intensity between blocks. Using this method, each block must be mapped to its source, and this is a fundamental limitation of the system. Gavade and Chougule [5] exploited the scale invariant feature transform (SIFT) technique to extract features and discover the region forged using the random sample consensus (RANSAC), which reduces false matching and improves accuracy. However, when the environment light changed in the video, the texture of the adjacent frames changed as well, leading to a false match. Su *et al.* [6] developed a method to detect forgeries in static and complex backgrounds. The energy factor identifies a forged frame by extracting a particular region in the detected frame using an adaptive parameter-based visual background extractor (AVIBE) algorithm. It identifies a specific part of the tampered trace, though not the whole.

Fayyaz *et al.* [7] computed the sensor pattern noise (SPN) to discover noise residue in a video using the average discrete cosine transform (DCT) method to detect and localize forged areas. This approach has the disadvantage of being computationally expensive and complex. Al-Sanjary *et al.* [8] estimated the optical flow using two successive frame features. In this technique, pixel- and block-based estimation is undertaken to detect copy-move forgery videos. The limitation of this approach is that forged areas are not detected in their entirety. Raskar and Shah [9] utilized copy-move video forgery detection using the histogram of second-order gradients (VFDHSOG) technique. A correlation coefficient value of the contrast limited adaptive histogram equalization (CLAHE) identifies suspicious frames. To detect a copy-move forgery, the value of the histogram of second-order gradients (HSOG) is computed by calculating the distance and similarity threshold. The effectiveness of this technique depends on how it is applied to determine a threshold. Ren *et al.* [10] presented a technique that identifies duplicate regions using the improved Levenshtein distance, but this experiment cannot be applied to identifying duplicate regions using dynamic backgrounds. To extract noise features using temporal correlation, Sadddique *et al.* [11] suggested a technique that merged the video binary pattern (VBP) and extreme learning machine (ELM) with the radial basis function (RBF), offering better accuracy and low computation costs. The limitation of this method is that video sequences of extremely short lengths cannot be dealt with effectively. Rodriguez-Ortega *et al.* [12] worked on generalizing custom and transfer learning models using the VGG-16. A large volume of data is used to evaluate the model in this case. In addition, the transfer learning model produces better results than the custom model, since the VGG-16 activates the frozen point when the system degrades, while simultaneously improving accuracy. This contrasts with models constructed with transfer learning, which have more parameters and take a longer estimation time than models constructed with custom architectures. Hu and Lu [13] analyzed the architecture to extract spatial and temporal information using ResNet and the SiameseLSTM after fusing the information to facilitate the classification of forged and original videos. In this case, a convolutional neural network (CNN) and a recurrent neural network (RNN) are utilized to extract spatial and temporal features respectively. This model is limited in that it uses a large number of parameters, which makes it difficult to train the dataset.

Khudhur *et al.* [14] developed a method for detecting region duplication forgery. Each pixel of the luminance part of the image is divided into blocks of overlapping pixels. To extract the significant features from the image, DCT is applied to each block. A k-mean clustering algorithm is used for classification purposes. To sort the values according to the most significant digit (MSD) radix sort algorithm, and then find the correlation values. Using the correlation values, determine whether the forgery has taken place. According to Yang *et al.* [15] head pose inconsistency can be used as a method to detect deepfake faces. This type of forgery involves splicing and manipulating different parts of the face. Using the face detector to extract the facial landmarks and head poses are calculated for the whole and central face regions, then feature vectors are derived. By analyzing the feature values of the deep fake images, the SVM classified the images in which the real images have small values, and the fake images have large values. A technique called photo response non-uniformity (PRNU) analysis was suggested by Koopman *et al.* [16]. This technique involves cropping the extracted frames and splitting them evenly among eight groups. PRNU mean values are calculated for each group and then compared with those of the other groups. Based on the normalized cross-correlation values, classification is carried out. Li *et al.* [17], utilized the eye blink estimation principle in their framework for detecting deepfake videos. They used CNN based on VGG in the first phase, and long-term recurrent CNN in the second phase to detect forgeries. According to Guera and Delp [18], deepfake videos can be efficiently detected by the simple convolution long short-term memory (LSTM) model. An Xception model was used by Ganguly *et al.* [19] to extract the features of the face region. A feature map is generated from an affine transformed value. The purpose of this classification is to determine whether an image is genuine or not based on the discriminant and relevant features that appear in the face property database. Wang *et al.* [20] developed a method for detecting fake faces based on dual streams and dual utilization. To detect the inter-frame correlation, use CNN and LSTM to extract the temporal stream. A multi-angle filter (MAF) and convolutional neural network (CNN) are used for learning edge features from an image for spatial stream extraction. The best results can then be achieved by using an SVM classifier.

3.3. Temporal domain forgery detection

The temporal domain forgery detection technique helps to find frame-level forgery in terms of frame insertion, deletion, duplication, and shuffling. Sitara and Mehtre [21] designed a generalized extreme studentized deviate (ESD) algorithm to identify the localized forged portions in a video. The velocity field intensity (VFI) and variation of prediction artifact (VPF) techniques help detect and localize forgeries. The limitation of this work is that the VFI and VPF values rise abruptly when the camera lens changes suddenly. In this case, regardless of whether the video is in pristine condition otherwise, it is classified as a forgery. Fadl *et al.* [22] developed a method to detect frame insertion and deletion using the histogram of oriented gradients (HOG). Based on the correlation coefficient values, abnormal points are detected. In a canny edge image, frame duplication and shuffling are computed, based on the motion energy image (MEI) values. But the system fails to detect frame deletions in silent scenes and can only detect one type of forgery at a time, depending on the group of pictures (GOP) size. Parmani *et al.* [23] described a technique based on the normalized multi-scale one-level subtraction (NMOLS) and localized the forgery through the generalized extreme studentized deviate (ESD) test. This method is only applicable when the video is static and the number of frames inserted or deleted exceeds five. Bakas *et al.* [24] extracted features based on the discrete wavelet transform (DWT), prediction footprint variation (PFV), and variation of motion vectors (VMV). This method does not apply to cases where a GOP is to be inserted or deleted in a video sequence. Zhao *et al.* [25] computed the hue-saturation-value (HSV) color histogram for similarity detection, speeded-up robust features (SURF) for feature extraction, and the fast library approximate nearest neighbors (FLANN) to detect similar frames and localize forged portions appropriately. The limitation of the system is the failure to handle scenes with incorrectly obtained shots. Fadl *et al.* [26] calculated the spatio-temporal average (STP) fusion in preprocessing, using the 2D-CNN for feature extraction, and computed the feature vector with the structural similarity index (SSIM). Finally, the Gaussian RBF multi-class support vector machine (RBF-MSVM) is applied to identify the forged video. However, this system cannot detect more than one forgery in a single video. Li *et al.* [27] attempted to extract features using 2D-phase congruency and calculated the correlation between adjacent frames, detecting abnormalities by applying the k-means clustering algorithm. This method, however, cannot be used to determine whether a part of a frame belongs to the same video sequence. According to Aghamaleki and Behrad [28], spatiotemporal information can be determined from the DCT coefficient and quantization residual values. The fused values are used to establish the insertion or deletion of the video frame. This method, however, is not applicable to dynamic environment videos.

Yao *et al.* [29] advanced the frame interpolation technique, in which the adaptive overlapped block motion compensation (AOBMC), as well as global and local residual features, are used to detect deleted frames. However, there is a high degree of time complexity. Wei *et al.* [30] detected frame deletions and duplications using a multiscale standardized mutual information procedure which is not appropriate for a single video that contains more than one forgery. Selvaraj and Karuppiah [31] exploited the earth mover's distance (EMD) metric to detect the type of forgery and abnormality point. However, this method is not applicable when the frames are inserted/deleted at the start/end of the video. Kumar and Gaur [32] use statistical measures to detect multiple forgeries, such as frame insertions and frame deletions. The Haralick features are used to calculate correlation coefficients between adjacent frames. If a minimum correlation value is used, a forgery location can be determined; however, there may be the possibility of false positive values. For this reason, adaptive thresholds such as mean, standard deviation, and sigma coefficient values can be used to detect upper and lower bounds. In the case of removing or inserting frames that are less than five, this method cannot be used. Oraibi and Radhi [33] identified features using spatial and temporal information. A three-dimensional convolutional neural network (3D-CNN) is utilized to compute the difference between each adjacent frame. It is necessary to analyze a temporal feature with LSTM in order to detect forgery, and based on the result, calculate probability. In Shelke and Kasana [34], two-dimensional distributions and multiscale entropy were introduced for detecting multiple video forgeries. Features are analyzed for the purpose of calculating the inter-frame correlation coefficient. As a final step, median absolute deviation (MAD) is used to detect abnormal points. Saikia *et al.* [35] suggest that facial features can be used to detect deepfake faces. Through the use of the optical flow technique, the temporal inconsistencies between adjacent frames can be detected. In the next step, the hybrid CNN-RNN architecture is used to train and classify the fake/real frame.

3.4. Spatio-temporal domain forgery detection

Using spatio-temporal forgery detection techniques, a duplicate frame or region on a video can be detected. Aloraini *et al.* [36] used a Laplacian pyramid method (spatial filtering) in each frame, along with a high-pass filter, to circumvent static scenes in a video. In order to reduce computation complexity, sequential analysis is used to estimate object movements in both the spatial and temporal aspects of different resolution videos. This approach fails with dynamic background videos. Singh and Singh [37] used correlation coefficients and the coefficients of variation to detect duplicate frames and regions. Owing to this limitation, the scheme cannot detect a negligible number of duplicate frames and forgeries in tiny areas. Lin and Tsay [38] analyzed camera motion using frame grouping and alignment techniques. The group coherence abnormality pattern (GCAP) is used to ascertain the spatio-temporal coherence in each frame. Forged slices are discovered, based on the similarities in the coherence pattern. This approach is limited in that its performance is adversely impacted when compressed videos are used. Bestagini *et al.* [39] developed a method to detect frame duplication and copy-move forgeries in a video. The copy-move forgery detection algorithm uses a binary 3D map and a clustering algorithm. Phase correlation is employed to detect duplicate frames in a video. This approach, however, requires extensive processing time. Karthikeyan *et al.* [40] computed a motion vector using an optical flow technique for feature extraction and a block matching algorithm to generate the location of the forged frame. However, block-matching motion estimation methods suffer from a variety of issues, including block artifacts and inadequacies in motion compensation. Table 1 shows the techniques and attack types used in video forgery detection as well as their limitations in the spatial, temporal, and spatio-temporal domains.

Kaur and Jindal [41] applied the deep convolutional neural network (DCNN) model using spatial and temporal correlation values that localize the forged region through semantic segmentation. To make the method specific to unrelated situations, parameters and thresholds are set differently. Zampoglou *et al.* [42] used deep learning to detect frame and region duplication in videos. The technique employs a Q4 filter derived from discrete cosine transform technology and a cobalt filter to extract quantization error values. Finally, the filter output is used to differentiate between the original and forged videos. However, this approach is not suitable for videos of variable lengths. Aparicio-Díaz *et al.* [43] suggested the use of a block correlation matrix to detect and localize a region duplication in a frame. The block correlation matrix combines the spatial and temporal information of all the pixels to detect forgeries. A drawback of this method is that false positives may be created by a failure to set the threshold appropriately. Shelke and Kasana [44] used a technique referred to as polar cosine transform (PCT) and neighborhood binary angular pattern (NBAP) for feature extraction. GoogleNet architecture was utilized to detect inter-frame and intra-frame forgeries. However, this method cannot be used for live video streaming.

Table 1. Spatial, temporal, and spatio-temporal based forgery detection techniques: a survey

Reference	Techniques	Domain	Type of attack	Dataset	Time complexity
Bakas *et al.* [45]	– Haralick correlation distribution	Temporal	– Frame insertion – Frame deletion – Frame duplication	– Surrey library for forensic analysis (SULFA) – Video tampering dataset (VTD)	High
Yang *et al.* [46]	– Adaptive SIFT – Agglomerative hierarchical clustering	Spatial	– Copy move	– Developed own dataset	Low
Fadl *et al.* [47]	– Differential energy of residue	Temporal	– Frame insertion – Frame deletion – Frame duplication	– SULFA	Low
Huang *et al.* [48]	– Fast Fourier transform – Singular value decomposition – Principal component analysis	Spatial	– Copy move – Postprocessing – (Gaussian blur and noise attack)	– Developed own dataset	High
Bagiwa *et al.* [49]	– Statistical correlation of hessian matrix (SCHM)	Spatial	– Video inpainting	– SULFA	High
Aghamaleki and Behrad [50]	– Quantization error based on wavelet	Temporal	– Frame insertion – Frame deletion	– VTD	Low
Su *et al.* [51]	– K-singular value decomposition	Spatial	– Object addition – Object deletion	– SONY DSC-P10 camera videos	High
Zhang *et al.* [52]	– Quotients of consecutive correlation coefficient of local binary pattern (QCCoLBPs)	Temporal	– Frame insertion – Frame deletion	– KTH dataset	Low
Liu and Huang [53]	– Zernike opponent chromaticity moment	Temporal	– Frame insertion – Frame deletion – Frame duplication	– SULFA – Canon IXUS 220HS Camera – SONY DSC P10	High
Pandey *et al.* [54]	– SIFT for spatial extraction – Noise residue and correlation for temporal extraction	Spatio-Temporal	– Region duplication – Frame duplication	– SULFA – CANON camera videos – Nikon camera videos – Fujifilm camera videos	High

4. GENERALIZED VIDEO FORGERY DETECTION FRAMEWORK

Figure 2 provides a visual representation of the core principles that form the foundation of the methodology utilized in video forgery detection. It offers a clear understanding of the fundamental components and processes involved in identifying and detecting instances of video forgery. The process of analyzing a suspected video for forgery involves several steps. First, the video is segmented into frames, and then preprocessing techniques are applied to enhance the quality and prepare the frames for further analysis. Following that, feature extraction is performed to extract relevant information from the frames. After feature extraction, robustness testing is carried out to evaluate the authenticity of the video. This testing involves various techniques to assess the presence of any manipulation in the video. The specific methods employed for robustness testing may vary depending on the available tools and algorithms. Finally, based on the results obtained from the feature extraction and robustness testing, a classification is made to determine whether the video has been forged or not. This classification can be based on predefined criteria or machine learning algorithms trained on a dataset of genuine and manipulated videos.

4.1. Preprocessing

First, the input video must be split into image sequences called frames. The preprocessing methodology includes color conversion and resizing. Red green blue (RGB) images are converted to grayscale or YCbCr because they contain a lot of information, much of which is irrelevant to the forgery detection process. Color conversion is not necessary when detecting a video forgery using the color histogram process. Preprocessing reduces the complexity of transmission and storage.

4.2. Feature extraction

Feature extraction is essential to the forgery detection process. Much of the research has used frame prediction or residual errors, the mean square error (MSE), photo response non-uniformity (PRNU), and frame correlation as features. Feature extraction techniques used to detect forged videos include the SIFT, optical flow, and block division. SIFT is invariant to changes in uniform scaling and illumination, which makes it possible to identify objects with great accuracy [55]. Also, local binary pattern (LBP) is computationally less complex as well as rotation-invariant and scale-invariant, so it can detect manipulation more efficiently. The optical flow, which detects the motion feature in a video, is useful because operations undertaken on a video sequence are likely to disrupt the consistency of the video. Block division detects spatial domain forgeries by dividing the image into overlapping or non-overlapping fixed-size blocks. Further along, sub-blocks help identify defects easily.

Also, feature extraction is critical to reducing dimensionality, computation time, and complexity. Typically, dimensionality reduction techniques decrease the number of features prior to classification. Dimensionality reduction helps to deal with redundant features [56]. In the modified Markov model, the feature vector dimension is reduced by averaging all four Markov features together [57]. As well as down sampling, DWTs, and DCTs have been employed to reduce the computational complexity [58], [59].

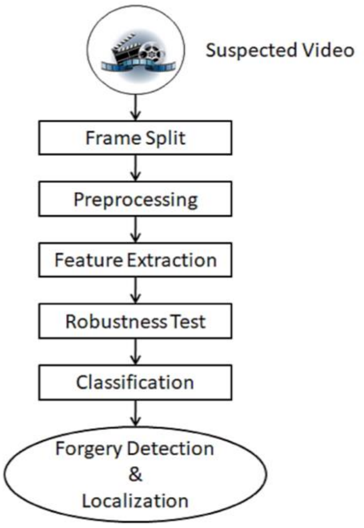

Figure 2. Block diagram of video forgery detection

4.3. Robustness tests

Robustness tests determine the efficiency of an algorithm or model. After the video is edited, post-processing operations may need to be applied to conceal the forged evidence. As a result, the human eye can no longer verify the legitimacy of altered frames. Therefore, robustness tests are essential to ensure that the performance of the system is not compromised. In addition to being an attack that operates on both the spatial and temporal domains, post-processing enhances the forged image. Spatial domain operations include adjusting the gamma factor in every channel, changing frame colors to gray/binary values, increasing and decreasing the contrast, shifting or flipping frames vertically or horizontally, adding a logo or subtitles, scaling the frame size with black pixels, and changing the angle of the frames [60]. Such operations in the temporal domain include reducing or increasing motion speed, modifying the frame rate, adjusting brightness values using gamma correction, adding Gaussian noise, and blurring. This phase reduces the number of false matches and misclassifications in forged videos.

4.4. Classification

Selected features from the feature extraction phase are examined to determine the suitability of each classifier for differentiating between the original and forged videos. The SVM and the RBF-MSVM detect all kinds of forgeries, particularly when it comes to establishing the authenticity or otherwise of an original video [61]. The random sample consensus algorithm (RANSAC), k-nearest neighbor (KNN), and extreme learning machine (ELM) methods are employed to discover suspect frames in a video [62]. The deep neural network with moth search optimization (DNN-MSO) is implemented for classification with optimization.

Abnormal points are usually detected through threshold methods such as correlation, the Tchebyshev inequality threshold technique, peak signal-to-noise ratio (PSNR), Z-score, or Grabb's test, and the mean squared error. Classification using convolutional and recurrent neural networks is also considered efficient [63], [64]. The final phase of the forgery detection and localization process determines whether the video is forged or not, the type of forgery, and the number of forged frames or regions.

4.5. Dataset descriptions

Several state-of-the-art benchmark forgery detection datasets and details of which are publicly available were used to evaluate the efficiency of the algorithm. Though researchers may opt to use the datasets outlined in Table 2 for analysis, there are relatively few datasets used by researchers. While SULFA is a famous dataset used for detecting copy-move forgeries and frame duplication, it has a limited number of test videos. SYSU-OBJFORG, one of the largest object-based forgery datasets is expensive. Datasets are typically available for this purpose and focus primarily on copy-move and frame duplication. Furthermore, very few datasets recorded on dynamic backgrounds work on static backgrounds. Consequently, researchers have resorted to constructing their datasets from YouTube videos or readily available ones.

Table 2. Video datasets related to forgery detection and their descriptions

Dataset	Number of Originals and Forged Videos	Type of Attack	Remarks
VTD [65]	Original-7 Forged-26	Inter and intra-frame forgery	Copy-move, frame shuffling, and splicing videos are shoot at static as well as dynamic positions
REWIND [66]	Original-10 Forgery-10	Inter and intra-frame forgery	Copy-move forgery videos
Tampered video dataset [67]	Original-6 Forged-160	Intra-frame forgery	Forged videos by various transformations like scaling, and shearing
SYSU-OBJFORG [68]	Original-100 Forged-100	Intra-frame forgery	Object-based forged videos
Panchal and Shah [69]	Forged-120 Smart forged-90	Inter-frame forgery	Frame insertion, frame deletion, frame duplication, and multiple forged videos
VIFDD [70]	Training data-272 Testing data-118	Inter-frame forgery	Frame insertion, frame deletion, frame duplication, and frame shuffling

5. DISCUSSION

An in-depth analysis of passive video forgery detection approaches has been presented in this paper. The rapid advancement of technology leads to an increase in video forgeries. The purpose of this paper is to discuss the types and techniques of digital video forgery. In addition, it discusses both the advantages and limitations of the approach. It has been found that passive video forgery detection techniques work best when based on a specific methodology and specific circumstances. To improve the forgery detection accuracy, it is crucial to consider the video quality, GOP structure, noise, video background, and compression rate. Forgery detection is influenced by the manipulated frame length as well. If the manipulated frame count is low for inter-frame forgery detection, the forgery cannot be accurately detected. It is, therefore, necessary to construct the techniques to cooperate with it. Research techniques currently use fixed GOP structures rather than variable GOP structures, which makes it hard to discern whether multiple GOPs or an entire GOP have been deleted. Because of this, these types of methodologies should be the most carefully considered. Since noise significantly affects system performance, a new methodology is required to identify different types of noise, such as salt and pepper, and Gaussian. Due to the widespread use of static video backgrounds in research, dynamic backgrounds should be considered in the future. A majority of researchers working on compression-based techniques use MPEG-4, MPEG-2, and H.264 codecs. In this way, it is impossible to detect forgeries in other codec formats. The quality of compression artifacts, bit rates, and quantization ratios may adversely affect system performance, so these factors need to be addressed as well. In addition, there is a lack of standard video datasets with descriptions of inter-frame forgery. It is therefore important to focus on the generation of such datasets. The majority of existing video forgery methods can only detect single inter-frame and intra-frame forgeries and cannot detect multiple forgeries within a single video. For these issues to be resolved, a more efficient approach is required. Also, deep learning methods such as CNN and RNN enhance the need for the analysis of large datasets. Overall, researchers can use the analysis of this survey to develop new methods of detecting video forgeries, which will benefit them in developing new forgery detection systems.

6. CONCLUSION

This research analysis offers valuable information about passive video forgery detection approaches. It provides researchers with important insights that can help them develop new methods to detect video forgeries. By addressing specific challenges such as variable GOP structures, different types of noise, dynamic background, various coded formats and different compression factors, the accuracy and effectiveness of forgery detection systems can be improved. Additionally, creating standardized video datasets that specifically focus on detecting forgeries between frames will advance research in this field. By applying the findings from this survey, researchers can contribute to the development of robust video forgery detection systems.

REFERENCES

[1] S. Bourouis, R. Alroobaea, A. M. Alharbi, M. Andejany, and S. Rubaiee, "Recent advances in digital multimedia tampering detection for forensics analysis," *Symmetry*, vol. 12, no. 11, Nov. 2020, doi: 10.3390/sym12111811.

[2] V. Kumar, A. Singh, V. Kansal, and M. Gaur, "A comprehensive analysis on video forgery detection techniques," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3563382.

[3] M. Saddique, K. Asghar, U. I. Bajwa, M. Hussain, and Z. Habib, "Spatial video forgery detection and localization using texture analysis of consecutive frames," *Advances in Electrical and Computer Engineering*, vol. 19, no. 3, pp. 97–108, 2019, doi: 10.4316/AECE.2019.03012.

[4] G. Chittapur, S. Murali, and B. S. Anami, "Forensic approach for detecting the region copy-create video forgery by applying frame similarity approach," *Research Journal of Computer and Information Technology Sciences*, vol. 7, no. 2, pp. 12–17, 2019.

[5] J. D. Gavade and S. R. Chougule, "A SIFT with RANSAC based spatial tampering detection in digital video," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 3, pp. 1156–1163, Mar. 2019, doi: 10.26438/ijcse/v7i3.11561163.

[6] L. Su, H. Luo, and S. Wang, "A novel forgery detection algorithm for video foreground removal," *IEEE Access*, vol. 7, pp. 109719–109728, 2019, doi: 10.1109/ACCESS.2019.2933871.

[7] M. A. Fayyaz, A. Anjum, S. Ziauddin, A. Khan, and A. Sarfaraz, "An improved surveillance video forgery detection technique using sensor pattern noise and correlation of noise residues," *Multimedia Tools and Applications*, vol. 79, no. 9–10, pp. 5767–5788, Mar. 2020, doi: 10.1007/s11042-019-08236-2.

[8] O. I. Al-Sanjary *et al.*, "Deleting object in video copy-move forgery detection based on optical flow concept," in *2018 IEEE Conference on Systems, Process and Control (ICSPC)*, Dec. 2018, pp. 33–38, doi: 10.1109/SPC.2018.8704160.

[9] P. S. Raskar and S. K. Shah, "VFDHSOG: Copy-move video forgery detection using histogram of second order gradients," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1617–1654, Jan. 2022, doi: 10.1007/s11277-021-08964-5.

[10] H. Ren, W. Atwa, H. Zhang, S. Muhammad, and M. Emam, "Frame duplication forgery detection and localization algorithm based on the improved levenshtein distance," *Scientific Programming*, pp. 1–10, Mar. 2021, doi: 10.1155/2021/5595850.

[11] M. Sadddique, K. Asghar, T. Mehmood, M. Hussain, and Z. Habib, "Robust video content authentication using video binary pattern and extreme learning machine," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 8, 2019, doi: 10.14569/IJACSA.2019.0100833.

[12] Y. Rodriguez-Ortega, D. M. Ballesteros, and D. Renza, "Copy-move forgery detection (CMFD) using deep learning for image and video forensics," *Journal of Imaging*, vol. 7, no. 3, Mar. 2021, doi: 10.3390/jimaging7030059.

[13] Y. Hu and X. Lu, "Learning spatial-temporal features for video copy detection by the combination of CNN and RNN," *Journal of Visual Communication and Image Representation*, vol. 55, pp. 21–29, Aug. 2018, doi: 10.1016/j.jvcir.2018.05.013.

[14] M. H. Khudhur, J. Waleed, H. Hatem, A. M. Abduldaim, and D. A. Abdullah, "An efficient and fast digital image copy-move forensic technique," in *2018 2nd International Conference for Engineering, Technology and Sciences of Al-Kitab (ICETS)*, Dec. 2018, pp. 78–82, doi: 10.1109/ICETS.2018.8724611.

[15] X. Yang, Y. Li, and S. Lyu, "Exposing deep fakes using inconsistent head poses," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 8261–8265, doi: 10.1109/ICASSP.2019.8683164.

[16] M. Koopman, A. M. Rodriguez, and Z. Geradts, "Detection of deepfake video manipulation," in *The 20th Irish machine vision and image processing conference (IMVIP)*, 2018, pp. 133–136.

[17] Y. Li, M.-C. Chang, and S. Lyu, "In ictu oculi: exposing AI created fake videos by detecting eye blinking," in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, Dec. 2018, pp. 1–7, doi: 10.1109/WIFS.2018.8630787.

[18] 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)*, Nov. 2018, pp. 1–6, doi: 10.1109/AVSS.2018.8639163.

[19] S. Ganguly, S. Mohiuddin, S. Malakar, E. Cuevas, and R. Sarkar, "Visual attention-based deepfake video forgery detection," *Pattern Analysis and Applications*, vol. 25, no. 4, pp. 981–992, Nov. 2022, doi: 10.1007/s10044-022-01083-2.

[20] J. Wang, X. Li, and Y. Zhao, "D3: A novel face forgery detector based on dual-stream and dual-utilization methods," in *International Conference on Artificial Intelligence and Security*, 2022, pp. 413–425.

[21] K. Sitara and B. M. Mehtre, "A comprehensive approach for exposing inter-frame video forgeries," in *2017 IEEE 13th International Colloquium on Signal Processing and its Applications (CSPA)*, 2017, pp. 73–78, doi: 10.1109/CSPA.2017.8064927.

[22] S. Fadl, Q. Han, and L. Qiong, "Exposing video inter-frame forgery via histogram of oriented gradients and motion energy image," *Multidimensional Systems and Signal Processing*, vol. 31, no. 4, pp. 1365–1384, Oct. 2020, doi: 10.1007/s11045-020-00711-6.

[23] R. Parmani, S. Butala, A. Khanvilkar, S. Pawar, and N. Pulgam, "Inter frame video forgery detection using normalized multi scale one level subtraction," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3424489.

[24] J. Bakas, R. Naskar, and S. Bakshi, "Detection and localization of inter-frame forgeries in videos based on macroblock variation and motion vector analysis," *Computers and Electrical Engineering*, vol. 89, Jan. 2021, doi: 10.1016/j.compeleceng.2020.106929.

[25] 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.

[26] S. Fadl, Q. Han, and Q. Li, "CNN spatiotemporal features and fusion for surveillance video forgery detection," *Signal Processing: Image Communication*, vol. 90, Jan. 2021, doi: 10.1016/j.image.2020.116066.

[27] Q. Li, R. Wang, and D. Xu, "An inter-frame forgery detection algorithm for surveillance video," *Information*, vol. 9, no. 12, Nov. 2018, doi: 10.3390/info9120301.

[28] J. A. Aghamaleki and A. Behrad, "Malicious inter-frame video tampering detection in MPEG videos using time and spatial domain analysis of quantization effects," *Multimedia Tools and Applications*, vol. 76, no. 20, pp. 20691–20717, Oct. 2017, doi: 10.1007/s11042-016-4004-z.

[29] H. Yao, R. Ni, and Y. Zhao, "An approach to detect video frame deletion under anti-forensics," *Journal of Real-Time Image Processing*, vol. 16, no. 3, pp. 751–764, Jun. 2019, doi: 10.1007/s11554-019-00865-y.
[30] W. Wei, X. Fan, H. Song, and H. Wang, "Video tamper detection based on multi-scale mutual information," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27109–27126, Oct. 2019, doi: 10.1007/s11042-017-5083-1.
[31] P. Selvaraj and M. Karuppiah, "Inter-frame forgery detection and localization in videos using earth mover's distance metric," *IET Image Processing*, vol. 14, no. 16, pp. 4168–4177, Dec. 2020, doi: 10.1049/iet-ipr.2020.0287.
[32] V. Kumar and M. Gaur, "Multiple forgery detection in video using inter-frame correlation distance with dual-threshold," *Multimedia Tools and Applications*, vol. 81, no. 30, pp. 43979–43998, Dec. 2022, doi: 10.1007/s11042-022-13284-2.
[33] M. R. Oraibi and A. M. Radhi, "Enhancement digital forensic approach for inter-frame video forgery detection using a deep learning technique," *Iraqi Journal of Science*, pp. 2686–2701, Jun. 2022, doi: 10.24996/ijs.2022.63.6.34.
[34] N. A. Shelke and S. S. Kasana, "Multiple forgeries identification in digital video based on correlation consistency between entropy coded frames," *Multimedia Systems*, vol. 28, no. 1, pp. 267–280, Feb. 2022, doi: 10.1007/s00530-021-00837-y.
[35] P. Saikia, D. Dholaria, P. Yadav, V. Patel, and M. Roy, "A hybrid CNN-LSTM model for video deepfake detection by leveraging optical flow features," in *2022 International Joint Conference on Neural Networks (IJCNN)*, Jul. 2022, pp. 1–7, doi: 10.1109/IJCNN55064.2022.9892905.
[36] M. Aloraini, M. Sharifzadeh, C. Agarwal, and D. Schonfeld, "Statistical sequential analysis for object-based video forgery detection," *Electronic Imaging*, vol. 31, no. 5, pp. 543-1-543–7, Jan. 2019, doi: 10.2352/ISSN.2470-1173.2019.5.MWSF-543.
[37] G. Singh and K. Singh, "Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11527–11562, May 2019, doi: 10.1007/s11042-018-6585-1.
[38] C.-S. Lin and J.-J. Tsay, "A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis," *Digital Investigation*, vol. 11, no. 2, pp. 120–140, Jun. 2014, doi: 10.1016/j.diin.2014.03.016.
[39] P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Local tampering detection in video sequences," in *2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP)*, Sep. 2013, pp. 488–493, doi: 10.1109/MMSP.2013.6659337.
[40] P. Karthikeyan, R. Bhavani, D. Rajinigirinath, and R. Priya, "Automatic forged scene detection in advanced video using combined Mpeg-2 and optical flow features," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 11, no. 2, pp. 246–258, 2020.
[41] H. Kaur and N. Jindal, "Deep convolutional neural network for graphics forgery detection in video," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1763–1781, Jun. 2020, doi: 10.1007/s11277-020-07126-3.
[42] M. Zampoglou *et al.*, "Detecting tampered videos with multimedia forensics and deep learning," in *MultiMedia Modeling*, Springer International Publishing, 2019, pp. 374–386.
[43] E. Aparicio-Díaz, R. Cumplido, M. L. Pérez Gort, and C. Feregrino-Uribe, "Temporal copy-move forgery detection and localization using block correlation matrix," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 5, pp. 5023–5035, May 2019, doi: 10.3233/JIFS-179048.
[44] N. A. Shelke and S. S. Kasana, "Multiple forgery detection and localization technique for digital video using PCT and NBAP," *Multimedia Tools and Applications*, vol. 81, no. 16, pp. 22731–22759, Jul. 2022, doi: 10.1007/s11042-021-10989-8.
[45] J. Bakas, R. Naskar, and R. Dixit, "Detection and localization of inter-frame video forgeries based on inconsistency in correlation distribution between Haralick coded frames," *Multimedia Tools and Applications*, vol. 78, no. 4, pp. 4905–4935, Feb. 2019, doi: 10.1007/s11042-018-6570-8.
[46] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, "A copy-move forgery detection method based on CMFD-SIFT," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 837–855, Jan. 2018, doi: 10.1007/s11042-016-4289-y.
[47] S. M. Fadl, Q. Han, and Q. Li, "Inter-frame forgery detection based on differential energy of residue," *IET Image Processing*, vol. 13, no. 3, pp. 522–528, Feb. 2019, doi: 10.1049/iet-ipr.2018.5068.
[48] D.-Y. Huang, C.-N. Huang, W.-C. Hu, and C.-H. Chou, "Robustness of copy-move forgery detection under high JPEG compression artifacts," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 1509–1530, 2017, doi: 10.1007/s11042-015-3152-x.
[49] M. A. Bagiwa, A. W. A. Wahab, M. Y. I. Idris, and S. Khan, "Digital video inpainting detection using correlation of hessian matrix," *Malaysian Journal of Computer Science*, vol. 29, no. 3, pp. 179–195, Sep. 2016, doi: 10.22452/mjcs.vol29no3.2.
[50] J. Abbasi 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.
[51] L. Su, T. Huang, and J. Yang, "A video forgery detection algorithm based on compressive sensing," *Multimedia Tools and Applications*, vol. 74, no. 17, pp. 6641–6656, Sep. 2015, doi: 10.1007/s11042-014-1915-4.
[52] Z. Zhang, J. Hou, Q. Ma, and Z. Li, "Efficient video frame insertion and deletion detection based on inconsistency of correlations between local binary pattern coded frames," *Security and Communication Networks*, vol. 8, no. 2, pp. 311–320, Jan. 2015, doi: 10.1002/sec.981.
[53] Y. Liu and T. Huang, "Exposing video inter-frame forgery by Zernike opponent chromaticity moments and coarseness analysis," *Multimedia Systems*, vol. 23, no. 2, pp. 223–238, Mar. 2017, doi: 10.1007/s00530-015-0478-1.
[54] R. C. Pandey, S. K. Singh, and K. K. Shukla, "Passive copy-move forgery detection in videos," in *2014 International Conference on Computer and Communication Technology (ICCCT)*, Sep. 2014, pp. 301–306, doi: 10.1109/ICCCT.2014.7001509.
[55] J. Waleed, D. A. Abdullah, and M. H. Khudhur, "Comprehensive display of digital image copy-move forensics techniques," in *2018 International Conference on Engineering Technology and their Applications (IICETA)*, May 2018, pp. 155–160, doi: 10.1109/IICETA.2018.8458084.
[56] M. Raveendra and D. K. Nagireddy, "DNN based moth search optimization for video forgery detection," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1, pp. 1190–1199, Oct. 2019, doi: 10.35940/ijeat.A9517.109119.
[57] G. Chittapur, S. Murali, and B. Anami, "Video forgery detection using motion extractor by referring block matching algorithm," *International Journal of Scientific and Technology*, vol. 8, no. 10, pp. 3240–3243, 2019.
[58] S. M. Fadl, Q. Han, and Q. Li, "Authentication of surveillance videos: detecting frame duplication based on residual frame," *Journal of Forensic Sciences*, vol. 63, no. 4, pp. 1099–1109, Jul. 2018, doi: 10.1111/1556-4029.13658.
[59] R. Kaur and E. J. Kaur, "Video forgery detection using hybrid techniques," *IJARCCE*, vol. 5, no. 12, pp. 112–117, Dec. 2016, doi: 10.17148/ijarcce.2016.51221.
[60] O. I. Al-Sanjary and G. Sulong, "Detection of video forgery: A review of literature," *Journal of Theoretical and Applied Information Technology*, vol. 74, no. 2, 2015.
[61] S. Agarwal, H. Farid, Y. Gu, M. He, K. Nagano, and H. Li, "Protecting world leaders against deep fakes," *CVPR Workshop*, 2019.
[62] J. Kharat and S. Chougule, "A passive blind forgery detection technique to identify frame duplication attack," *Multimedia Tools and Applications*, vol. 79, no. 11–12, pp. 8107–8123, Mar. 2020, doi: 10.1007/s11042-019-08272-y.
[63] K. G. R. Pillai *et al.*, "Compression based clustering technique for enhancing accuracy in web scale videos," *Multimedia Tools*

and Applications, vol. 80, no. 5, pp. 7077–7101, Feb. 2021, doi: 10.1007/s11042-020-10062-w.

[64] M. A. Younus and T. M. Hasan, "Abbreviated view of deepfake videos detection techniques," in *2020 6th International Engineering Conference "Sustainable Technology and Development" (IEC)*, Feb. 2020, pp. 115–120, doi: 10.1109/IEC49899.2020.9122916.

[65] O. I. Al-Sanjary, A. A. Ahmed, and G. Sulong, "Development of a video tampering dataset for forensic investigation," *Forensic Science International*, vol. 266, pp. 565–572, Sep. 2016, doi: 10.1016/j.forsciint.2016.07.013.

[66] Y. Wu, X. Jiang, T. Sun, and W. Wang, "Exposing video inter-frame forgery based on velocity field consistency," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2014, pp. 2674–2678, doi: 10.1109/ICASSP.2014.6854085.

[67] E. Ardizzone and G. Mazzola, "A tool to support the creation of datasets of tampered videos," in *Image Analysis and Processing ICIAP 2015*, Springer International Publishing, 2015, pp. 665–675.

[68] S. Chen, S. Tan, B. Li, and J. Huang, "Automatic detection of object-based forgery in advanced video," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 11, pp. 2138–2151, Nov. 2016, doi: 10.1109/TCSVT.2015.2473436.

[69] H. D. Panchal and H. B. Shah, "Video tampering dataset development in temporal domain for video forgery authentication," *Multimedia Tools and Applications*, vol. 79, no. 33–34, pp. 24553–24577, Sep. 2020, doi: 10.1007/s11042-020-09205-w.

[70] X. Nguyen and Y. Hu, "VIFFD-A dataset for detecting video inter-frame forgeries," *Mendeley Data*, vol. 6, 2020.

BIOGRAPHIES OF AUTHORS

Liba Manopriya Jegaveerapandian received the B.C.A. degree from Govindammal Aditanar College for Women, Thiruchendur, Tamilnadu, India, and obtained an M.C.A. degree from Amrita Viswa Vidyapeetham, Coimbatore, India. She has completed her M.Phil. degree at Manonmaniam Sundaranar University, Tirunelveli, India. She is pursuing a Ph.D. degree in the Department of Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli, India. Her areas of interest are digital image processing and computer network. She can be contacted at email: libamanopriya06@gmail.com.

Arockia Jansi Rani graduated B.E. in Electronics and Communication Engineering from Government College of Engineering, Tirunelveli, Tamil Nadu, India, in 1996 and M.E. in Computer Science and Engineering from National Engineering College, Kovilpatti, Tamil Nadu, India in 2002. She has more than 10 years of teaching and research experience. She completed her Ph.D in Computer Science and Engineering from Manonmaniam Sundaranar University, Tamil Nadu, India, in 2012. She currently serves as Associate Professor at the Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli. Her research interests include digital image processing, neural networks, and data mining. She can be contacted at email: jansi_cse@msuniv.ac.in.

Prakash Periyaswamy received a Ph.D. in Information and Communication Engineering from Anna University in 2016. He currently serves as Associate Professor at the Department of Computer Science Engineering, Vellore Institute of Technology, Chennai. His research interests include cloud computing and artificial intelligence. He can be contacted at email: npprakash@gmail.com.

Sakthivel Velusamy currently serves as an assistant professor in Senior Grade, School of Computer Science Engineering, Vellore Institute of Technology, Chennai. His research interests include cloud computing, IoT, and machine learning. He can be contacted at email: sakthivel.v@vit.ac.in.