A COMPREHENSIVE REVIEW OF VIDEO FORGERY DETECTION TECHNIQUES

Abstract

In this digital era, the rapid increase in the number of video content caused a rise in video forgeries, raising significant concerns regarding their potential impact on society, politics, and justice. This comprehensive review paper delves into the multifaceted landscape of video forgery detection, addressing its critical importance in contemporary media forensics. We categorize video forgeries into various types, including inter-frame and intra-frame, object removal forgery etc, and illustrate their prevalence and motivations. An extensive analysis of detection methods is presented, encompassing traditional techniques, as well as cutting-edge approaches involving machine learning and deep learning. We assess the strengths and limitations of these methods, discussing recent advancements and their implications. Anticipating future developments, we outline emerging trends and the need for more comprehensive datasets. As video forgery detection continues to evolve, its implications for society and the legal landscape underscore the necessity of continued research and development in this crucial field.

Keywords: Video forgery detection, splicing, multimedia forensics

Authors

Wincy Abraham
Department of Computer Science
Assumption College Autonomous
Changanacherry, Kerala, India
wincya@gmail.com

Sunil Kumar D S
Department of Computer Applications
Administrative Management College
Bangalore, Karnataka, India
dssunil6@gmail.com

I. INTRODUCTION

With the availability of large number of multimedia capturing and manipulation tools available today, there is a huge number of such multimedia files existing. But the authenticity of such contents must be examined before it can be used for various purposes like as evidence in digital forensics, or before publishing it through the various media. Video forgery detection methods proposed by researchers in this field try to address this issue. Some of the key terms related to this field are detailed below.

1. **Digital Forensics:** Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.[17] Depending on various aspects of investigation, like the type of devices, media or material, digital forensics investigation is categorized into computer forensics, mobile device forensics, network forensics, database forensics, forensic data analysis etc.

   Computer forensics tries to analyse, recover and present facts and ideas concerning the digital content. With the proliferation of multimedia manipulation tools today, the multimedia forensic data retrieved is not trustworthy. So, the evidences collected for computer forensics must be examined for genuineness. There comes the importance of digital media forgery detection tools. Once computer forensics collects evidence of this type it must be examined to check its genuineness. So, audio and video forgery detection tools play their roles in digital forensics.

2. **Video Forensics:** Scientific examination, comparison and evaluation of video in legal matters is referred to as Forensic video analysis. It is usually carried out in a forensic lab equipped with tools in the most secure and flawless manner. Surveillance video cameras provide the much-needed evidences as they are easily available. These video recordings are used by Police and judiciary to make judgements. Interpreting the images and video recordings for extracting the sequence of events which occurred is a crucial task which is done by a forensic expert. A video forensic expert usually compares and analyses the results. This becomes difficult in some situations due to the manipulations done on the video knowingly or unknowingly.

3. **Video Forgery:** The technique of creating altered or fake videos by altering or combining existing videos is called Video Forgery. Due to the presence of such manipulations the authenticity of digital videos is questionable and needs to be verified [18]. Based on the approaches taken for manipulation , video forgery can be categorized as

   - **Spatial Forgery:** In spatial forgery, modifications are done on the frame of the video. It may be done by changing the position of objects within the same frame, copying objects from the frame and placing them in other regions in the same frame (copy-move) or by placing objects in a frame by copying them from other frames. (Splicing).

   - **Temporal Forgery:** Alterations are done within the frames of the video. It includes copy-move, frame insertion/deletion, frame duplication etc.

- **Frame insertion/deletion:** Frames from other video are inserted in the video, or frames from the same video may be duplicated. Also, some frames in the video can be deleted.

- **Spatial temporal forgery** Alterations within the frame (intra frame) and in between the frames (inter frames) take place. So, it is called as spatial temporal forgery.

This paper tries to provide comprehensive overview of the field of video forgery detection. It aims to analyse and evaluate the various methods and techniques used for video forgery detection and summarize the key research findings and developments in the area.

II. REVIEW OF THE RELATED LITERATURE

Several approaches have been taken by researchers to detect forgery in video. And still better methods are being discovered.

"An approach to detect video frame deletion under anti-forensics"[1] addresses the challenging issue of detecting video frame deletion in the context of anti-forensics. It states that the approaches to frame deletion detection can be categorized in to those based on the traces left after recompression after frame deletion and those based on the inter frame continuity.

But some anti-forensic methods invalidate several detection methods by making several modifications in the tampered video. So the methods developed must also consider the effects of anti-forensics in the tampered video. But according to the authors, there is no anti-forensic method which conceals the inter frame continuity traces. The paper proposes an easy anti-forensic strategy to attack inter-frame continuity based forensic methods. Two frames on both sides of the FDP (frame deletion point) are taken as templates and uses interpolation to smooth the spike caused by frame deletion. And the paper also proposes a frame deletion detection method which overcomes the above proposed anti -forensic strategy. The frame residual in the actual frames and the interpolated frames are found to be near to zero in H.265/HEVC videos unlike in H.264/AVC videos where it is distinguishable. So the method makes use of the local and global, spatial and frequency domain features to detect frame deletion under anti-forensics.

In "Detecting tampered videos with multimedia forensics and deep learning"[2] two forensic filters used for manual verification like those based on DCT coefficients and video re-quantisation errors, are combined with deep convolutional networks designed for image classification. The forgery detection methods are categorized in to double/multiple quantisation detection, inter-frame forgery detection, and region tampering detection. This paper deals with the third category, the region tampering detection. Parts of a video sequence are inserted in the frames of another video sequence. Here the assumption is that some invisible pattern originated from the capturing or compression process which is detectable is altered by the insertion of the foreign content. The filters used produce visible output maps that can be analysed by humans viz. Q4 and Cobalt filter. Q4 filter is obtained using an NXN block in the video frame. Each such block is transformed using DCT and the NXN coefficient arrays are created from blocks in the video frame, corresponding to each coefficient in the DCT of various blocks. Each array will be of size 1/N of the original image in each

dimension. For getting arrays which are large enough the DCT of 2X2 blocks are taken and 3 of the arrays for coefficients (0, 1),(1,0) and (1,1) are displayed using RGB colour channels. Cobalt filter makes use of the MPEG-4 re-quantization error to detect forgery. The video is re-quantized with a different constant quality level and calculate the per pixel value and an error video is created which depicts the differences with the original video. If the difference is high the intensity of the error video is high and the non-homogeneity in intensity of the error video shows difference in quantization parameters in the original frame itself which indicates frame manipulation. Both the outputs which are RGB images are fed to Convolutional neural networks are trained for classification.

"Tampering detection and localization in digital video using temporal difference between adjacent frames of actual and reconstructed video clip" [3] proposes an algorithm which is based on the temporal difference between adjacent frames in the actual video and its reconstructed form. Video is reconstructed using the frame prediction error. The recompression of a MPEG video results in two distinct fingerprints-spatial and temporal. Spatial fingerprint occurs in a single I frame, when zero, or integer multiple of fixed GOP length frames are added or deleted. Temporal fingerprint occurs in the sequence of B frame or P frame prediction errors only if frames are added or deleted. When a frame is added or deleted from a fixed GOP, its structure gets altered and the prediction error will increase. Frame prediction error is used as a strong feature to detect forgery because no forger is able to delete these fingerprints from the video sequence. Its framework is as follows.

1. A video clip in MP4 or AVI format is taken as input and passed to proposed system for computation of prediction error vector and optical flow.

2. The full-length video sequence given as input is divided into frames and saved in a folder in the form of JPEG images.

3. The structural similarity is extended to measure similarity between two frames of video clip. Then the similarities between frames in the temporal domain are measured and used to calculate prediction error between two frames.

4. Frame prediction error for each frame is calculated and frames are reconstructed based on this error. The calculated errors are stored in Excel sheets for further use.

5. Frame prediction errors of these reconstructed frames are also calculated. And again, stored in excel sheets.

6. Plots of actual video and its reconstructed form are drawn based on these frame prediction errors.

7. These plots easily show the variation between frame prediction errors of forged video and genuine video. So, by comparing these plots one can easily classify between forged and genuine video.

8. Finally, optical motion is calculated using method proposed by Lucas-Kanade for input video clip as well as predicted video clip. A plot is drawn to show optical flow of each video clip. With the help of plot, tampering can be accurately detected and localized. Already proven feature of optical flow is used to verify correct classification of video.

"Spatial video forgery detection and localization using texture analysis of consecutive frames" [5] states that spatial forgery results in inconsistency in the texture and micro patterns in the frames which can be found out from the difference in consecutive frames. For that purpose, two features viz. Chrominance value of consecutive frame difference (CCD) and Discriminative Local Robust Binary Pattern (DRLBP) are made use of. Support Vector Machine (SVM) is used to find out forgery based on the feature vector which combines CCD and DRLBP. These descriptors incorporates both texture and shape information which makes it robust to noise, shape and side variations. The paper focuses on spatial tampering. When the difference of consecutive frames (DOCFs) is found out it clearly shows the traces of forgery in forged frames but not in authentic ones.

First the video is divided in to segments (VSs) of 30 frames each and the frames are extracted. The DOCFs are found out and the features are extracted which are then passed to the SVM model. The model returns a decision as whether the video is authentic or forged. A new descriptor called CCD-DRLBP is proposed to extract features which are efficient for forgery detection.

"Toward video tampering exposure: inferring compression parameters from pixels" [8] proposes a method to detect QP of a H.264/AVC compressed video. Although other methods like the one by Boss et.al exists, it can only detect the QP of key frames only and the estimation of QP of individual patches in the frame shows much deviation although the averaged QP of a frame is somewhat accurate. This paper tries to resolve these issues and it finds QP for predicted frames as well. The model makes use of video and image datasets with labelled patches to find the QP. Three CNNs are pre-trained with different but not adjacent QP values. It is found that estimation becomes more accurate with large patch size and larger stride to minimize the correlation between patches. The performance is evaluated and improvements suggested. Paper concludes saying that the QP estimation of predicted frames are not as accurate as of key frames. Further improvements are recommended.

In "Video tampering localisation using features learned from authentic content" [9] it is found that vast majority of video compression is in H.264/AVI or MPEG2 format. The paper uses the similar methods as in [8] to estimate quantisation parameter, inter-intra frame type and frame delta directly from pixels. CNN is trained to identify these values. Frame delta is used to identify key frames. It locates tampering in some manipulated video by identifying distinct compression profiles in the same video.

In "Coarse-to-fine Copy-move Forgery Detection for Video Forensics" [10], the approaches to detect frame copy-move forgeries are categorized in to image feature based and video feature based. This paper proposes a video feature based approach to detect frame copy-move forgery. The methods already which exist already, demand high computational cost, have unstable detection performance and limited applicability. The authors try to overcome these limitations by the proposed method. The method depends on the Lucas-

Kanade Optical Flow, proposed by B.D. Lucas and T. Kanade [15], to compute the OF for each frame. Merits of this method are rapid computation, simple application, and robustness under noise. OF between adjacent frames i and i+1 are found out and stored as OFi. Then the correlation between the OF of adjacent frames are calculated which ranges from -1 to +1. High correlation indicates higher similarity between frame pairs and hence genuineness.

To reduce the computational demand in finding the correlation to detect forgery, another feature OF sum is found out for each frame by adding the OXi and OYi of each frame for all pixel positions. Then in order to detect forgery OF sum consistency is made use of which either shows sudden spikes when frames are inserted in between or local symmetries when alterations in the video sequence are done carefully. The tampering location can be easily identified and further correlation calculations can be done once the location is identified greatly alleviating the computational burden.

"Detection Of Video Forgery: A Review Of Literature "[11] states that video forgery primarily falls into two methods based on their approaches; active approaches and passive-blind approaches. In this paper, some typical video forgery algorithms are compared for performance and also a demonstration of passive digital video authentication method is performed. According to the authors, some statistical image model for splicing detection was proposed by Farid, and the same with some modifications are the blind image forgery detection method that performs feature extraction for classification via the Hilbert-Huang transform (HHT) and the statistical model that uses the moments of characteristic functions. Splicing forgery is detected using wavelets transform. Passive splicing forgery detection and localization are performed at high accuracy. Other authors [20] developed a method to detect suspicious regions in video recorded from a static scene with the help of noise characteristics of the acquisition device described in frame sequence through a noise level function (NLF).

In "Video Forgery Detection Using HOG Features and Compression Properties" [12] the intrinsic properties of the video are used to detect copy-move tampering. The copy-move video forgery is classified in to spatial tampering and temporal tampering. There are methods proposed which are based on SIFT features matching, Fourier-Mellin Transform etc. which can be used for spatial copy-move forgery detection, but not for temporal forgery detection. Video forgery detection based on noise characteristics may not work if the duplicated region belongs to the same video. SIFT features may not detect forgery for small patch size if a forged patch has undergone scaling transformation even if the feature is robust. Therefore, features such as HoG which are dense image or block wise descriptors are useful in detecting such form of tampering.

"A Frame Tampering Detection Algorithm for MPEG videos" [13] states that in MPEG-2 standard, the structure of group of pictures (GOP) defines the orientation of inter and intra frames in the temporal sequence. During tampering when some frames are inserted or removed the structure gets changed in the subsequent compression. The coding type change helps to detect tampering in MPEG videos.

In "Photo Forensics from JPEG Dimples" [14]it is said that the artefact is introduced in JPEG compression when the DCT coefficients after quantization are converted from floating point type to integer using ceiling, or floor mathematical operators rather than rounding operator. The artefact introduced by various camera models differs and this

becomes helpful in forgery detection by analysing the associated correlation energy of different blocks.

"Fighting Fake News: Image Splice Detection via Learned Self-Consistency" [16] proposes a learning algorithm to detect visual image manipulations which trains the model using large dataset of real photographs. It is trained to check the self-consistency whether the image is created using the same image pipeline using the EXIF metadata of the image. It achieves acceptable performance even without seeing any manipulated image during training. A consistency classifier is learned for each EXIF tag using pairs of photographs and the learned model is used to estimate self-consistency given two input image patches. The method uses a Siamese network to check whether different pairs of patches in an image have the same value for all of the EXIF attributes. Then calculates the overall consistency by combining all the metadata attribute consistency values. A low consistency shows that the patches originated from two different sources.

"A critical literature survey and prospects on tampering and anomaly detection in image data" [21]discusses forgery detection using illumination-based texture descriptor and the FOA-SVNN based classifier for the datasets DSO-1,DSI-1 [33] and gets an accuracy of 95.23% and 94.59% respectively.

In "Recent advances in digital image manipulation detection techniques: A brief review" [22] the authors make it known that although many datasets have been released in the field of image manipulation detection the number of tampered images is very less. The generation of synthesized images will help to overcome the problem and enough data becomes available for training in neural network-based methods. By combining many machine learning models for manipulation detection at multiple scales and by transfer learning a general-purpose image manipulation detection system can be generated. The paper gives the details of the various publicly available datasets.

"An efficient approach for forgery detection in digital images using Hilbert–Huang transform" [23] deals with image forgery detection with post-processing attacks such as image compression, adding Gaussian noises or adjusting the contrast of the image and produce very high accuracies for the datasets CASIA –V1 ,CASIA-V2 , MICC-F2000 , MICC-F600 , MICC-F220 , CoMoFoD ,Internet websites and social media.

III. DATASET

The already existing datasets support any one type of forgery which can be used for evaluating such forgeries. But to evaluate and train for combination of spatial and temporal forgeries, new dataset may need to be created. The existing ones which seem useful are listed below.

SULFA forged [24] -contains 150 original videos of about 10 seconds duration and some spatio-temporal copy-move forgery videos for camera identification.

TDTVD [27]- dataset is created by removing events, objects, or persons at single or multiple locations in a video.

VTD [26]-33 tampered videos of 16 seconds duration. Contains three types of tampering- copy-move, splicing and swapping. Contains complete information about the tampering in the doctored videos.

InVID Fake Video Corpus [28] contains 117 fake videos and 110 real videos with the annotations and descriptions.

GRIP Dataset[25]- contains ten videos with splicing forgeries using Adobe After Effects.

The dataset for analyzing the image forgeries include CASIA –V1[29], CASIA-V2[29], MICC-F2000[30], MICC-F600[30], MICC-F220[30], COVERAGE [32], Columbia Image Splicing dataset t[31], Columbia Uncompressed[31] etc.

IV. STEPS IN METHODOLOGY

Whichever be the methodology adopted, the video forgery detection consists of the following steps.

Step I: Feature extraction

Features provide clues regarding the authenticity of frames. It may measure the discontinuity in spatial, temporal and frequency domain. It may also include both inter-frame and intra-frame forgery details, such that a single feature vector can handle both types of forgeries. Several techniques like Principal Component analysis(PCA), Discrete Cosine Transform(DCT), Scale Invariant Feature Transform(SIFT), Hilbert-Huang transform (HHT), Histogram of Oriented Gradients(HoG) and Difference of Consecutive Frames are used for feature extraction. Based on how much and what information is needed for the detection of video forgery, the required features are extracted from the video after the application of the necessary transformations like those mentioned above. Once the feature extraction process is completed the extracted features are used the next step.

Step II: Classification

For classification of the video as genuine or forged, there are many techniques available. The classification techniques can be categorized as

- Rule based
- Machine Learning based
- Deep Learning based

In rule based classification simple if then rules using some threshold may be used for classification. In Machine Learning (ML) based classifier machine learning models like SVM (Support Vector Machine), Decision Tree Classifier, Linear Regression or ANN (Artificial Neural Network) are used and in Deep Learning (DL) based classification, Deep Learning model like CNN, RNN etc are used for classification. Whether it is ML based or DL based, the model has to be trained well first using available

information and only after that it can be used for the classification. Compared to ML based models, DL models require large volume of data for training the model. So, the choice of classifier very much depends on the dataset size. The type of available data and the type of the required result also affect the choice of the classifier. If all the fields in the data are not numeric, it must be converted to numeric format before supplying it for training and classification.

There are tools and libraries available in all popular programming languages which can be used easily to accomplish the task in both the above steps.

V. CHALLENGES

Detecting video forgeries is a complex and challenging task due to the ever-evolving sophistication of forgery techniques and the sheer volume of digital video content available. Some of the key challenges in video forgery detection include:

1. **Advancements in Forgery Techniques:** Malicious actors continuously develop new and more sophisticated forgery methods, including deepfake technology, which makes it challenging to keep up with the latest trends in video manipulation.

2. **Realism and Quality:** Many forgeries are created with high-quality content that is challenging to distinguish from genuine videos, making it difficult for detection algorithms to identify alterations.

3. **High Volume of Video Data:** The sheer volume of digital video content available on the internet and social media platforms makes it a challenge to monitor and analyse all potential instances of forgery effectively.

4. **Computation and Resource Intensity:** Many forgery detection techniques, especially those based on machine learning and deep learning, require substantial computational resources, which can be a barrier for real-time or large-scale analysis.

5. **Diverse Types of Forgeries:** Video forgeries can take various forms, such as splicing, deepfakes, object removal, and frame manipulation, each requiring specific detection approaches. Developing methods that can address all types of forgeries is complex.

6. **Data Availability:** Access to a diverse and comprehensive dataset of both genuine and forged videos for training and testing is crucial for developing robust detection methods. However, obtaining such datasets can be challenging due to privacy and ethical considerations.

7. **Ethical and Legal Considerations:** The use of forgery detection techniques in legal and investigative contexts raises ethical and legal questions about privacy, consent, and the admissibility of evidence.

8. **Interpretability:** Many advanced forgery detection techniques, particularly those based on deep learning, are often seen as "black boxes" where it's challenging to explain why a particular decision was made, which can be problematic in legal proceedings.

9. **Scalability:** As the volume of video content continues to grow, scalable forgery detection solutions are needed to process and analyse vast amounts of data efficiently.

10. **Adversarial Attacks:** Malicious actors may actively attempt to thwart forgery detection algorithms by using adversarial attacks. These attacks aim to make the detection process more challenging by intentionally introducing subtle manipulations that evade detection.

Overcoming these challenges in video forgery detection requires interdisciplinary research involving computer vision, machine learning, signal processing, and forensic analysis. Additionally, collaboration between researchers, industry experts, and legal professionals is essential to address the ethical and legal aspects of this field.

VI. CONCLUSION

In an era characterized by the widespread dissemination of digital video content, the detection of video forgeries emerges as a paramount challenge with far-reaching implications for society, security, and trustworthiness. This comprehensive review has ventured into the multifaceted landscape of video forgery detection, aiming to distill the essence of research endeavors, methodologies, challenges, and future prospects within this pivotal domain.

From the categorization of video forgeries into diverse forms, including splicing, deepfakes, and object removal, to the exploration of cutting-edge detection methodologies spanning digital watermarking, machine learning, and compression analysis, this review has illuminated the evolving arms race between forgers and forensic analysts. As the fidelity and accessibility of manipulation tools continue to advance, the urgency of robust detection mechanisms becomes increasingly evident.

As we look toward the future, emerging trends such as blockchain integration and increasingly transparent and interpretable AI models hold promise for addressing current limitations. The societal and legal implications of effective video forgery detection cannot be overstated. It is incumbent upon researchers, practitioners, and policymakers to forge a path forward that balances technological advancements with ethical considerations and societal safeguards.

In closing, this comprehensive review underscores the multifaceted nature of video forgery detection, offering a panoramic view of the field's challenges, achievements, and future directions. The quest for preserving the integrity of digital video content continues, with each discovery, innovation, and collaboration propelling us closer to a more secure and trustworthy digital landscape.

REFERENCES

[1] Haichao Yao, Rongrong Ni, Yao Zhao: An approach to detect video frame deletion under anti-forensics, (2019) Journal of Real-Time Image Processing

[2] Markos Zampoglou, Foteini Markatopoulou, Gregoire Mercier, Despoina Touska: Detecting tampered videos with multimedia forensics and deep learning Proc. 25th Int. Conf. on Multimedia Modeling (MMM 2019), Springer

[3] Vaishali Joshi, Sanjay Jain: Tampering detection and localization in digital video using temporal difference between adjacent frames of actual and reconstructed video clip, Bharati Vidyapeeth's Institute of Computer Applications and Management 2019 Int. j. inf. tecnol.

[4] Mubbashar saddique *et al.* Spatial video forgery detection and localization using texuture analysis of consecutive frames *,(2019)*Advances in the electrical and computer engineering

[5] Pevny, T., Bas, P., Fridrich, J.: Steganalysis by subtractive pixel adjacency matrix. IEEE Trans. Inf. Forensics Secur. (2010)

[6] Johnston, p., Elyan, e., Jayne, C. 2018. Toward video tampering exposure: Inferring compression parameters from pixels ,19th International Conference on Engineering Applications of Neural Networks (EAN). Springer International Publishing

[7] Pamela Johnston, Eyad Elyan, and Chrisina Jayne. Video tampering localisation using features learned from authentic content, Neural Computing and Applications, Springer, 2019

[8] Shan Jia,Zhengquan Xu, Hao Wang, Chunhui Feng, and Tao Wang, Coarse-to-fine Copy-move Forgery Detection for Video Forensics CVPR Workshop 2019 IEEE Access

[9] Omar Ismael Al-Sanjary, Ghazali Sulong: Detection of video forgery: a review of literature, (2015)Journal of Theoretical and Applied Information Technology. Vol.74 No.2

[10] A.V. Subramanyam, Sabu Emmanuel: Video forgery detection using hog features and compression properties, 2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP) 2012 IEEE

[11] Yuting Su, Weizhi Nie, Chengqian Zhang : A Frame Tampering Detection Algorithm for MPEG videos , 6th IEEE Joint International Information Technology and Artificial Intelligence Conference 2011 IEEE

[12] Shruti Agarwal and Hany Farid: Photo Forensics from JPEG Dimples, 2017 IEEE Workshop on Information Forensics and Security (WIFS)

[13] B. D. Lucas, and T. Kanade, "An iterative image registration technique with an application to stereo vision." International Joint Conference on Artificial Intelligence. Morgan Kaufmann Publishers Inc 1981.

[14] [Minyoung Huh, Andrew Liu, Andrew Owens, Alexei A. Efros: Fighting Fake News: Image Splice Detection via Learned Self-Consistency ECCV2018

[15] M Reith, C Carr, G Gunsch: "An examination of digital forensic models". International Journal of Digital Evidence (2002).

[16] Rohini Sawant, Manoj Sabnis: A Review of Video Forgery and Its Detection IOSR Journal of Computer Engineering (IOSR-JCE) (2018)

[17] Kobayashi, M., Okabe, T., & Sato, Y. : Detecting forgery from static-scene video based on inconsistency in noise level functions, *Information Forensics and Security*(2010).

[18] Kelton A.P. da Costa et.al : A critical literature survey and prospects on tampering and anomaly detection in image data, Applied Soft Computing Journal(2020)

[19] Rahul Thakur, Rajesh Rohilla : Review Article Recent advances in digital image manipulation detection techniques: A brief review, *Forensic Science International*(2020)

[20] H. Kasban a,∗ , Sabry Nassar b: "An efficient approach for forgery detection in digital images using Hilbert–Huang transform", Applied Soft Computing Journal(2020)

[21] Surrey University Library for Forensic Analysis (SULFA) of video content January 2012 DOI: 10.1049/cp.2012.0422 Conference: Image Processing (IPR 2012)

[22] D'Avino D, Cozzolino D, Poggi G, Verdoliva L : Autoencoder with recurrent neural networksfor video forgery detection. Electron Imaging 2017(7):92–99. https://doi.org/10.2352/ISSN.2470-1173.2017.7.MWSF-330

[23] Al-Sanjary OI, Ahmed AA, Sulong G : Development of a video tampering dataset for forensicinvestigation. Forensic Sci Int 266:565–572. https://doi.org/10.1016/j.forsciint.2016.07.013 (2016)

[24] Hitesh D. Panchal, Dr. Hitesh Shah: Video tampering dataset development in temporal domain for video forgery authentication September 2020 Multimedia Tools and Applications 79(33-34) DOI: 10.1007/s11042-020-09205-w

[25] O. Papadopoulou, S. Papadopoulos, M. Zampoglou, I. Kompatsiaris (CERTH-ITI), D. Teyssou (AFP): InVID Fake Video Corpus 2018 (v2.0), https://mklab.iti.gr/results/fake-video-corpus/

[26] Jing Dong,Wei Wang,Tieniu Tan: CASIA Image Tampering Detection Evaluation Database, Conference on Signal and Information Processing (ChinaSIP), 2013 IEEE China Summit & International, July 2013,DOI: 10.1109/ChinaSIP.2013.6625374

[27] Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra: "A sift-based forensic method for copy–move attack detectionand transformation recovery," IEEE Transactions on Infor-mation Forensics and Security, vol. 6, no. 3, pp. 1099–1110,2011.

[28] Y.-F. Hsu and S.-F. Chang: "Detecting image splicing usinggeometry invariants and camera characteristics consistency,"in Proceedings of the International Conference on Multimediaand Expo (ICME), Toronto, Canada, July 2006.

[29] B. Wen, Y. Zhu, R. Subramanian, T.-T. Ng, X. Shen, and S. Winkler: "COVERAGE-A novel database for copy-moveforgery detection," in Proceedings of the 2016 IEEE Interna-tional Conference on Image Processing (ICIP), pp. 161–165,Phoenix, AZ, USA, September 2016

[30] https://recodbr.wordpress.com/code-n-data/

