JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Analysis of Various Fraud in Videos Detection Types And Techniques

Prof. Kamal Kishore
Associate professor
Modern Group of colleges
Email: kamalmehta30880@gmail.com

Abstract

With the advancement in technology Video processing tools and techniques are available for altering the Videos for forgery. The modification or changes in current Video is vital to detect since this Video can be used in the authentication process. Video credibility hence required to be verified. This is accomplished by the use of forgery detection mechanism. There are different ways by which Video can be tempered. For example: resampling, copy and move, splicing etc. In this paper techniques used to detect forgery from within the Video is analysed. The techniques analysed in this literature includes i) inter frame forgery detection ii) intra frame forgery detection iii) object based mechanism iv) pixel based approach. Examination of different techniques and expressing best possible mechanism for forgery detection is aim of this literature. Object based and pixel based approaches are of prime concern in most of research work. Object based approach uses applications of abstraction and provide difference approach to detect maliciousness within video. Pixel based approach can handle forgery but modification in terms of neighborhood selection must be made for better classification accuracy.

Keywords: Forgery, forgery detection, copy move, splicing

1. INTRODUCTION

Fraud in Videos in the modern era requires attention significantly. The prime reason for the same is transmission of information using multimedia is preferred choice due to low encryption cost. The processing of information within multimedia is through frame reading. Due to mass utilization of this mechanism in transmission, it is maliciously attacked by hackers and frames are altered. To this end researcher uses distinct mechanism to perform encryption and detecting forgery if any within video frames.

[1]The digital video tampering in which the contents of videos is modified or changed to made it doctored or fake video. [2]Tampering can be done using various techniques. There are following types of tampering that are applied to videos:

a) Shot level Tampering
b) Frame level Tampering
c) Block level Tampering
d) Pixel level Tampering

a) Shot Level Tampering
In this type tampering the scene is detected from videos and then this scene is copied to another place or manipulation is done in scene. This tampering is used in temporal or spatial level.

b) Frame Level Tampering
The frame from videos are extracted first than tampering is done on these frames. The forgery may remove, add or copy the frames for changing the contents of videos. It is one of temporal tampering mechanisms used to alter frames within the videos.

c) Block Level Tempering

The tampering is applied on blocks of videos that is any specified area of video frames. In this blocks are cropped and replaced in videos. It is spatial tampering that are performed at block level.

d) Pixel Level Tempering

In this video frames are change at pixel level. In this pixels of videos are modified or copied
or replaced. The spatial attacks are performed at pixel level.

[3]These tempering mechanisms can be avoided by the use of Fraud in Videos detection mechanisms. The mechanisms are distinguished as inter, intra and compression based forgery detection mechanisms. These mechanisms are described briefly in section 2.

Rest of the paper is organized as under: section 2 gives literature survey describing Fraud in Videos detection procedures , section 3 presents qualitative analysis of Fraud in Videos detection procedure, section 4 gives comparative analysis and section 5 gives conclusion and future scope.

2. VIDEO FOREGRY DETECTION MECHANISMS

Fraud in Videos Detection is a significantly emerging discipline in Image Processing that acts as a countermeasure to intentional misuse of visual data like videos and different digital editing tools. [4]Fraud in Videos Detection's aims to establish the authenticity of a video and to expose the potential modifications and forgeries that the video might have undergone. Undesired post processing operations or forgeries generally are irreversible and leave some digital footprints. Fraud in Videos detection techniques scrutinize these footprints in order to differentiate between original and the forged videos. When a video is forged some of its fundamental properties change and to detect these changes is what is called as Fraud in Videos Detection techniques used for. Thus it is the scientific understanding and skill required to amplify and authenticate video recordings.

There are two fundamental approaches for Fraud in Videos Detection: Active Approach and Passive Approach.

Active Approach: Active Forgery Detection includes techniques like Digital Watermarking and [5]Digital Signatures which are helpful to authentic Content Ownership and Copyright Violations. Tough the basic application of Watermarking and Signatures is Copyright protection it can be used for Fingerprint, Forgery Detection, Error concealment etc. There are several drawbacks to the active approach as it requires a signature or watermark to be embedded during the acquisition phase at the time of recording or an individual person to embed it later after acquisition phase at the time of sending. This limits the application of active approach due to the need of distinctive hardware like specially equipped cameras. Other issues which have an impact on the robustness of Watermarks and Signatures are factors like compression, scaling, noise etc.

Passive Approach: Passive Forgery Detection techniques are considered as an advancing route in Digital security. [6]The approach works in contrast to that of the Active approach. This approach works in without the constraint for specialized hardware nor does it require any firsthand information about the video contents. Thus it is also called as Passive-Blind Approach. The basic assumption made by this approach is that Videos have some inherent properties or features which are consistent in original videos. When a video is forged these patterns are altered. Passive approaches extract these features from a video and analyze them for different forgery detection purposes.

Thus to overcome the inefficiency encountered in the Active Approach the use of Passive Approach for Fraud in Videos detection can be made. Passive Approach thus proves to be better than the Active ones as it works on the firsthand information without the need for extra information bits and hardware requirements. It totally relies on the available forged video data and its intrinsic features and properties without the need of original video data.

To be specific active techniques includes motion detection mechanisms and passive technique includes static mechanisms. The forgery under static mechanisms falls under inter, intra and compression based mechanisms

- **Inter frame forgery detection**

Inter frame forgery detection mechanism exploit the temporal correlation between the frames within the video[7]. The parity difference between frames is used as a footprint to locate any problems within the video frames. The parity difference between frame is exploited by the use of even or odd parity check mechanisms. The parity check mechanism incorporated checks weather data transmission includes even number of frames or odd number of frames. In case sent frames in even parity and transmitted frames are in odd parity then forgery is detected.

- **Intra frame forgery detection**

Intra frame forgery detection uses the gaps between the frames to detect the forgery if any between the video frames. These mechanisms include copy move forgery, splicing etc. The image frames within videos are altered by the use of this mechanism. To detect such forgery, boundary colors and frames distinguishment is analyzed. Result in terms of bit error rate is expressed using these mechanisms.

- **Compression based mechanisms**

The compression based mechanisms includes discrete cosine transformation. These mechanisms replace multiple distinct values from within the image frame with single valued vectors. The feature vector then identified any malicious activity within the video frames. Results are most often expressed in the form of peak signal to noise ratio.

Fraud in Videos Detection Mechanisms are critical and are divided into following two categories: active and passive forgery detection.

The techniques considered for Fraud in Videos detection expressed in terms of comparison table in this section.

3. QUALITATIVE ANALYSIS OF FRAUD IN VIDEOS DETECTION

Fraud in Videos detection mechanisms analyzed in section 2 are compared in terms of parameters in this section. The comparative analysis of Fraud in Videos detection including both inter frame as well intra frame forgery detection mechanisms are highlighted in table 1

Categories of method	S.No.	Paper Name	Author	Year	Description	Advantages	Disadvantages	Accuracy
Inter frame forgery: **Insertion**	[8]	Inter-frame forgery detection in H.264 videos using motion and brightness gradients	Staffy Kingra & Naveen Aggarwal & Raahat Devender Singh	2017	It proposes methodology that utilizes prediction residual and optical flow inconsistencies to detect frame-insertion, removal and duplication in MPEG-2 and H.264 encoded Videos. It is used for detecting forgeries in videos by exhibiting object motion.	It reduces the conflicting results It gives precise localization of forgery	Performance of system suffers when high illumination videos are used	It has average detection accuracy around 83% which is depended upon number of deleted frames.
Inter frame forgery: Deletion	[9]	Video Inter-frame Forgery Detection Approach for Surveillance and Mobile Recorded	S. Kingra, Staffy Aggarwal, Naveen Singh, Raahat Devender	2017	It proposes hybrid mechanism that uses motion and gradient feature to measure variation	The defects are automatically detected using spikes count. It is	It unable to detect forgery frame in slow motion videos	Detection is depended on the bit rate of video sequences . it detect maximum and

		Videos			between various frames. In this forensic artifacts are analyzed using objective methodology	independent of the number and location of the tampered frames		minimum number of frames forged is 60 and 10.
Compression based forgery detection	[10]	Frame-wise Detection of Relocated I-frames in Double Compressed H.264 Videos Based on Convolutional Neural Network	He, Peisong Jiang, Xinghao Sun, Tanfeng Wang, Shilin Li, Bin Dong, Yi	2017	Proposed a methodology that utilizes preprocessing and CNN mechanism for frame wise detection of compressed videos forgery.	It has high performance for relocating I-frames in compressed videos	In preprocessing phase the filtering mechanism should be enhanced for better detection It does not apply frame wise detection result for various detection of inter frame forgeries	The average accuracy is around 96% which is bsed on GOPs
Double compression detection	[11]	Double Compression Detection in MPEG-4 Videos Based on Block Artifact Measurement with Variation of Prediction Footprint	Wei, Wei Gulla, Jon Atle Fu, Zhang	2016	Technique uses block artifacts for detection of compression based forgery . it combined VPF along with block artifacts for robust and efficient detection abilities.	It handles compressed videos efficiently	Low compression bit rate videos are no handled	It gives better discriminative performances compared existing technique
Inter-frame Fraud in Videos: insertion based	[12]	Inter-frame Fraud in Videos Detection Based on Block-Wise Brightness Variance Descriptor	Zheng, Lu Sun, Tanfeng Shi, Yun-qing	2016	Describes method called block-wise brightness variance descriptor (BBVD) that is based on detecting Fraud in Videos using new features.	It gives better precision and detection rate	It is not suitable for compressed videos	This method is efficient to detect motion object from static background subtraction technique, & then the object boundary is located

Inter frame using duplication method	[13]	This is a copy move forgery detection mechanism that is used to detect the forgery from the background of the image	G.Ulutas, Guzin Muzaffer, Gul	2016	Copy move forgery is detected using the hybrid mechanism. The result is presented in terms of classification accuracy	This method is helpful in inserting new frame and removing existing frames	Feature extraction and detection procedure is slow in nature	The detection is better although process can be made more faster by eliminating the similar pixels
Intra frame forgery: object level	[14]	Reasoning mechanism from the object within video is used	Fabien Baradel, Natalia Neverova, Christian Wolf, Julien Mille, and Greg Mori	2018	Object detection mechanism is used using reasoning based mechanism	Forged regions within the image is detected quickly	Compress videos are difficult to handle	Detection accuracy is less and menitude is only 46%
Intra frame : forgery detections	[15]	Authentication mechanism on videos is applied to determine the forgery	Raahat Devender Singh · Naveen Aggarwal	2017	This paper conducted the review on Fraud in Videos detection mechanism	Merits and demerits of each mechanism is highlighted	Classification accuracy and mean square error is not printed	Methodology of distinct algorithms is clearly described using the said mechanism
Inter frame : insertion, deletion	[16]	Inter-frame forgery detection mechanisms are elaborated	Sitara K. , B. M. Mehtrea	2018	New forensic mechanisms are elaborated using the said mechanisms	Result is given in terms of reliability metric	More than one compress video is used hence it is not considered effective forgery detection mechanism	Detection rate is better but can be further improved
Compression based	[17]	Double compressed image is detected using this mechanism	Yao, Heng Song, Saihua Qin, Chuan Tang, Zhenjun Liu, Xiaokai	2017	Proposed a mechanism in order to detect the abnormality from the transmitted image. The transmitted image is detected using pre-processing mechanism. The mechanism performs the operation at very high speed as compared to normal	The accuracy of forgery detection is better as compared to existing method	Only robust to MPEG compression and recompression	The rank of accuracy is better

					compression mechanism			
Intra frame detection: copy move	[18]	Review of copy move forgery detection mechanism is conducted.	Zhang, Zhi Wang, Chengyou Zhou, Xiao	2018	It provide the in-depth study of copy move forgery detection mechanism	This method is good enough for high quality videos	The complexity associated with computation is very high	Rate of detection is low. The detection rate can be improved by compressing the image using decomposition levels.
Inter-frame Fraud in Videos: deletion based	[19]	Localization mechanism in inter frame forgery detection mechanism is used	Abbasi Aghamaleki, Javad Behrad, Alireza	2016	Inter frame tempering mechanism is employed to determine the forgery within the image.	Splitting of image into different bands and then complexity of operation is reduced significantly.	Rejoining of spitted image may not give original image	Classification accuracy is poor
Inter frame: insertion based	[20]	A Digital Forensic Technique for Inter–Frame Fraud in Videos Detection Basedon3DCNN	Ouedraogo, Moussa Mouratidis, Haralambos Dubois, Eric	2015	This mechanism uses 3D Convolution neural network to overcome the problem of forgery detection. This mechanism is based on forming layers and then problem is resolved using processing mechanism	Image is processed using the object model	Unable to detect the exact formation of the object	Double MPEG compression can be supported using this mechanism
Intra frame: slicing based	[21]	A compact model for forgery detection is implemented using this mechanism	Afchar, Darius Nozick, Vincent Yamagishi, Junichi Echizen, Isao	2018	Detection of facial images using the model based approach is efficient	Scale invariant feature extraction is implemented to detect abnormality from within the video.	Exact extraction of the pixel intensity is not possible using the above said mechanism	Automatic detection of problems within the facial image is possible this mechanism
Intra frame : copy	[22]	Coarse-to-fine Copy-move Forgery	Jia, Shan Xu, Zhengquan	2018	It proposed a coarse-to-fine approach based	Duplicated regions detect with	High computation time of the	Accuracy was found to

move		Detection for Video Forensics	Wang, Hao Feng, Chunhui Wang, Tao		on video OF features. It detects copy move forgery from videos with the help of overflow feature.	changed contrast values and blurred regions can also be detected.	algorithm.	be 98.79
Intra frame : object detection based	[23]	Fraud in Videos detection using Hybrid techniques	Randeep Kaur, Er. Jasdeep Kaur	2016	Proposed a hybrid technique that utilizes DWT & optical flow. The DWT is used to compress the frame and optical flow is used to detect the flow of the moving objects and the forgery object. e	Extracting features and sorting are done in different algorithms in parallel, less computational time, good for real-time applications.	Not applicable to color images.	14 video sequences allowing an accuracy of 95%
Intra frame: copy move forgery	[24]	Improvement in Copy -Move Forgery Detection Using Hybrid Approach	Gurmeet Kaur Saini, Manish Mahajan	2016	Scale invariant feature extraction along with the support vector machine is used to detect problems from within the image	Multi-dimensional and multi-directional gives precise results.	Cannot be applied on compressed images.	Videos is first converted into image frames that can have JPEG extension only. This is a problem however using this mechanism classification accuracy is significantly improved.
Intra frame: Upscale crop	[25]	Semi-automatic Methods in Fraud in Videos Detection Based on Multi-view Dimension	Alade, Oyekale Abel Selamat, Ali Sallehuddin, Roselina	2018	Visual inspection framework is suggested to detect forgery if an from within the image. Video is first of all converted into image frames and then analysis is	Low complexity in calculation allow execution time to be minimized	In case image contains multiple forgery regions then this mechanism cannot detect the forged region	Detection rate is good and approximately in range of 84%

					conducted. The analysis is highlighted by the use of bounding box mechanism. This means abnormality is highlighted and hence can be improved greatly using the proposed mechanism		efficiently.	
Inter frame: compression based	[26]	FRAUD IN VIDEOS DETECTION USING HOG FEATURES AND COMPRESSION PROPERTIES	A.V. Subramanyam, Sabu Emmanuel School	2017	Copy move forgery is described through this literature. This mechanism can be further improved using clustering mechanism. The clustering of similar regions can be made to reduce execution ime.	It gives good accuracy in case of compressed, scaling and filtered videos.	Complexity is high	Detection accuracy is ≈ 84.5% for 60x60 forged region
Intra frame: object level	[27]	A Fraud in Videos Detection Using Discrete Wavelet Transform and Scale Invarient Feature Transform Techniques	Gurjinder Kaur, Rishamjot Kaur	2016	Describes a SIFT and DWT based algorithm that first of all extract features of video frames then forged region is detected. It is mostly used for Location of vindictive control with computerized recordings (advanced frauds)	It can robustly identify objects even among clutter and under partial occlusion	It is not useful for real time videos	The leaving model 98.2143 exactness quality is figured while in proposed model we get the estimation of precision 99.2454.The proposed model get more phony Frame when contrasted with exiting mode
Inter frame: Insertion	[28]	PASSIVE FRAUD IN VIDEOS DETECTION	Bagiwa, Aminu Mustapha;	2017	Proposed a correlation based mechanism to	It minimize the rate of wrong conviction	It can only detect inpainting for object	The detection rate is

based		USING FRAME CORRELATION STATISTICAL FEATURES			detect forgery from within the videos. The highest correlation attributes are compared at first place within test and training data. The entire test data hence is not required to be compared using this mechanism. This means execution time in detecting the forgery is reduced significantly. In addition true positive rate is also improved. True positive rate is directly related with classification accuracy.	based on inconclusive digital vide	removal in a video that is on a static background	91.08%
Intra frame: upscale crop	[29]	Data Authentication and Security Using Video Watermarking	Ritesh Bagalkoti, Heena Sheikh, Ankita Pawar, Nikita Dhawade	2015	Proposed a video watermarking technique that are used for hiding data and discourage forged data to be transmitted.	Security achieved through video watermarking is described through this literature	No filtering mechanism to tackle noise within the video frames is discussed	It has 93 % accuracy to hide data
Intra frame: sampling based	[30]	AN EFFICIENT I-ENCRYPTED VIDEO WATERMARKING SCHEME USING ENCHANCED PCA-SVD-DWT BLOCK EMBEDDING AND EXTRACTION	T.SRINIVASA RAO, 2DR.RAJASEKHAR R KURRA	2016	Proposes i-Encrypted PCA-SVD-DWT model that is used for video authentication as well as security to data modification. It optimized data and check its integrity during	Modern video content monitoring that could be used to block certain contents could be useful for children	Monitoring does not includes any filtering mechanism that could improve overall process of content monitoring	has high efficiency in terms of time and accuracy is concerned.

		MODEL			video watermark schemes.			
Inter frame: Duplication based	[31]	Inter frame forgery detection mechanism using bling fold strategy is implemented	Dong-Ning Zhao, & Ren-KuiWang & Zhe-Ming Lu	2018	This mechanism is partitioned into phases. The first phase is applied to remove noise if any within the image frame extracted from within the video. Second phase includes applying segmentation procedure that divides entire image into critical and non-critical regions.	Motion based detection mechanism is implemented and hence is more efficient then static videos.	Motion within the videos cannot be tackled and hence problem of motion videos cannot be resolved	Classification accuracy of 80% is achieved which can be further iproved.
Intra frame: Object level	[32]	Object Detection in Video with Spatiotemporal Sampling Networks	Qian Xie, Oussama Remil, Yanwen Guo, Mingqiang Wei, Meng Wang, Jun Wang	2018	Proposed an approach that segment and track forged region from video using RGB-D technique. It uses clustering technique that collects objects in terms of keyframes and then segmentation is done to detect object.	High performance processor lead to faster processing of videos	It does not process 3d videos	tradeoff between segmentation quality and computation cost is minimum
Intra frame: object level	[33]	Object-Level Motion Detection from Moving Cameras Article	Chen, Tao Lu, Shijian	2017	Proposes a context-aware motion descriptor (CMD) for object-level motion detection from a moving camera. The CMD is constructed based on the contextual flow field around an	High performance processor and video processing of static video frames with noise filtering	Motion video processing with camera motion is not considered in this approach	Classification accuracy is better,

					object and it consists of several component modules			
Intra frame: Object detection based	[34]	Context Matters: Refining Object Detection in Video with Recurrent Neural Networks	Tripathi, Subarna Lipton, Zachary C. Belongie, Serge Nguyen, Truong	2016	Describes a new framework for improving object detec-tion in videos that captures temporal context and encourages consistency of predictions. First, it train a pseudo-labeler, that is, a domain-adapted convolutional neural network for object detection	It optimizes both accuracy on the target frame and consistency across con-secutive frames.	Improvement in localization of multiple objects is needed.	It has mean Average Precision (mAP) of 68.73, an improvement of 7.1 over the strongest image-based baselines
Intra frame: Object level	[35]	Optimizing Video Object Detection via a Scale-Time Lattice Kai	Kai Chen1 JiaqiWang1 Shuo Yang1	2018	Proposed a hybrid approach that uses detection, temporal propagation, and across-scale refinement. The various configurations designed under this space and demon- strated their competitive performance against state-of-the- art video object detectors with much faster speed.	The symmetry reduces execution time	Classification accuracy can be further improved by the use of STLK	It quantify the mAP of detections on adaptively selected key frames than uniformly sampled ones (73.3 vs 74.1
Intra frame: Object level	[36]	Fast and accurate object detection in high resolution 4K and 8K video using	V´ ıt R˚zi˘ u˘ cka and Franz Franchett	2018	Describes a methodology that is based on pipeline for detection of forged object into videos. It has two stages	Video processing with great speed using GPU is achieved	This procedure is expensive and cannot be employed for simple applications	Detection is 81.3 % accurate

		GPUs V´			firstly evaluation of each image or video frame under rough and then refined resolution to limit the total number of necessary evaluation.			
Intra frame: upscale based	[37]	Detection of Upscale-Crop and Partial Manipulation in Surveillance Video Based on Sensor Pattern Noise Dai-Kyung	Dai-Kyung Hyun 1, Seung-Jin Ryu 1, Hae-Yeoun Lee 2 and Heung-Kyu Lee 1,*	2013	Describes technique based on sensor pattern noise to detect video surveillance forgeries. It checks the video frames and traces the upscaling in video.	Analysis of cracked region of surface is accurately done using this mechanism	Filtering mechanism description along with motion video processing is not given	detected forgeries with over 90% accuracy regardless of the size of the doctored region
Intra frame: object level	[38]	Salient Object Detection with Chained Multi-Scale Fully Convolutional Network	Youbao Tang, Xiangqian Wu	2017	Describes methodology that uses multi-scaled CNN for detecting forgeries in videos. It uses chain based mechanism for detecting deteriorate frames	It improve the saliency prediction results.	Complexity is high	Precision is better
Intra frame: copy move based	[39]	Survey On Keypoint Based Copy-move Forgery Detection Methods On Image	Devanshi Chauhana*, Dipali Kasatb	2016	Describes various techniques that are used to detect keypoint frames in copy move forgeries.	Review of techniques used to detect object from the video frame.	Motion based object detection is not conducted hence area interlacing mechanisms with noise handling is missing	
Inter frame: insertion based	[40]	Detection of video double encoding with GOP size estimation	D. V´ azquez-Pad´ ın#1 , M. Fontani∗§	2013	Describes technique that handled twice encoded Fraud in Videos. It estimate the	It is very robust even in realistic settings	The re-encoding of video frame is not considered	Detection rate is better along with size estimation

					size of the Group Of Pictures (GOP) employed during the first encoding			
Inter frame: deletion based	[4]	Detection of frame deletion for digital video forensics	Tamer Shanableh*	2013	Proposed technique for detecting deletion of frames within the videos. It is machine learning based strategy in which first of all features are extracted and the video is reconstructed	It is capable of detecting forged videos with various numbers of deleted frame	High Execution time	a true positive rate of around 95% and a false negative rate of 4% were reported
Inter frame: insertion and deletion based	[41]	A VIDEO FORENSIC TECHNIQUE FOR DETECTING FRAME DELETION AND INSERTION	Gironi, A Piva, A It, Siena	2014	Describes technique that is based on localization. It detect removal or insertion of frames within the digital videos. It is reliable method in which compression is strong and performance is good.	It is able to locate the point in time where frames have been deleted or inserted.	Motion of frames are not considered	accuracy of methodology is around 83%.
Inter frame :object based	[42]	Identifying Fraud in Videos Process Using Optical Flow	Wan Wang1, Xinghao Jiang	2016	In this variation between various frames of videos is detected using optical flow mechanism. It identify deletion / insertion of frames within digital videos.	It is robust algorithm	It is not suitable for large forgery dataset	The accuracy for tempered videos is around 93.3 %.
Inter frame: compression based	[43]	Detection of Re-Compression, Transcoding and Frame-Deletion for Digital Video	Raahat Devender Singh, Naveen Aggarwal	2016	Describes a compression based technique which firstly transcode the videos and then	It is inexpensive and independent of heuristically-	The frame addition is not considered in this approach	frame-removal detection technique achieved an average accuracy of

		Authentication			recompress it to identify forged frames. It uses optical flow so accuracy is better.	computed thresholds		99.3%
Inter frame: object detection based	[44]	A Novel Video Inter-frame Forgery Model Detection Scheme Based on Optical Flow Consistency	Juan Chao, Xinghao Jiang, and Tanfeng Sun	2018	Proposes binary search based detection of insertion of new frames within the video. It uses window based techniques for detecting deletion/insertion.	Gives better accuracy	Complexity is high	Recall rate reaches 95% and the precision rate reaches 98% of frame insertion forgery detection. For frame deletion forgery detection.
Inter frame: duplication based	[45]	Chroma Key Background Detection For Digital Video Using Statistical Correlation Of Blurring Artifact	Mustapha Aminu Bagiwa, Ainuddin Wahid Abdul Wahab ,	2016	Describes technique based on artifacts to detect features of videos. It first of all extract the frame that has blurring effect than it is further analyzed for forged region.	Gives better recall rate with efficiency	It does not handled background color.	Technique achieving detection accuracy of 91.12% for chroma key forgery Technique
Intra frame: copy move based	[46]	Detection of Regional Copy/Move Forgery in MPEG Videos using Optical Flow	Amir Bidokhti, Shahrokh Ghaemmaghaam	2015	Proposes a coefficient based detection of forged frames that uses optical flow.	Copy move forgery by the use of segmentation mechanism	High Execution time	Accuracy is around 88 s%

Table 1: Analysis of Fraud in Videos detection mechanisms

COMPARATIVE STUDIES

The comparative study suggest that motion based forgery detection mechanism are uncommon and hard to detect. In category 1(inter frame forgery) mechanism 40% of the research papers are analyzed and major part of the research is focused upon the parameters such as mean square error and peak signal to noise ratio. In category 2(intra frame forgery)35% of research papers falls and noise handling procedure accommodated within these papers allow peak

signal to noise ratio to enhance. In category 3(compression mechanism) 25% of the papers lies and Fraud in Videos detection mechanism employed within such situation causes frame rate to decrease and hence noise within frame increases. The detection mechanism allows parameters like PSNR and MSE to be optimized.

CONCLUSION

This paper analyse the various techniques used in order to tackle the forgery within the digital Videos. Technology is enhancing by leaps and bounds. Information now days represented through Videos rather than textually. Earlier forgery commonly takes place with text information but now days Fraud in Videos is common. In order to tackle the issue forgery detection mechanisms are researched over.

References

[1] S. Kingra, N. Aggarwal, and R. D. Singh, "Inter-frame forgery detection in H.264 videos using motion and brightness gradients," *Multimed. Tools Appl.*, vol. 76, no. 24, pp. 25767–25786, 2017.

[2] S. Kingra, N. Aggarwal, and R. D. Singh, "Video inter-frame forgery detection approach for surveillance and mobile recorded videos," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 2, pp. 831–841, 2017.

[3] P. He, X. Jiang, T. Sun, S. Wang, B. Li, and Y. Dong, "Frame-wise detection of relocated I-frames in double compressed H.264 videos based on convolutional neural network," *J. Vis. Commun. Image Represent.*, vol. 48, pp. 149–158, 2017.

[4] W. Wei, J. A. Gulla, and Z. Fu, "Advanced Intelligent Computing Theories and Applications," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6215, no. 2, pp. 380–391, 2010.

[5] L. Zheng, T. Sun, and Y. Shi, "Digital-Forensics and Watermarking," vol. 9569, pp. 18–30, 2016.

[6] G. Ulutas and G. Muzaffer, "A New Copy Move Forgery Detection Method Resistant to Object Removal with Uniform Background Forgery," *Math. Probl. Eng.*, vol. 2016, 2016.

[7] F. Baradel, N. Neverova, C. Wolf, J. Mille, and G. Mori, "Object level visual reasoning in videos," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11217 LNCS, pp. 106–122, 2018.

[8] R. D. Singh and N. Aggarwal, "Video content authentication techniques: a comprehensive survey," *Multimed. Syst.*, vol. 24, no. 2, pp. 211–240, 2018.

[9] K. Sitara and B. M. Mehtre, "Detection of inter-frame forgeries in digital videos," *Forensic Sci. Int.*, vol. 289, pp. 186–206, 2018.

[10] H. Yao, S. Song, C. Qin, Z. Tang, and X. Liu, "Detection of double-compressed H.264/AVC video incorporating the features of the string of data bits and skip macroblocks," *Symmetry (Basel).*, vol. 9, no. 12, pp. 1–17, 2017.

[11] Z. Zhang, C. Wang, and X. Zhou, "A survey on passive image copy-move forgery detection," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 6–31, 2018.

[12] J. Abbasi Aghamaleki and A. Behrad, "Inter-frame Fraud in Videos detection and localization using intrinsic effects of double compression on quantization errors of video coding," *Signal Process. Image Commun.*, vol. 47, pp. 289–302, 2016.

[13] M. Ouedraogo, H. Mouratidis, and E. Dubois, *Information Systems Security Criticality*. Springer International Publishing, 2015.

[14] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "MesoNet: A compact facial Fraud in Videos

detection network," *10th IEEE Int. Work. Inf. Forensics Secur. WIFS 2018*, 2019.

[15] S. Jia, Z. Xu, H. Wang, C. Feng, and T. Wang, "Coarse-to-Fine Copy-Move Forgery Detection for Video Forensics," *IEEE Access*, vol. 6, no. c, pp. 25323–25335, 2018.

[16] R. Kaur and E. J. Kaur, "Fraud in Videos detection using Hybrid techniques," *Ijarcce*, vol. 5, no. 12, pp. 112–117, 2016.

[17] G. Kaur Saini and M. Mahajan, "Improvement in Copy -Move Forgery Detection Using Hybrid Approach," *Int. J. Mod. Educ. Comput. Sci.*, vol. 8, no. 12, pp. 56–63, 2016.

[18] O. A. Alade, A. Selamat, and R. Sallehuddin, "Recent Trends in Information and Communication Technology," vol. 5, no. May, 2018.

[19] A. V. Subramanyam and S. Emmanuel, "Fraud in Videos detection using HOG features and compression properties," *2017 IEEE 14th Int. Work. Multimed. Signal Process. MMSP 2017 - Proc.*, pp. 89–94, 2017.

[20] G. Kaur and R. Kaur, "A Fraud in Videos Detection Using Discrete Wavelet Transform and Scale Invarient Feature Transform Techniques," vol. 5, no. 11, pp. 1618–1623, 2016.

[21] A. M. Bagiwa, "Passive Fraud in Videos Detection Using Frame Correlation Statistical Features," 2017.

[22] R. Bagalkoti, H. Sheikh, A. Pawar, and N. Dhawade, "An Approach to Secure Data in Disruption Tolerant Network," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 11, pp. 0396–0400, 2015.

[23] T. Srinivasa Rao and R. R. Kurra, "An efficient i-Encrypted video watermarking scheme using enchanced PCA-SVD-DWT block embedding and extraction model," *J. Theor. Appl. Inf. Technol.*, vol. 93, no. 1, pp. 123–132, 2016.

[24] D. N. Zhao, R. K. Wang, and Z. M. Lu, "Inter-frame passive-blind forgery detection for video shot based on similarity analysis," *Multimed. Tools Appl.*, vol. 77, no. 19, pp. 25389–25408, 2018.

[25] G. Bertasius, L. Torresani, and J. Shi, "Object Detection in Video with," *Eccv*, pp. 1–16, 2018.

[26] T. Chen and S. Lu, "Object-Level Motion Detection from Moving Cameras," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 11, pp. 2333–2343, 2017.

[27] S. Tripathi, Z. C. Lipton, S. Belongie, and T. Nguyen, "Context matters: Refining object detection in video with recurrent neural networks," *Br. Mach. Vis. Conf. 2016, BMVC 2016*, vol. 2016–Septe, pp. 1–12, 2016.

[28] K. Chen *et al.*, "Optimizing Video Object Detection via a Scale-Time Lattice," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 7814–7823, 2018.

[29] V. Ruzicka and F. Franchetti, "Fast and accurate object detection in high resolution 4K and 8K video using GPUs," *2018 IEEE High Perform. Extrem. Comput. Conf. HPEC 2018*, 2018.

[30] D. K. Hyun, S. J. Ryu, H. Y. Lee, and H. K. Lee, "Detection of upscale-crop and partial manipulation in surveillance video based on sensor pattern noise," *Sensors (Switzerland)*, vol. 13, no. 9, pp. 12605–12631, 2013.

[31] Y. Tang and X. Wu, "Salient object detection with chained multi-scale fully convolutional network," *MM 2017 - Proc. 2017 ACM Multimed. Conf.*, pp. 618–626, 2017.

[32] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on Keypoint Based Copy-move Forgery

Detection Methods on Image," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 206–212, 2016.

[33] D. Vázquez-Padín, M. Fontani, T. Bianchi, P. Comesaña, A. Piva, and M. Barni, "Detection of video double encoding with GOP size estimation," *WIFS 2012 - Proc. 2012 IEEE Int. Work. Inf. Forensics Secur.*, pp. 151–156, 2012.

[34] T. Shanableh, "Detection of frame deletion for digital video forensics," *Digit. Investig.*, vol. 10, no. 4, pp. 350–360, 2013.

[35] A. Gironi, A. Piva, and S. It, "A VIDEO FORENSIC TECHNIQUE FOR DETECTING FRAME DELETION AND INSERTION Dept . of Information Engineering , Universit ` a di Firenze , Firenze ( IT ) CNIT , Universit ` Dept . of Electronic and Telecommunications , Politecnico di Torino , Torino (IT) Dept," pp. 6267–6271, 2014.

[36] W. Wang, X. Jiang, S. Wang, and M. Wan, "Digital-Forensics and Watermarking," vol. 9569, pp. 244–257, 2016.

[37] R. D. Singh and N. Aggarwal, "Detection of re-compression, transcoding and frame-deletion for digital video authentication," *2015 2nd Int. Conf. Recent Adv. Eng. Comput. Sci. RAECS 2015*, no. December, 2016.

[38] J. Chao, X. Jiang, and T. Sun, "A Novel Video Inter-frame Forgery Model Detection," *Springer-Verlag Berlin Heidelb.*, pp. 267–281, 2018.

[39] M. A. Bagiwa, A. W. A. Wahab, M. Y. I. Idris, S. Khan, and K. K. R. Choo, "Chroma key background detection for digital video using statistical correlation of blurring artifact," *Digit. Investig.*, vol. 19, pp. 29–43, 2016.

[40] A. Bidokhti and S. Ghaemmaghami, "Detection of regional copy/move forgery in MPEG videos using optical flow," *Proc. Int. Symp. Artif. Intell. Signal Process. AISP 2015*, no. June 2016, pp. 13–17, 2015.