Analysis of Various Video Forgery Detection Types and Techniques

Jagminder Kaur[1] and Raman Kumar[2]

[1,2]Department of Computer Science and Engineering
[1,2]I K Gujral Punjab Technical University, Kapurthala, Punjab, India

---

Abstract - *Now a day the automation of 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. Therefore the credibility of video must be verified and it is done with the help of forgery detection mechanism. The various video Tampering ways are resampling, copy and move, splicing etc. In this paper techniques used to detect forgery from within the Video are analyzed. The technique analyzed 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. The object-based approaches uses applications of abstraction and provide different approach to detect maliciousness within video. The pixel- based approach can handle forgery but modification in terms of neighborhood selection must be made for better classification accuracy*

Key Words: Forgery, Forgery detection, Copy move, Splicing

1. INTRODUCTION

Video forgery in the modern era requires attention significantly. The prime reason for the same is transference of information using multimedia is preferred choice due to low encryption cost. The processing of information within multimedia is through frame reading. This why the mass infliction 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) Low level tempering
b) Capturing frame by frame Tampering
c) Mass level Tampering
d) Voxel level Tampering

a) Low 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 by Frame Level Tampering

The frame from videos are extracted first than tampering is done on these frames. The forger 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) Mass 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) Voxel Level Tempering

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

[3] These tempering are avoid for using forgery detection mechanism. The mechanisms are distinguished as inter, intra and compression based forgery detection mechanisms. These mechanisms are described briefly in section 2.

The rest of this paper is assembled as under : section 2 gives literature survey narrate video forgery detection procedures , section 3 presents qualitative analysis of video forgery detection procedure, section 4 gives comparative analysis and section 5 gives conclusion and future scope.

2. VIDEO FOREGRY DETECTION MECHANISMS

Video Forgery 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]Video Forgery 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. Video forgery 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 Video Forgery 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 Video Forgery Detection: Active Approach and Passive Approach.

i. 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 in the least amount of time for recording or an individual staff to implant behind time after acquisition phase sending at a time. 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.

ii. 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. The 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 video forgery 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 utilized the temporal correlation between the frames within the video. The parity difference between frames is used as a footprint to locate any problems within the video frames. The utilization of frames by the using 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. Using this mechanism image frames are altered within the video. 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.

Video Forgery Detection Mechanisms are critical and This mechanism are divided into following two categories: active and passive forgery detection.

This techniques considered for video forgery detection expressed in terms of comparison table in this section.

3. Qualitative analysis of video forgery detection

Analyzations of video forgery detection mechanism in section 2 are compared in terms of parameters in this section. The comparative analysis of video forgery 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	[7]	Inter-frame forgery detection in H.264 videos using motion and brightness gradients	Staffy Kingra& Naveen Aggarwal &RaahatDevender Singh	2017	It proposes methodology H.264 encoded videos to detect frame insertion deletion and duplication in MPEG-2 that utilizes prediction residual and optical flow inconsistencies. It is used for detecting tampered 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	[8]	Video Inter-frame Forgery Detection Approach for Surveillance and Mobile Recorded Videos	S.Kingra, Staffy Aggarwal, Naveen Singh, RaahatDevender	2017	It proposes hybrid mechanism that uses action and incline feature to evaluate discrepancy between various frames. Using this forensic artifacts are analyzed the objective methodology.	The defects are automatically detected using spikes count. The number and location of the tempered frames are independent.	It unable to detect forgery frame in slow motion videos.	Detection is depended on the bit rate of video sequences . It detect maximum and minimum number of frames forged is 60 and 10.
Compression based forgery detection	[9]	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 tempering.	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	[10]	Double Compression Detection in MPEG-4 Videos Based on Block Artifact Measureme	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

		nt with Variation of Prediction Footprint						
Inter-frame Video Forgery: insertion based	[11]	Inter-frame Video Forgery 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 video forgery using new features.	It gives better precision and detection rate	It is not suitable for compressed videos	This manner is competent to discover the location of object boundary and static background subtraction technique to spot motion object.
Inter frame using duplication method	[12]	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	[13]	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	[14]	Authenticati on mechanism on videos is applied to determine the forgery	RaahatDe vender Singh · Naveen Aggarwal	2017	This paper conducted the review on video forgery detection mechanism	Merits and demerits of each mechanism is highlighted	Classification accuracy and mean square error is not printed	Methodolog y of distinct algorithms is clearly described using the said mechanism
Inter frame : insertion, deletion	[15]	Inter-frame forgery detection mechanism s 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
Compressio n based	[16]	Double compressed image is detected using this mechanism	Yao, Heng Song, Saihua Qin, Chuan Tang, Zhenjun	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	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

			Liu, Xiaokai		high speed as compared to normal compression mechanism			
Intra frame detection: copy move	[17]	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 Video Forgery: deletion based	[18]	Localization mechanism in inter frame forgery detection mechanism is used	AbbasiAghamaleki, 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	[19]	A Digital Forensic Technique for Inter–Frame Video Forgery Detection Basedon3D CNN	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	[20]	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 move	[21]	Coarse-to-fine Copy-move Forgery Detection for Video Forensics	Jia, Shan Xu, Zhengquan Wang, Hao Feng, Chunhui Wang, Tao	2018	It proposed a coarse-to-fine approach based on video OF features. It helps to overflow feature for identify copy move forgery from videos.	Duplicated regions detect with changed contrast values and blurred regions can also be detected.	High computation time of the algorithm.	Accuracy was found to be 98.79
Intra frame : object detection based	[22]	Video Forgery detection using Hybrid techniques	RandeepKaur, Er. JasdeepKaur	2016	Proposed a hybrid technique that utilizes DWT & optical flow. The DWT is used to compress the frame and optical flow is used to discover the copy item. E and the flow of moving objects.	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	[23]	Improvement in Copy - Move Forgery Detection Using Hybrid Approach	GurmeetKaurSaini, 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	[24]	Semi-automatic Methods in Video Forgery 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 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	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 efficiently.	Detection rate is good and approximately in range of 84%

Table 1: Analysis of video forgery detection mechanisms

4. COMPARATIVE STUDIES

The comparative study suggest that motion based forgery detection operations 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 video forgery 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

5. CONCLUSION

In this paper study 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 Video forgery is common. In order to tackle the issue forgery detection mechanisms are researched over.

REFERENCES

[1] R. Saranya, S. Saranya, and R. Cristin, "Exposing Video Forgery Detection Using Intrinsic Fingerprint Traces 1 1,2,3," pp. 73–76, 2017.

[2] F. Kelly, "Fast Probabilistic Inference and GPU Video Processing," IEEE Libr., no. May, 2006.

[3] N. Sedcole, "Reconfigurable platform-based design in FPGAs for video image processing," IEEE Libr., no. January, pp. 1–206, 2006.

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

[5] C. C. Hsu, T. Y. Hung, C. W. Lin, and C. T. Hsu, "Video forgery detection using correlation of noise residue," Proc. 2008 IEEE 10th Work. Multimed. Signal Process. MMSP 2008, no. June 2014, pp. 170–174, 2008.

[6] S. R. Papinwar, "Forgery Detection in Video Using Watermarking : A Review," vol. 7, no. 1, pp. 270–274, 2016.

[7] G. Chittapur, S. Murali, and B. S. Anami, "Video forgery detection using motion extractor by referring block matching algorithm," Int. J. Sci. Technol. Res., vol. 8, no. 10, pp. 3240–3243, 2019.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

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

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

[16] 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.

[17] 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.

[18] 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 Process. Image Commun., vol. 47, pp. 289–302, 2016.

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

[20] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, "MesoNet: A compact facial video forgery detection network," 10th IEEE Int. Work. Inf. Forensics Secur. WIFS 2018, 2019.

[21] 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.

[22] R. Kaur and E. J. Kaur, "Video Forgery detection using Hybrid techniques," Ijarcce, vol. 5, no. 12, pp. 112–117, 2016.

[23] 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.

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