Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105142, November 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Video Inter-frame Forgery Detection: A Survey

Staffy Kingra*, Naveen Aggarwal and Raahat Devender Singh

UIET, Panjab University, Chandigarh - 160014, Punjab, India; staffysk@gmail.com, navagg@gmail.com, raahat.singh@hotmail.com

Abstract

Objectives: This paper summarizes all the proposed techniques involved in digital video inter-frame forgery detection for MPEG-1, 2, 4 and H.264/AVC encoded videos. **Methods/Statistical Analysis**: Double compression detection techniques are classified here on the basis of footprints analyzed during detection. The detection methods designed for videos that use fixed GOP structure for first and any of the subsequent compression are different from the videos that use different GOP structure. Video inter-frame forgery detection techniques are then analyzed on the basis of type of forgery they detect and the type of codec used for video encoding. **Findings:** Digital videos often provide forensic evidence in legal, medical and surveillance applications but are more prone to inter-frame forgeries, which are not only easy to perform but are equally difficult to detect as well. The analysis of the literature ascertained that majority of the proposed techniques are dependent on the number of frames tampered and video codec used to encode the videos. Among these proposed techniques, double MPEG compression was best detected using the technique which utilizes Benford's law and was proposed by Chen and Shi on MPEG-1 and MPEG-2 encoded videos. On the other hand, Wang et al. gave sound results for all kinds of inter-frame forgeries on MPEG-2 encoded videos by utilizing the measure of optical flow consistency. Since very few authors focussed on forgery detection in MPEG-4 encoded videos and thereby such techniques have not been discussed in many survey papers. Moreover, digital cameras especially surveillance cameras which generate massive amount of videos these days have built-in MPEG-4 codec because it offers a better compression rate. **Application/Improvements:** Video forensics domain, therefore, is in dire need of a technique that will detect any kind of inter-frame forgery in MPEG-4 encoded videos.

Keywords: Digital Forensics, Inter-frame Forgery, Video Forgery Detection, Video Forgery Detection Survey, Video Tampering Detection

1. Introduction

Video editing techniques were primarily meant for enhancement of the digital content. But the increase in availability and usage of inexpensive and easy-to-use content editing software has escalated the side effects and potential hazards of such editing techniques. Any individual can utilize these techniques to make unauthorized modifications to the video content thereby harming its integrity and authenticity. Although majority of the forgeries are not visually identifiable, they meddle with the underlying characteristics of the digital content under consideration and introduce certain abnormalities. These abnormalities, when statistically analyzed, make it easy to observe the artifacts left by tampering. To ensure the authenticity of digital content, the domain of digital video forensics was conceived. Digital video forensics encompasses tools and techniques which help clarify whether the contents of a given digital video are veritable or not. Video forgeries can generally be classified as inter-frame or intra-frame.

1.1 Intra-frame Forgeries

A digital video is essentially a sequence of still images or frames and intra-frame forgery tends to tamper each frame individually. Intra-frame forgeries can be further classified as:

- Pixel-level Forgeries: Pixel level is the most basic level at which visual contents can be modified using copy-move, splicing and re-sampling techniques[1].

*Author for correspondence

- Object-level Forgeries: These forgeries entail cloning an object or region from one location to another in a single frame and inserting or removing an object to/from a frame[2–5].
- Frame-level Forgeries: These forgeries imply manipulating the whole frame. For instance, upscale-crop forgery is a kind of frame-level forgery where a frame is enlarged and cropped to remove the evidence of a crime occurring on the frame extremities[6].

1.2 Inter-frame Forgeries

These exploit temporal correlation between frames and rely upon the detection of characteristic footprints left by video processing operations. These are classified as:

- Frame Removal[7].
- Frame Insertion[8].
- Frame Replication[9].

Over the years, numerous digital video forgery detection methods have been proposed. Some techniques detect forgeries based on sensor pattern noise[10] while some techniques detect intra-frame forgeries like object insertion or removal in a particular frame. Video inter-frame forgery detection has been an important problem in the past decade. One can easily insert or remove a particular frame or set of frames to tamper the original video content. To illustrate, consider surveillance footage of traffic on a street. From such a video sequence, it would be very easy to remove a passing vehicle by removing a handful of frames. It would also be quite feasible to insert vehicle captured using different camera and/or at different time periods. But detection of such kind of inter-frame forgery is a complicated task because in such cases, human eye can't easily comprehend the difference between an original video and a forged one. Different survey papers[11–13] are available in the domain of video forensics; to the best of author's knowledge, neither they analyze all the available video inter-frame forgery detection technique nor do they address forgery detection in MPEG-4 videos. This paper presents an overview of various video inter-frame forgery detection approaches that have been designed so far. Section 2 presents an overview of active and passive approaches for video forgery detection to provide a foundation for understanding the basics of the video forgery detection domain. Video inter-frame forgery detection is addressed in Section 3 followed by review of the techniques designed to detect inter-frame forgeries. Section 4 concludes the survey and provides future directions to determine new research problems in the field of video inter-frame forgery detection.

2. A Brief Overview of Video Forgery Detection Approaches

Video forgery detection procedures attempt to ascertain whether the given digital content has undergone any unethical post-processing operations. Such operations leave some footprints in the reconstructed signal. Video forgery detection mechanisms analyze these footprints in order to differentiate between original videos and tampered ones. There are two fundamental approaches to video forgery detection:

2.1 Active Approach

The active approach embeds authentication data like watermarks or digital signatures in the video, either at the time of recording or later with the help of some specialized software, so as to enable verification of the origin and authenticity of its contents afterwards. The problem with this approach is that pre-embedding of watermarks or signatures degrades the quality of the video. Moreover, not all camera manufacturers support pre-embedding[14–17].

2.2 Passive Approach

These techniques rely on the intrinsic characteristics of the video content instead of data that provides authentication. These are also known as blind tamper detection techniques and generally work under the assumption that tampering introduces specific static and temporal artifacts in the video content which can be examined in order to detect fallacious videos. This is the most commonly utilized approach in video forensics domain due to its significant advantages over active approach. Categorization of various proposed video forgery detection techniques is shown in Figure 1.

3. Video Inter-frame Forgery Detection

Digital videos take up a lot of space and therefore, to enable effective storage and transmission, these are usually stored in a compressed format. So, in order to perform any type of tampering operation, individual frames

are first extracted and edited with the intention to deceive the user. The reconstruction of the tampered video using the edited frames results in double compression because some amount of compression is inevitable whenever a video is saved. The earliest innovations in the field of video inter-frame forgery detection were based on detection of traces of double compression in video sequences. These techniques are discussed in Section 3.1. However, double compression occurs even if video is transmitted, uploaded, downloaded or even viewed[18]. This means that a video that shows signs of recompression may not necessarily have undergone any inter-frame forgery. So, merely detecting double compression to detect the presence of forgery in video sequence is not considered to be an effective approach for forgery detection. This induces the need to detect the presence of inter-frame forgery artifacts with the help of some other specialized methods that do not rely on recompression artifacts. These are discussed in Section 3.2.

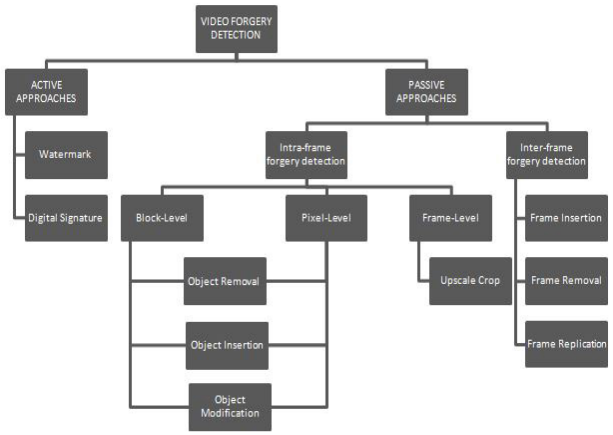

Figure 1. Categorization of video forgery detection techniques.

3.1 Methods for Double Compression Detection

3.1.1 Fixed GOP Based Approaches

3.1.1.1 DCT Coefficient Analysis

Frame based tampering leads to re-shuffling of frames amongst neighbouring GOPs which causes GOP de-synchronization. As a result, DCT coefficient distribution is disturbed. The authors used different approaches[19–21] to study this disruption in the distribution of quantized DCT coefficients; subsequently overcoming the limitation of the previous approaches. Wang and Farid first proposed a method[19] to detect double MPEG compression in video sequences by analyzing periodic pattern in the histogram of DCT coefficients of I-frames and motion error of P-frames. They did not provide any quantitative analysis of the performance of their approach but claimed that their method worked well if number of frames deleted or inserted was a multiple of 3. Furthermore, the technique's performance dropped if an entire GOP or multiples of GOP were deleted. Thorough analysis of this approach revealed that it also failed to detect forgery at macro-block level where different quantization scales were used during the first and second compression. The same authors proposed another technique to detect double quantization by extending their former work[19] to macro-block level[20]. This technique detected doubly compressed videos which were either manually compressed or were the consequence of composition of two videos of different qualities, i.e. green screening. The authors here utilized the Gaussian distribution for doubly compressed DCT coefficients to detect double compression in every frame macro-block as small as 16 x 16 pixels. They used different quantization scales (in the range 1-31) for the first and second compression; the technique's detection accuracy varied accordingly with an average of 47.7%. The author in[21] analyzed convex pattern in the histogram of double quantized DCT coefficients of each macro-block rather than detecting peak and periodicity. A detection function was defined using empirically selected threshold of 0.1. After thorough analysis of the proposed technique, it was realized that selection of new thresholds for every new video dataset incurred a large computational overhead. The authors tested the technique on 100 video sequences using bit-rates in the range 4 Mbps-8 Mbps with an average True Positive Rate (TPR) of 93.4%.

3.1.1.2 Usage of Benford's Law

The author in[22] found that the disturbance in DCT coefficients due to double compression also violated the parametric logarithmic law for first digit distribution of quantized AC coefficients. For each GOP, a 36-D feature vector was computed using first digit probabilities of non-zero MPEG quantized AC coefficients and three goodness-to-fit statistics. SVM classifier was adopted to test the approach using different quantization scales in Variable Bit Rate (VBR) encoded videos and using different bit rates in Constant Bit Rate (CBR) encoded videos on three groups having 10 videos in each. Group 1 and

Group 2 contained CBR encoded videos and Group 3 contained VBR encoded videos. Average detection rate for this approach was found to be 96.9%. The methodology proposed in[23] utilized the same features as in[22] and developed a new approach where instead of a 36-D feature, a 12-D feature vector was computed by considering the I-frames only. Experiments were performed on 12 video sequences considering bit-rates in the range 0.5 to 1.5 Mbps. The technique failed to generate accurate results when the target bit rate was smaller than the original bit rate of the given video. It extended their previous work of double JPEG compression detection[24] to videos. They generated a 63-D feature vector using first digit statistics. Videos violating Benford's law were further classified by applying a set of binary SVM classifier on the basis of k-means clustering. The technique detected up to three compressions with accuracy higher than 73% in H.264/AVC encoded video sequences.

3.1.1.3 Detection Approach using Markov Statistics

A Markov statistics based double compression detection method for MPEG-4 videos was proposed in[25], where the authors assumed a fixed GOP pattern IPPPPP. The concept of JPEG recompression detection scheme used in[26] was applied to intra-coded frames of MPEG-4 video blocks. By extracting Markov features from an object based representation model of the given video and an empirically calculated threshold, final classification resulted in an average detection rate of 96.72%. Comparative analysis of Markov statistics with first digit distribution demonstrated that Markov features performed better when quantization scales for second compression were an even multiple of the first quantization scale.

3.1.2 Variable GOP based Approaches

All the techniques mentioned so far assumed a fixed GOP structure for the first and second compression and as a result, did not work in scenarios where different GOP structures were used during the initial and any of the subsequent compressions. To overcome this limitation, the authors in[27–29] proposed techniques where the GOP structures were assumed to vary with every compression.

3.1.2.1 Detection using Block Artifact Strength (BAS)

Compression introduces different block artifacts into video frames and recompression further disturbs the average of these artifacts; BAS score was used to quantify this variation. BAS depends on the number of deleted frames and type of GOP used in first and second compression. Along with the detection of videos re-encoded using different GOP structure, this approach also detected frame removal if number of deleted frames were not multiple of 3.

3.1.2.2 Detection using Variation of Prediction Footprint (VPF)

The author in[28] proposed a technique utilizing the feature called VPF which was based on the variation in number of I and S macro-blocks in re-encoded P-frames which were I-frames in first encoding. This method also estimated the size of GOP used during first compression. Experiments were performed on videos encoded using three different encoders (MPEG-2, MPEG-4, H.264) generating an average detection rate of 87%. Each encoding was performed by specifying four different constant bit rates (100, 300, 500, 700 kbps). This method gave best results for short videos having uniform regions and for H.264 encoded videos re-encoded at high bit rates.

3.1.2.3 Detection using both BAS and VPF

With MPEG-4 compression, discontinuity exists in 8 × 8 block boundaries as quantization and transform coding is different for each block. Instead of analysing variation in the number of macroblocks, VPF was measured by analyzing the variation in the block artifact strength. Average detection accuracy of this approach was found to be 92.46% after testing using bit rates of 100, 300, 500 and 700 kbps. All these techniques are summarized in Table 1 and after thorough analysis of these techniques, it can be concluded that Chen and Shi[22] provided better accuracy for double compression detection in MPEG-1 and MPEG-2 videos recorded using both CBR and VBR modes. However, most of the techniques were not tested on MPEG-4 videos. On the other hand, The author in[29] detected double compression in MPEG-4 videos recorded in CBR mode with substantial accuracy, but this accuracy was dependent on the target bit rates of the final forged videos.

3.2 Specialized Techniques for Inter-frame Forgery Detection

3.2.1 Frame Insertion Detection

In[8] found that inter frame forgery disturbs the consistency ratio of Block-wise Brightness Variance Descriptor (BBVD) because of decrease in correlation between adja-

Table 1. Double compression detection approaches (q: ratio of first and second quantization scale values; A: Accuracy; TPR: True Positive Rate; TNR: True Negative Rate)

Algorithm (Ref)	Methodology	Database	Results	Remarks
(19)	Periodicity analysis of static and temporal artifacts	Two MPEG-1 encoded videos	Quantitative results not reported	Works for VBR videos. Inaccurate for whole GOP deletion. Accurate for sub-GOP deletion. Failed at macro-block level.
(20)	Gaussian distribution for quantized DCT coefficients on I- frames	3 MPEG-2 encoded videos	q<1.3, A: 2.5% 1.3 <q <1.7,A: 41.2% q>1.7, A: 99.4%	Effective for good quality videos. Accuracy depends on quantization values.
(21)	Analyze convex pattern in histogram of quantized DCT coefficients	100 MPEG-2 encoded videos	TPR: 98-100% (at 8 Mbps, max) TNR: 93% (at 8 Mbps, min)	Inaccurate for slow motion videos. Accuracy depends on output bit-rate. Empirical thresholds.
(22)	Analyze Benford's law violation SVM classification using 36-D feature vector for I,P and B-frames	Group-1**::** MPEG-2 videos Group-2:: MPEG-1videos Group-3:: MPEG-1videos	Group-1:: A: 95.8% Group-2:: A: 95.8% Group-3:: A: 99.3%	Inaccurate for videos having low re-encoding quality. Inaccurate for slow motion videos. Empirical thresholds. Works for both CBR and VBR videos.
(23)	Analyze Benford's law violation SVM classification using 12-D features for I frames	12 MPEG-2 encoded CBR video clips	TNR : 97.92% TPR : 100%	Inaccurate if target bit rate is smaller.
(18)	Analyze Benford's law violation SVM classification using 63-D feature	12 videos	A: >73%	Accuracy decreases as number of compression stages increase.
(25)	Use Markov statistics	30 MPEG-4 encoded YUV videos ; 5040 video clips	A: 90%	Detection performance degrades if second quantization scale is an odd multiple of first one. Empirical thresholds. Works for VBR videos only.
(27)	Analyze block artifact strength	MPEG-2 encoded videos	Only qualitative analysis using Feature curve	Inaccurate for sub-GOP deletion. Applicable to VBR videos only. Detects GOP conversion also.
(28)	Variation in Prediction Footprint using variation in number of macro-blocks	14 Video sequences	Re-encoding using -- H.264:: A: 94%(best) MPEG-x:: A: 80%	Accuracy declines for low quality of second compression. Best for H.264 encoded videos.
(29)	Variation in prediction footprint using block artifact strength	14 MPEG-4 encoded videos	A: 95% (for high target bit rate)	Works for CBR videos. Accuracy depends on bit rates.

cent frames. Most importantly, sub-sequence analysis instead of adjacent frame analysis increased the speed of forgery detection. Adaptive threshold selected using 3σ rule was compared with BBVD ratio of each sub-sequence which generated two peak points at location of frame insertion. This approach detected frame insertion and localized it with an average accuracy of 96.38% and 89.23% respectively.

3.2.2 Frame Removal Detection

A technique was proposed for detecting frame deletion in MPEG-2 coded videos in[7] based on[30] which utilized prediction error on VBR coded videos. The proposed technique used eight features which were based on prediction error energy, percentage of intra-coded macro-blocks, quantization scale values and estimated PSNR values. Results were analyzed using three types of classifiers (KNN, SVM and logistic regression) on 4 sets of MPEG-2 video sequences. This approach achieved average accuracy of 94.2%. Furthermore, The author in[31] determined the exact location of frame deletion by analyzing spikes in the fluctuation histogram of motion residual. Enhanced Fluctuation Feature (EFF) was measured for a range of frames selected in a window of variable sizes. The forged frames were classified using an adaptive threshold. General threshold of 1.2 and window size of 3 provided effective determination of deletion point with a TPR of 90%. In the meantime, The author in[32] put forward a new feature named Sequence of Average Residual of P-frames (SARP) and analyzed it in time and frequency domain like in[27,19] respectively. Periodicity of SARP of a video was analyzed in time domain and its spikes were detected in frequency domain using discrete time Fourier transform. This approach was tested on 240 videos and an average accuracy of 92.08% was obtained.

3.2.3 Frame Replication Detection

Frame duplication and region duplication were detected in[9] digital videos based on temporal correlation between all frame pairs in a subsequence and spatial correlation between all block pairs in a frame. Frame duplication was detected by comparing correlation coefficients of a video subsequence with an empirically selected threshold with an average accuracy of 90.48%. Region duplication was detected by analyzing peaks in the inverse Fourier transform of power spectrum of two frames with an average accuracy of 72.63%.

3.2.4 Frame Insertion/Removal Detection

The author in[33] proposed a technique to detect frame based video tampering by analyzing spikes in the FFT spectrum of Motion Compensated Edge Artifact (MCEA) difference between adjacent P-frames. This approach eliminated the need for hard threshold factor used in[34] and calculated MCEA as the difference of DCT energies. Moreover, they also estimated the original GOP structure of video. This approach was tested on 4 MPEG-2 video sequences, two of which demonstrated simple motion and the remaining two contained complex motion. Thorough analysis of the technique's functionality revealed that it did not investigate the influence of B-frames and required at least three P-frames in a single GOP. Meanwhile, in[35] utilized optical flow consistency measure to detect frame insertion and removal. Optical flow is basically the measure of movement in brightness patterns of individual frames in a video, which shows the continuity of frames. They utilized window-based analysis for frame insertion detection and adjacent frame-pair analysis for frame deletion detection. This model achieved precision of 98% for frame insertion and 89% for frame deletion and proved to be effective for detection of insertion or removal of a large number of frames only. The author in[36] utilized an approach similar to[35]. They classified original and forged videos by training an SVM classifier where optical flow consistency was used as discriminating feature. Any forgery, if present, was also differentiated as being either frame-insertion or frame-removal. Thorough experimentation was performed on 598 videos classifying original and forged videos with an average accuracy of 96.75%.

3.1.5 Frame Insertion/Removal/Replication Detection

Another optical flow based approach was proposed in[37] where the authors detected statistical anomalies and discontinuity points in optical flow with the help of a Gaussian model. It was found that while frame deletion introduced single discontinuity point, frame insertion and duplication introduced two discontinuity points in the optical flow, which were located with the help of Grubb's test. The proposed approach generated an average classification accuracy of 90%. A significant limitation of this approach was the use of empirical thresholds. Thorough analysis of these techniques summarized in Table 2 led to the conclusion that proposed techniques did not focus much on inter-frame forgery detection in H.264 videos.

Table 2. Inter-frame forgery detection approaches (P: Precision)

Algorithm (Ref)	Methodology	Database	Results	Remarks
(8)	Analyze block wise brightness variance descriptor	240 videos from KTH database	Frame insertion detection: P: 94.09%, A: 98.67% Forgery localization: P: 79.45%, A: 89.23%	Small dataset. Fast detection (suitable for real time applications). Accuracy drops down with fewer frames insertion.
(7)	Prediction error energy of non-I macro-blocks in each P frame percentage of I-macro-blocks Quantization scale values Estimated PSNR values	4 sets; 36 MPEG-2 coded videos in each	Fixed GOP length: CBR: SVM 94.3, KNN 95.6, LR 94.8 VBR: SVM 94.3, KNN 95.6, LR 94.8 Variable length GOP: CBR: SVM 94.0, KNN 92.9, LR 94.0 VBR: SVM 95.4, KNN 91.5, LR 93.2	Not accurate for deletion of whole GOP. Applicable to both VBR and CBR. Distinguish between recompressed videos with or without frame deletion.
(31)	Enhanced fluctuation feature	130 YUV videos:: 30:downloaded from Traces 100: manually recorded	TPR: 90% (maximum)	Effective for videos compressed using different encoders exhibiting simple and complex motion. Detects multiple GOP deletion.
(32)	Sequence of average residual of P frames	240 H.264 Videos	A: 92.08% TPR: 91.82% FPR: 5%	Works well for slow motion sequences. Hard threshold.
(9)	Frame duplication: Temporal and spatial correlation Region duplication: Peaks in Fourier transform of power spectrum	2 MPEG videos	Average accuracy:: Frame duplication: A: 85.7% (static camera) A: 95.2% (handheld) Region(256 × 256) duplication: A: 66.62% (static camera) A: 78.65%(handheld)	Small dataset. Empirical thresholds. Accuracy depends on output bit-rates and region size.
(33)	Motion compensated edge artifact	4 MPEG-2 videos	Quantitative results not reported	Small database. Effective for multiple of sub-GOP deletion.
(35)	Optical flow consistency measure	KTH database	Average recall Rate : 90% Average precision Rate: 93.5%	Fast operation. Less accurate for fewer number of frames tampered.

(36)	Optical flow consistency measure	5 video databases (598 videos)	Original and forged videos classification: 96.75% Insertion/Removal: 96%	Works for videos with static background. Effective classification of forgery.
(37)	Gaussian model based statistical anomaly detection technique from optical flow	Surveillance videos (MPEG-2) from TRECVID	Average Classification accuracy: 90% Average Localization accuracy:: Insertion: 100% Removal: 96.9% Duplication: 86.2%	. Complex but limited Dataset. Unified approach.

Although Liu et al.[29] utilized H.264 encoded videos for frame removal detection; their technique was extremely dependent on empirical selection of hard thresholds. Furthermore Wang et al.[34] detected all kinds of frame tampering with sound accuracy but this classification were performed only on very limited dataset of MPEG-2 encoded videos.

4. Discussion and Conclusion

The tremendous increase in the use of mobile phones, digital cameras and surveillance cameras has elevated the importance of digital videos in today's world. Visual content of digital videos serves as evidence in various legal, medical and political matters. However, great advancement in multimedia technology has made video editing software highly accessible to any individual, which has further increased the probability of tampering. Although numerous video forgery detection techniques have been proposed in the literature, they all suffer from their share of limitations. Surveillance footage usually provides significant evidence in the court of law but is more prone to inter-frame forgeries. Inter-frame forgery is not only very easy to perform but is equally difficult to detect as well. This makes inter-frame forgery detection a crucial branch of digital video forensics. This paper analyzed the various inter frame forgery detection approaches proposed so far, all the while highlighting the strengths and weaknesses of each technique discussed. A major shortcoming of many methodologies was that their detection accuracy depended on the number of frames deleted or inserted in a video sequence. Performance of majority of the techniques was found to be dependent on the compression scales used in first and second compression. Some authors focussed on forgery detection in MPEG-4 encoded videos and the usage of this encoding standard is continuously increasing. Even the surveillance cameras these days have in built-in MPEG-4 encoder. Detection of forgery in MPEG-4 videos is, therefore, of great significance. Moreover, most of the existing methods assume similar GOP for every video, which caused unreliable performance. Another important limitation of the exiting methods was lack of sufficient validation on standardized video databases. The authors usually tested their techniques on self-recorded videos, thereby making it difficult to perform effective comparative analysis among existing techniques. Further studies are required to analyze the effect of noise and acoustics on detection accuracy. There is an absolute necessity to develop more effective methods that are capable of providing a clear distinction between normal content enhancement operations and malicious manipulations in digital videos.

5. References

1. Kobayashi M, Okabe T, Sato Y. Detecting video forgeries based on noise characteristics. Springer Berlin Heidelberg; 2009 Jan. p. 306–17.
2. Lin CS, Tsay JJ. A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. Digital Investigation. 2014 Jun; 11(2):120–40.
3. Su L, Huang T, Yang J. A video forgery detection algorithm based on compressive sensing. Multimedia Tools and Applications. 2015 Sep; 74(17):6641–56.
4. Video forgery detection using HOG features and compression properties. 2012. Available from: http://ieeexplore.ieee.org/document/6343421/
5. Video forgery detection using correlation of noise residue. 2008. Available from: http://ieeexplore.ieee.org/document/4665069/
6. Hyun DK, Ryu SJ, Lee HY, Lee HK. Detection of upscale-crop and partial manipulation in surveillance video based on sensor pattern noise. Sensors. 2013 Sep; 13(9):12605–31.

7. Shanableh T. Detection of frame deletion for digital video forensics. Digital Investigation. 2013 Dec; 10(4):350–60.
8. Zheng L, Sun T, Shi YQ. Inter-frame video forgery detection based on block-wise brightness variance descriptor. Springer International Publishing; 2014 Oct. p. 18–30.
9. Wang W, Farid H. Exposing digital forgeries in video by detecting duplication. Proceedings of the 9th Workshop on Multimedia and Security; 2007 Sep. p. 35–42.
10. Lin GS, Chang JF, Chuang CH. Detecting frame duplication based on spatial and temporal analyses. International Journal of Pattern Recognition and Artificial Intelligence. 2012 Nov; 26(7):1–18.
11. An overview on video forensics. 2012. Available from: http://ieeexplore.ieee.org/document/6334348/
12. Pathak A, Patil D. Review of techniques for detecting video forgeries. International Journal of Computer Science and Mobile Computing. 2014 Feb; 3(2):438–42.
13. Sowmya KN, Chennamma HR. A survey on video forgery detection. International Journal of Computer Engineering and Applications. 2015 Feb; 9(2):17–27.
14. Fallahpour M, Shirmohammadi S, Semsarzadeh M, Zhao J. Tampering detection in compressed digital video using watermarking. IEEE Transactions on Instrumentation and Measurement. 2014 May; 63(5):1057–72.
15. Mobasseri BG, Sieffert MJ, Simard RJ. Content authentication and tamper detection in digital video. Proceedings of IEEE International Conference on Image Processing. 2000 Feb; 1:458–61.
16. Arab F, Abdullah SM, Hashim SZ, Manaf AA, Zamani M. A robust video watermarking technique for the tamper detection of surveillance systems. Multimedia Tools and Applications. 2016 Sep; 75(18):10855–85.
17. A robust content based digital signature for image authentication. 1996. Available from: http://ieeexplore.ieee.org/document/560425/
18. Multiple compression detection for video sequences. 2012. Available from: https://pdfs.semanticscholar.org/276f/9625e1b4ca4d7a38e344e698901b3a9e9dc3.pdf
19. Wang W, Farid H. Exposing digital forgeries in video by detecting double MPEG compression. Proceedings of the 8th ACM Workshop on Multimedia and Security; 2006 Sep. p. 37–47.
20. Wang W, Farid H. Exposing digital forgeries in video by detecting double quantization. Proceedings of the 11th ACM Workshop on Multimedia and Security; 2009 Sep. p. 39–48.
21. Detection of double-compression in MPEG-2 videos. 2010. Available from: http://ieeexplore.ieee.org/document/5473474/
22. Chen W, Shi YQ. Detection of double MPEG compression based on first digit statistics. Springer Berlin Heidelberg; 2008 Nov. p. 16–30.
23. Exposing video forgeries by detecting MPEG double compression. 2012. Available from: http://ieeexplore.ieee.org/document/6288150/
24. Milani S, Tagliasacchi M, Tubaro S. Discriminating multiple JPEG compressions using first digit features. APSIPA Transactions on Signal and Information Processing. 2014; 3:1–10.
25. Jiang X, Wang W, Sun T, Shi YQ, Wang S. Detection of double compression in MPEG-4 videos based on Markov statistics. Signal Processing Letters. IEEE. 2013 May; 20(5):447–50.
26. A machine learning based scheme for double JPEG compression detection. 2008. Available from: http://ieeexplore.ieee.org/document/4761645/
27. MPEG recompression detection based on block artifacts. 2008. Available from: http://spie.org/Publications/Proceedings/Paper/10.1117/12.767112
28. Detection of video double encoding with GOP size estimation. 2012. Available from: http://ieeexplore.ieee.org/document/6412641/
29. He P, Sun T, Jiang X, Wang S. Double compression detection in MPEG-4 videos based on block artifact measurement with variation of prediction footprint. Springer International Publishing; 2015 Aug. p. 787–93.
30. Stamm MC, Lin WS, Liu KJ. Temporal forensics and anti-forensics for motion compensated video. IEEE Transactions on Information Forensics and Security. 2012 Aug; 7(4):1315–29.
31. Feng C, Xu Z, Zhang W, Xu Y. Automatic location of frame deletion point for digital video forensics. Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security; 2014 Jun. p. 171–9.
32. Liu H, Li S, Bian S. Detecting frame deletion in H 264 video. Springer International Publishing; 2014 May. p. 262–70.
33. Dong Q, Yang G, Zhu N. A MCEA based passive forensics scheme for detecting frame-based video tampering. Digital Investigation. 2012 Nov; 9(2):151–9.
34. Exposing digital video forgery by detecting motion-compensated edge artifact. 2009. Available from: http://ieeexplore.ieee.org/document/5366884/
35. Chao J, Jiang X, Sun T. A novel video inter-frame forgery model detection scheme based on optical flow consistency. Springer Berlin Heidelberg; 2012 Nov. p. 267–81.
36. Wang W, Jiang X, Wang S, Wan M, Sun T. Identifying video forgery process using optical flow. Springer Berlin Heidelberg; 2013 Oct. p. 244–57.
37. Wang Q, Li Z, Zhang Z, Ma Q. Video inter-frame forgery identification based on optical flow consistency. Sensors and Transducers. 2014 Mar; 166(3):229–34.