International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 2, April 2017, pp. 831~841
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i2.pp831-841

Video Inter-frame Forgery Detection Approach for Surveillance and Mobile Recorded Videos

Staffy Kingra, Naveen Aggarwal, Raahat Devender Singh
University Institute of Engineering and Technology Panjab University, Chandigarh, India

Article Info

Article history:

Received Dec 8, 2016
Revised Feb 10, 2017
Accepted Feb 26, 2017

Keyword:

Inter-frame forgery detection
Optical flow
Prediction residual
Video forgery detection
Video tampering detection

ABSTRACT

We are living in an age where use of multimedia technologies like digital recorders and mobile phones is increasing rapidly. On the other hand, digital content manipulating softwares are also increasing making it easy for an individual to doctor the recorded content with trivial consumption of time and wealth. Digital multimedia forensics is gaining utmost importance to restrict unethical use of such easily available tampering techniques. These days, it is common for people to record videos using their smart phones. We have also witnessed a sudden growth in the use of surveillance cameras, which we see inhabiting almost every public location. Videos recorded using these devices usually contains crucial evidence of some event occurence and thereby most susceptible to inter-frame forgery which can be easily performed by insertion/removal/replication of frame(s). The proposed forensic technique enabled detection of inter-frame forgery in H.264 and MPEG-2 encoded videos especially mobile recorded and surveillance videos. This novel method introduced objectivity for automatic detection and localization of tampering by utilizing prediction residual gradient and optical flow gradient. Experimental results showed that this technique can detect tampering, regardless of the video codec and recording device utilized and number of frames tampered.

Corresponding Author:

Staffy Kingra
University Institute of Engineering and Technology Panjab University,
Chandigarh, India.
Email: staffysk@gmail.com

1. INTRODUCTION

In this technology oriented world, digital video recorders especially surveillance cameras are commonly available at every place which generates massive amount of multimedia content. Moreover, technology enthusiasm among young generation has increased the usage of mobile phones causing increase in the availability of captured digital content [1]. Digital videos often provide significant forensic evidence in various medical, legal and surveillance applications which make such applications extremely dependant on the credibility of visual content portrayed in these videos. The substantial usage of digital videos in our day-to-day lives has also led to an increase in the utilization of easy to use and inexpensive video editing software which enhance the visual contents of digital videos. However, an individual can easily utilize such content editing software to make unauthorized modifications, termed as forgery, to the digital content making it extremely difficult to place complete trust in the integrity of such digital content [2]. To make ethical utilization of recorded digital videos in crucial matters, it becomes essential to ascertain that the visual contents of a video under consideration have not undergone any post-production manipulation and are a reliable depiction of reality.

Although lot of techniques have been proposed in the literature to detect forgery in images [3], numerous video tampering detection techniques have also been proposed. These techniques fall into one of the two basic categories of forensic schemes: active schemes and passive schemes. Active forensic scheme

maintain the authenticity of digital media throughout the entirety of their usage by embedding watermark or digital signature in the video [4], [5]. But this pre-embedding generally degrades the quality of digital content and also requires special hardware for engrafting watermark or digital signature. To overcome this issue, the field of passive forensics was conceptualized. Passive forensic schemes analyze specific static and/or temporal artifacts which arise due to the meddling of tampering operations with the underlying characteristics of digital content. Such approaches are utilized to detect any unauthorized manipulation performed either at intra-frame level or at inter-frame level. Forgery performed at intra-frame level manipulates a frame at pixel level, object level [6], [7] or at entire frame level [8]. On the other hand, Inter-frame tampering can be performed by mere removal [9], insertion [10] and/or replication [11] of a frame or set of frames to/from a video.

Video inter-frame forgery is very easy to perform but it is very difficult for a human eye to detect the presence of such forgeries without the help of any specialized technique. Surveillance and mobile recorded videos are easily generated and are very prone to such forgeries as one can easily counterfeit the absence or presence of certain objects in the footage by simply removing or inserting suitable frames from/to the respective footage. This reconstructed video is then used as a fallacious proof of evidence. With increase in the probability of such malicious operations, the techniques to detect these tampered videos also require significant improvements.

Numerous approaches have been proposed in the literature to detect the presence of inter-frame forgery in the video sequence. Such forgeries are usually performed by first converting the video into a sequence of frames followed by deletion/insertion/replication of some frames and finally reencoding the video. As some amount of compression is inevitable whenever a video is saved, the reconstruction of a doctored video after manipulation always results in double compression. So, some of the authors in the literature utilized the analysis of double MPEG compression to ensure the existence of inter-frame forgery. The prominent technique in this context was proposed by Wang and Farid in [15] where the authors analyzed periodicity in DCT coefficients of I-frames and prediction error of P-frames. However, they did not provide any quantitative results. Some researchers examined Benford's law violation in quantized DCT coefficients by utilizing 36-D, 12-D and 63-D feature vector in [16-18] respectively. Double compression in MPEG-4 encoded videos was firstly detected in [19] by utilizing Markov Statistics, which was dependent on quantization scale values of reconstructed video. Other techniques for double compression detection were proposed by authors in [20-22] based on Block Artifact Strength (BAS), Variation in Prediction Footprint (VPF) and their combination respectively.

The authors in [18], however, stated the fact that not every video that shows signs of recompression has been tampered with inter-frame forgery because double compression can occur after uploading, downloading or even transmitting a video. This fact induced the need to detect the presence of some other artifacts that could ensure the presence of inter-frame forgery. Frame insertion detection technique proposed in [10] utilized a feature called Block-wise Brightness Variance Descriptor (BBVD). Different frame removal detection techniques have been proposed in [9], [23], [12]. The technique proposed in [9] used multiple features which were based on prediction error energy and number of intra-coded macro-blocks, quantization scale and Peak Signal-to-Noise Ratio values. Likewise, the authors in [23] and [12] utilized Enhanced Fluctuation Feature (EFF) and Sequence of Average Residual of P-frames (SARP) respectively for frame removal detection with sound accuracy. One of the frame removal detection technique proposed in [24] utilized the measure of brightness variance. Another type of frame based tampering named frame replication was detected by analyzing disturbance in the temporal correlation of all adjacent frame pairs [11]. Moreover, Motion Compensated Edge Artifact (MCEA) difference [25] and prediction residual error [14] between adjacent P-frames are significant clues to detect both frame insertion and removal of set of frames. Technique proposed in [26], [27] analyzed the autocorrelation of VPF pattern and utilized the measure of optical flow consistency among adjacent frames respectively. However, the author in [13] efficiently detected all kinds of frame tampering using optical flow consistency measure but validated on limited dataset of MPEG-2 encoded videos. Most of these techniques utilized subjective analysis of the artifacts left after tampering operation which requires human-computer interaction. Some of these techniques were affected by the number of frames tampered and bit-rates of the video. Moreover, most of the techniques were developed for forgery detection in MPEG-2 encoded video sequences but since, emerging digital recorders utilize H.264 codec. There is a need to develop effective technique that can detect any type of inter-frame forgery in H.264 encoded videos.

To overcome the shortcomings of techniques proposed so far, a unique hybrid detection model has been developed based on the analysis of Prediction Residual Gradient (PRG) [14] and optical Flow Gradient (OFG) [13] to effectively analyze the temporal consistency between successive frames of the video sequence. Prediction residual measures the variation in the object location whereas optical flow computes brightness variation among adjacent frames. Prediction residual artifacts are generally caused by reencoding of frames

from one GOP to another and have previously been utilized by the authors in [14], [15], [25], [26]. All these approaches detected forgeries by analyzing the abnormalities in prediction residual patterns in a different manner. The proposed approach introduced objectivity in the analysis of tampering artifacts by measuring the degree of variation from prediction residual of two adjacent frames to prediction residual of next consecutive pair of adjacent frames. In videos that exhibit very large motion, the prediction residual gradient computed between adjacent frame pairs can be very high, which can in turn causes PRG based schemes to generate false alarms. To overcome this limitation, the proposed technique utilizes two different features PRG and OFG to enable forgery detection in all kind of video sequences. The techniques proposed in [13], [27], [28] measured the movement in brightness pattern of individual frames and estimated Lucas-Kanade optical flow between adjacent frames. The discontinuity in the consistency of measured brightness pattern ensures the existence of tampering. Our approach utilized Horn-Schunck optical flow method which is discussed in Section 2.The main contributions of the proposed technique are described below.

1.1. Contribution of the proposed technique

a. An automatic detection and localization model has been developed that can detect and localize inter-frame forgeries with an average accuracy of 89% and 81% respectively.
b. A hybrid technique has been proposed which utilizes both the motion and brightness gradient features to measure variation among adjacent frames.
c. Since subjective analysis of forensic artifacts could induce the possibility of contradiction. The proposed technique analyzed these artifacts in an objective manner.
d. The performance of the proposed technique is independent of the number and location of the tampered frames. Moreover, we have demonstrated the efficacy of the technique on videos recorded using different devices, different bit-rates and compression standards.

2. PROPOSED APPROACH

The forgery detection scheme proposed in this paper relies on the fact that prediction residual and optical flow of consecutive P frames varies greatly at the location where inter-frame tampering has been performed. Figure 1 illustrates the functionality of the proposed model. As demonstrated in this figure, desired features (PRG and OFG) are computed first after extraction of I and P frames from the video sequence. These computed features are then compared with thresholds to generate spikes for larger magnitudes of PRG and OFG features. Further, check is performed on the count and continuity in these spikes to distinct original and forged videos. The method of computing selected features and procedure of detecting forgery by comparing these selected features with threshold using Algorithms 1 and 2 are discussed further. If continuity check provides negative results in Algorithm 1, then concerned video sequence is retested using Algorithm 2. If the video generates discontinuous spikes, then that indicates that the video is authentic. Continuous spikes, however, indicate the detection of forgery.

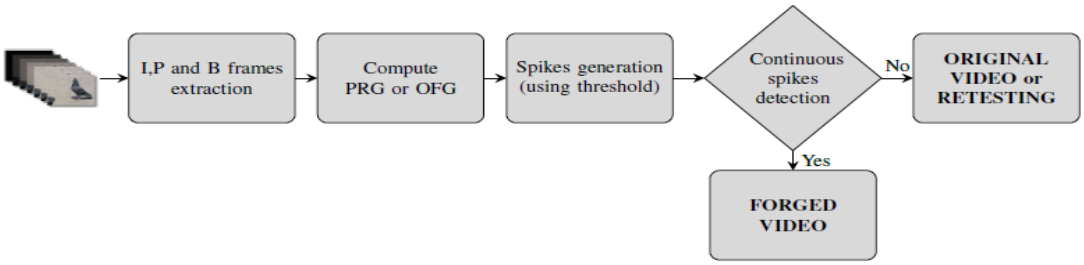


Figure 1. Proposed Video Forgery Detection Model

2.1. Feature Selection

2.1.1. Prediction Residual Gradient

The concept of prediction residual plays a very important role in the domain of video forgery detection. It has been extensively used in many areas like motion estimation and object tracking. Prediction residual is the difference between original frame and the next frame predicted from the original frame and it provides an idea of variation amongst adjacent frames. To predict the next frame, a standard block-matching algorithm is typically employed which utilizes the information of neighboring blocks from the reference

frame. The prediction residual is then obtained by calculating mean square error difference of each pixel in the block of size 16 ×16 with its motion shifted counterpart in the reference frame as given below.

$$pr(i) = f(i+1) - BM(f(i)) \quad (1)$$

$$prg_i = pr_{i+1} - pr_i \quad (2)$$

In Equation (1), $f(i)$ denotes reference frame and $BM(.)$ is considered as the block matcher function which predicts next frame by taking previous P or I frame as reference frame. $BM(f(i))$ computes the predicted version of frame $f(i+1)$. pr_i, prediction residual of ith frame pair, is then obtained by computing the difference between original $(i+1)_{th}$ frame, $f(i+1)$, and predicted version of $(i+1)_{th}$ frame, $BM(f(i))$. Then, objectivity in the analysis approach is introduced by computing gradients of the magnitudes of prediction residual as shown in Figure 2.

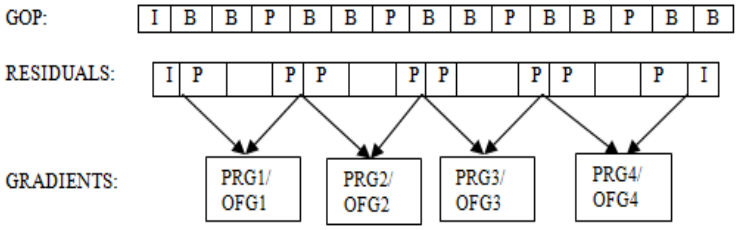


Figure 2. Computation of Gradients

Since GOP pattern for most of the videos sequences utilized in this dataset has been computed using ffmpeg[1] and was determined to be IBBPBBPBBPBBPBB. Since this technique computes gradient between prediction errors of consecutive P frames or consecutive I frame and P frame which are at a distance of 3 from each other, an n-length video sequence generates nearly $\frac{n}{3}$ gradients. This value will be utilized in the localization procedure discussed in Section 2.3.

2.1.2. Optical Flow Gradient

The measure of movement in brightness patterns among the neighboring frames is represented by the optical flow. It is used in many areas like video forgery detection, object detection and tracking, action recognition, video compression and motion estimation. Horn-Schunck algorithm [29] of optical flow is employed here to estimate the brightness variation from one P frame to another. This is a global method which introduces smoothness constraint on brightness variations at each pixel and causes smooth variation of brightness pattern everywhere in the frame which minimizes distortions caused due to unnecessary motion. By adjusting the smoothness factor, it can become adaptable to both slow and fast motion videos. Large positive scalar value of smoothness factor is used for videos exhibiting large motion and vice-versa. For the proposed technique, most suitable value of smoothness factor was empirically determined to be 10.

Let us assume EHS(x, y, t) to be the frame brightness of a pixel (x, y) at time t. However, any movement in pattern never changes the brightness of particular point in the pattern and thereby brightness at a point always remains constant. Therefore,

$$\frac{\delta E}{\delta x}\frac{dx}{dt} + \frac{\delta E}{\delta y}\frac{dy}{dt} + \frac{\delta E}{\delta t} = 0 \quad (3)$$

Equation 3 represents the constraint on local flow velocity. Horn Schunck method introduced brightness constraint along with velocity constraint which is expressed by minimizing the square of magnitude of optical flow velocities as $(|(|\Delta u|)|^2 + |(|\Delta v|)|^2$ where u and v denotes $\frac{dx}{dt}$ and $\frac{dy}{dt}$ respectively. Smoothness control factor is represented by α. Optical flow originated by Horn Schunck is hence represented as

[1]ffmpeg is a standard audio and video convertor, also adopted as a toolbox in MATLAB.

$$of_i = \iint [(I_x u + I_y v + I_t)^2 + \alpha^2((||\Delta u||)^2 + (||\Delta v||)^2)]\, dxdy \quad (4)$$

$$ofg_i = of_{i+1} - of_i \quad (5)$$

Here, I_x, I_y and I_t represent the derivatives of image intensities values along x, y and time dimensions respectively. The optical flow gradient, in Equation 5, is then computed by measuring the variation between optical flows of adjacent pairs.

2.1.3. Influence of Forgery on Selected Features

Each MPEG video exhibit fixed GOP pattern depending on the motion of objects among adjacent frames. Since frames in one particular GOP are highly correlated to each other, videos having large variation among neighboring frames exhibit large number of GOPs of shorter length. However, videos exhibiting smooth variation leads to less number of long length GOPs. Performing any type of inter-frame forgery shuffles the frames amongst neighboring GOPs which causes GOP de-synchronization and decrease in correlation. Due to this decreased correlation, a large variation can be observed in the prediction residual and optical flow of neighboring P frames. Therefore, during experimentation, high gradient value is obtained for large motion video sequences and low for slow ones inducing need of different thresholds for different videos. This need has been overcome by utilizing two features.

To illustrate the effect of forgery on both of these features, six frames (7-12) have been deleted from first GOP as shown by arrows in Figure 3 causing transfer of frames from second GOP to first. Hence, the third and fourth P-frames of first GOP in the reconstructed video represent I-frame and first P-frame of second GOP respectively of the original video. In this way, large variation can be found between second and third P-frame as they both originate from different GOPs. Due to this, magnitude of prediction residual and optical flow also increases.

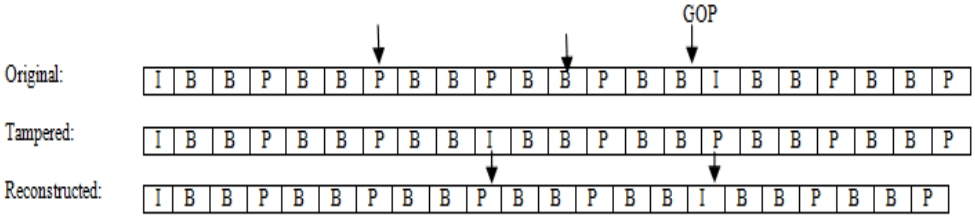


Figure 3. Effect of Tampering (GOP: shows end of first GOP)

2.2. Proposed Methodology

An inter-frame forgery detection model has been presented here that automatically distinguishes original video and a forged one without any user-computer interaction. The procedure for forgery detection adopted in this detection model uses two mechanisms, the first of which utilizes PRG feature given by Algortihm 1. In this method, prediction residual between adjacent P frames is computed first. The loop starting at line 7 then computes the desired feature, PRG, as explained in Section 2.1.1. Lines 11 to 13 compare each obtained PRG with an empirically selected threshold (th_{prg}) to generate spikes at tampered location. Presence of continuous pair of spikes ensures the presence of forgery and their location represents forgery location. The continuity check is provided by the lines 15 to 19.

In case of discontinuous spikes, retesting of the concerned video is done using Algorithm 2, which utilizes OFG feature. This retesting is also done if number of spikes generated is greater than the maximum number of spikes possible. To compute the maximum number of relevant spikes, a window based mechanism is adopted here. A video sequence is partitioned into small sub-sequences of w frames. Some irrelevant spikes may be generated due to regular fluctuation among consecutive frames. This technique is based on the principle that one spike may exist in each window even for non-tampered video. Therefore, for n frames video sequence, presence of at most n/w spikes is possible even in the absence of any tampering operation. Utilizing this approach, window size of 80 was determined empirically. The spikes generated are discontinuous for non-tampered video but a continuous pair must exist in case of doctored video. Moreover, the videos generating more than the expected spikes have been observed to be those exhibiting large motion. Such videos have a high probability of generating irrelevant pair of continuous spikes. OFG value thus computed is then compared with another threshold (th_{ofg}) selected empirically. Distinction between original and forged videos is performed here by analyzing spikes continuity.

After testing thresholds in the range of 0.1 to 20 using the proposed approach on different set of videos, we observed that threshold 1.8 and 2.3 provide effective results to detect forgery in low quality surveillance videos. Threshold value of 2.3 was found effective only for fast motion video sequences. So, PRG threshold of 1.8 was used for slow or moderate motion videos followed by OFG threshold of 0.2 adjusted for large motion video sequences. Instead of analyzing object motion in fast motion videos, changes in the brightness pattern of adjacent frames are computed using optical flow. However, mobile videos require a threshold of 19 for PRG and OFG. Need of different threshold for mobile video is due to the different inter-coding technique utilized by the encoder H.264 (main profile) and different bit rate of approximately 20 Mbps to record the video. On the other hand, surveillance videos are encoded at a bit-rate of around 200 Kbps with H.264 high profile codec. This high variation in the bit-rate makes the use of different thresholds inevitable. This threshold can be set adaptively based on the bit-rates and resolution of the video. However, same threshold can work efficiently for videos recorded using bit-rates in the range of around 10 Mbps.

2.3. Localization of Forgery

An automatic localization of forgery has been done by considering variable length GOP of pattern IBBPBBPBBPBB. As explained previously, this GOP structure has P frames located at a distance of 3 from each other. So, the concerned n-length video sequence exhibits $n/3$ gradients. Generalizing the proposed approach for any GOP pattern, localization procedure is given below.

Algorithm 1 PRG-Test

```
procedure PRGTEST
    seq ← sequenceofIandPframes
    th_prg ← thresholdselectedforPRG − Test
    prg_count ← 0
    spikes ← 0
    compute Prediction Residual (pr)
    for each pr do
        prg_i ← pr_{i+1} − pr_i
        t ← prg_i
        prg_count ← prg_count + 1
        if t > th_prg then
            spikes ← spikes + 1
        end if
    end for
    if spikes < n/w and continuous pair of spikes then
        return FORGED VIDEO
    else
        goto Algorithm 2
    end if
end procedure
```

Algorithm 2 OFG-Test

```
procedure OFGTEST
    seq ← sequenceofIandPframes
    th_ofg ← thresholdselectedforOFG − Test
    ofg_count ← 0
    spikes ← 0
    compute Optical Flow (of)
    for each of do
        ofg_i ← of_{i+1} − of_i
        t ← ofg_i
        ofg_count ← ofg_count + 1
        if t > th_ofg then
            spikes ← spikes + 1
        end if
    end for
    if continuous pair of spikes is/are present then
        return FORGED VIDEO
    else
        return ORIGINAL VIDEO
    end if
end procedure
```

Forgery Localization Steps:

a. Locate the position on x-axis representing PRG or OFG value where two continuous peak points are present, $(loc(i), loc(i+1))$.
b. Multiply $loc(i+1)$ with m, where m is the difference in position of two continuous P frames or consecutive I frame and P frame.
c. This obtained value indicates the exact frame location from where frame insertion/deletion starts or frame duplication ends. Sometimes, it may be possible that the obtained value indicates the forgery location within the range of GOP length. Therefore, exact location of tampering was found within the GOP length range.

Forgery Type Classification:

1. In case of frame deletion, continuous spikes are observed at the start of tampering.
2. In case of frame duplication, forgery is localized at the end of series of duplicated frames.
3. Frame insertion forgery is indicated at two locations by two pairs of continuous spikes.

3. RESULTS AND ANALYSIS

Video sequences generated from smart phones and surveillance cameras installed at public places are highly prone to inter-frame forgery. Hence, our dataset is composed of variety of video sequences categorized in

two groups according to the recording device used. First group contains videos recorded using surveillance cameras embedded in the office of an institution. On the other hand, videos contained in the second group have been recorded manually using mobile phones from different locations. The effect of tampering on these videos has been presented in this section to demonstrate the efficiency and feasibility of the proposed inter-frame forgery detection technique. All experiments have been performed in MATLAB 2014a version in Windows 10 environment.

3.1. Video Dataset

There are not many publically available datasets that contain forged videos for testing video inter-frame forgery detection techniques. Hence, the main dataset experimented in this paper is from the DIC-Panjab University [30] which includes videos from real world surveillance cameras employed in an educational institute and manually recorded mobile phone videos. Each video is further segmented into video clips and each of these clips exhibit 800 to 900 frames. The dataset contain videos exhibiting extremely slow motion, slow motion, large motion and very large motion. Some of these videos represent the scenario of ATM vestibule and some video sequences are utilized to conceal the activity performed by respective people. Figure 4 illustrates some sceanrios of the test videos available in this dataset where first row shows some frames from the surveillance videos of Group 1. The same figure shows frames from manually recorded videos of group 2 in the second row.

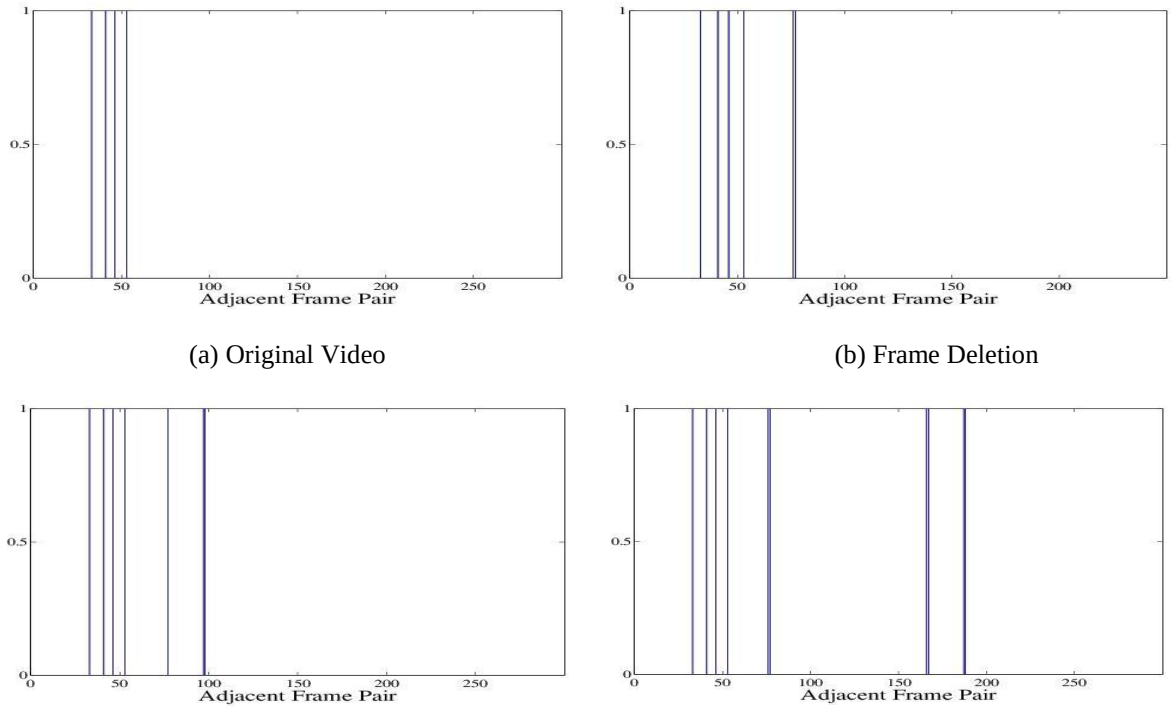
Figure 4. Rows showing some frames from two video sequences (first row: group 1, second row: group 2)

3.2. Experimental layout

a. The dataset of Group 1 has been acquired from the surveillance camera named 'Presto' and 'Hikvision' embedded at institute's office and block entrance respectively. These videos contain both indoor and outdoor scenario, with and without the presence of sunlight.
b. The dataset of Group 2 has been recorded using SONY XPERIA Z2 originally in H.264 main profile format.
c. Video sequences are recorded using bit-rates in the range of 100 Kbps to 20 Mbps. H.264 and MPEG-2 encoders are used to perform encoding and re-encoding on the concerned video sequences.
d. Frame replication has been performed after removal of preexisting sequence of frames. Frame insertion forgery is done either by swapping two particular frame sequences with each other or by inserting a frame sequence at another location after movement of preexisting frames ahead by required steps.
e. Minimum and maximum number of frames tampered is 10 and 60 respectively.

3.3. Detection and Localization Results of Original and Forged Videos

In this section, we present the results of experimental validation of the proposed technique. Group-1 contains 30 non-tampered and 70 tampered videos. Among 70 tampered videos, 30 have undergone frame deletion forgery and remaining video sequences are equally partitioned for frame duplication and frame insertion forgery. For H.264 and MPEG-2 videos, this technique generated a True Positive Rate of 81% and 77% respectively. On the other hand, Group 2 contains 100 videos out of which 20 are non-tampered. 30 videos are utilized for frame removal forgery and 25 videos exhibit frame insertion and replication forgery separately. The proposed technique was found to detect video inter-frame forgery on mobile recorded H.264 videos with an average accuracy of 86%.



(a) Original Video (b) Frame Deletion

(c) Frame Replication (d) Frame Insertion

Figure 5. Demonstrating the Effect of Forgery

Table 1. Detection and localization of forged videos (in %) (DA: Detection Accuracy, LA: Localization Accuracy)

	Group 1		Group 2	
Forgery / Result	DA(%)	LA(%)	DA(%)	LA(%)
Original	93	-	70	-
Frame Insertion	80	80	92	92
Frame Removal	83	73	83	76
Frame Replication	75	70	88	88

Table 1 show the detection and localization accuracies for all types of inter-frame forgeries on Group 1 and Group 2 videos and demonstrated that this technique is effective for frame removal and insertion forgery. The testing of proposed algorithm on some of these videos is demonstrated in Figure 5. Four non-contiguous spikes are generated in the gradient pattern as shown in Figure 5(a) depicting non-tampered video according to the algorithm. After deleting some frames (231-292) from the original video, testing is perfomed using the proposed approach which yields six spikes as shown in Figure 5(b). Among these spikes, continuous pair occurs at (76, 77) which shows that frame deletion starts from 231st frame (77×3=231). Thin lines represent single spikes which are non-contiguous whereas two continuous spikes in Figure 5 and are shown by thick blue lines.

In the same video, replication of frame 230 on the sequence (231-291) yields continuous peak points at (97, 98) as in Figure 5(c). It indicates that frame duplication ends at 294th frame (98×3=294). Likewise, we performed frame insertion forgery on another video sequence and inserted the frame sequence (231-292) in place of frames (501-562). This forgery yields continuous spikes at (76, 77), (166, 167) and (187, 188) in Figure 5(d). These spikes depict that tampered sequence may contain 231st (77×3=231), 501st (167×3=501) and 564th (188×3=564) frame.

Further analysis of group 1 of the dataset is performed by varying the initial bit-rate of the video in the range 100 Kbps to 9 Mbps and then reencoding each video using H.264 codec by varying bit-rates in the same range. Table 2 presents the detection performance of the proposed technique as a function of various bit-rates used during recording and re-encoding. First column of this table reveals that the technique generated ineffective results if reconstruction of tampered video is done with low quality encoder or at low bit-rate. If target bit-rate is at atleast 300 Kbps larger than the initial bit-rate, the technique was found to give

effective results. Figure 6 is shows Detection accuracies for video sequences recorded using different bit-rates.

Table 2. Detection Accuracy under varying bit-rate environment of Group 1 video sequences (in %). (K:Kbps, M:Mbps, TBR: Target Bit Rate, IBR: Initial Bit Rate)

TBR/ IBR	100K	200K	300K	400K	500K	600K	700K	800K	900K	1M	3M	6M	9M
100K	60	60	66	60	66	66	66	60	66	66	73	66	66
200K	73	60	66	60	66	66	73	66	66	66	73	66	66
300K	66	60	80	80	73	60	73	80	73	73	80	80	73
400K	73	60	73	66	73	73	86	86	80	80	73	73	66
500K	66	66	73	73	66	80	73	80	80	80	80	80	80
600K	66	66	60	73	73	66	73	80	80	80	80	80	80
700K	73	66	66	80	73	73	73	80	80	80	73	80	80
800K	66	66	80	73	80	80	80	80	66	80	73	80	80
900K	66	60	73	73	73	73	66	73	66	73	66	66	66
1M	73	66	66	86	66	80	73	73	66	80	73	80	80
3M	66	73	66	66	80	73	66	66	73	66	80	73	80
6M	60	86	73	73	73	66	66	66	73	73	73	73	73
9M	60	80	73	73	80	73	73	66	73	73	73	73	73

The proposed technique was then validated on different surveillance videos from Group 1 by varying the initial bit-rates from 100 Kbps to 9 Mbps. If same bit-rates are used to record and encode the video sequence, then best results are found at 100 Kbps, 700 Kbps and 9 Mbps bit-rate. To determine the effectiveness of the proposed technique on any kind of video sequence, a test set is prepared by deleting and replicating frames in the range 10 to 60. Experimental results demonstrate that this technique can detect inter-frame forgery irrespective of the number of frames deleted or replicated, although accuracy increases with increase in number of tampered frames as shown in Figure 7. Any activity in the video sequence cannot be concealed by tampering a mere one second which means that tampering with less than 30 frames can not cause any significant damage to the video. The proposed technique yields efficient results if more than 30 frames are deleted or replicated. The decrease in detection accuracy in case of deletion of 50 frames or duplication of 45 frames was due to testing of proposed algorithm on extremely slow motion video sequence.

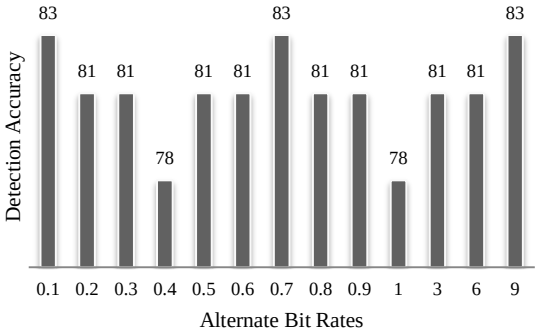


Figure 6. Detection accuracies for video sequences recorded using different bit-rates

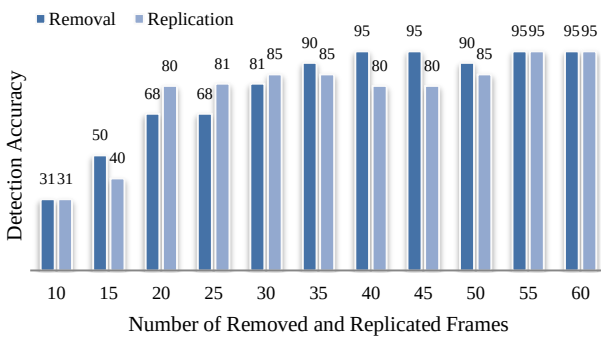


Figure 7. Detection accuracies for frame deletion and replication in the range 10-60

4. CONCLUSION

This paper presents a novel technique for video inter-frame forgery detection which address all types of inter-frame forgeries like frame insertion, frame removal and frame replication by utilizing two forensic features from the literature, Prediction Residual and Optical Flow. The proposed technique works quite effectively for videos recorded using surveillance cameras and manually recorded mobile videos. Furthermore, rather than the subjective analysis of the footprints left after tampering operation, a detection model proposed in this paper automatically detects forged video by simply utilizing the spikes count. This technique was found independent of motion of objects in a video sequence, number of frames tampered, number of objects in a video sequence, illumination variation, recording device or compression codec utilized. The proposed technique can detect inter-frame forgery with an average accuracy of 83%. Even using

alternate bit-rates for recording and reconstructing a video does not affect the detection results of this technique unless the target bit-rate is extremely high or extremely low. However, our tests revealed that this technique suffers from performance loss when applied to videos with extremely slow motion. Tampering of large number of frames was found to increase the probability of forgery detection. Enhancing the efficiency of the proposed technique for low quality videos remains the focus of our future research. Along with prediction residual and optical flow, some other features can also be utilized for more effective results.

REFERENCES

[1] Wilska TA, "Mobile Phone Use as Part of Young People's Consumption Styles", *Journal of consumer policy*, 2003 Dec 1;26(4):441-63.

[2] Farid H, "*Exposing Digital Forgeries in Scientific Images*", In Proceedings of the 8th workshop on Multimedia and security 2006 Sep 26 (pp. 29-36). ACM.

[3] Jin H, "Research of Blind Forensics Algorithm on Digital Image Tampering", *Indonesian Journal of Electrical Engineering and Computer Science*, 2014 Jul 1;12(7):5399-407.

[4] 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, 2015:1-31.

[5] Suryavanshi H, Mishra A, Kumar S, "Digital Image Watermarking in Wavelet Domain*", International Journal of Electrical and Computer Engineering*, 2013 Feb 1;3(1):1.

[6] Kobayashi M, Okabe T, Sato Y, *"Detecting Video Forgeries Based on Noise Characteristics"*, InPacific-Rim Symposium on Image and Video Technology 2009 Jan 13 (pp. 306-317). Springer Berlin Heidelberg.

[7] 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 30;11(2):120-40.

[8] 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 18;13(9):12605-31.

[9] Shanableh T, "Detection of Frame Deletion for Digital Video Forensics", *Digital Investigation* 2013 Dec 31;10(4):350-60.

[10] Zheng L, Sun T, Shi YQ, *"Inter-frame Video Forgery Detection Based on Block-Wise Brightness Variance Descriptor*", InInternational Workshop on Digital Watermarking 2014 Oct 1 (pp. 18-30), Springer International Publishing.

[11] Wang W, Farid H, *"Exposing Digital Forgeries in Video by Detecting Duplication"*, InProceedings of the 9th workshop on Multimedia & security 2007 Sep 20 (pp. 35-42). ACM.

[12] Feng C, Xu Z, Zhang W, Xu Y, *"Automatic Location of Frame Deletion Point for Digital Video Forensics",* In Proceedings of the 2nd ACM workshop on Information hiding and multimedia security 2014 Jun 11 (pp. 171-179), ACM.

[13] Wang Q, Li Z, Zhang Z, Ma Q, "Video Inter-frame Forgery Identification Based on Optical Flow Consistency", Sensors & Transducers, 2014 Mar 1;166(3):229.

[14] Gironi A, Fontani M, Bianchi T, Piva A, Barni M, "A Video Forensic Technique for Detecting Frame Deletion and Insertion", In 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2014 May 4 (pp. 6226-6230). IEEE.

[15] Wang W, Farid H, *"Exposing Digital Forgeries in Video by Detecting Double MPEG Compression"*, In Proceedings of the 8th workshop on Multimedia and security 2006 Sep 26 (pp. 37-47), ACM.

[16] Chen W, Shi YQ, *"Detection of Double MPEG Compression Based on First Digit Statistics"*, InInternational Workshop on Digital Watermarking 2008 Nov 10 (pp. 16-30), Springer Berlin Heidelberg.

[17] Sun T, Wang W, Jiang X, *"Exposing Video Forgeries by Detecting MPEG Double Compression",* In 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2012 Mar 25 (pp. 1389-1392). IEEE.

[18] Milani S, Bestagini P, Tagliasacchi M, Tubaro S, *"Multiple Compression Detection for Video Sequences",* In Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on 2012 Sep 17 (pp. 112-117). IEEE.

[19] Jiang X, Wang W, Sun T, Shi YQ, Wang S, *"Detection of Double Compression in MPEG-4 Videos Based on Markov Statistics"*, IEEE Signal processing letters. 2013 May;20(5):447-50.

[20] Luo W, Wu M, Huang J, *"MPEG Recompression Detection Based on Block Artifacts",* In Electronic Imaging 2008 2008 Feb 14 (pp. 68190X-68190X). International Society for Optics and Photonics.

[21] Vazquez-Padin D, Fontani M, Bianchi T, Comesaña P, Piva A, Barni M, *"Detection of Video Double Encoding with GOP Size Estimation*", In 2012 IEEE International Workshop on Information Forensics and Security (WIFS) 2012 Dec 2 (pp. 151-156). IEEE.

[22] 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",* In International Conference on Intelligent Computing 2015 Aug 20 (pp. 787-793). Springer International Publishing.
[23] Liu H, Li S, Bian S, *"Detecting Frame Deletion in H. 264 Video",* In International Conference on Information Security Practice and Experience 2014 May 5 (pp. 262-270). Springer International Publishing.
[24] Singh RD, Aggarwal N, *"Detection of Re-Compression, Transcoding and Frame-Deletion for Digital Video Authentication",* In 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS) 2015 Dec 21 (pp. 1-6). IEEE.
[25] Dong Q, Yang G, Zhu N, "A MCEA Based Passive Forensics Scheme for Detecting Frame-Based Video Tampering", *Digital Investigation*, 2012 Nov 30;9(2):151-9.
[26] Stamm MC, Lin WS, Liu KR, "Temporal Forensics and Anti-Forensics for Motion Compensated Video", *IEEE Transactions on Information Forensics and Security*, 2012 Aug;7(4):1315-29.
[27] Chao J, Jiang X, Sun T, *"A Novel Video Inter-Frame Forgery Model Detection Scheme Based on Optical Flow Consistency"*, In International Workshop on Digital Watermarking 2012 Oct 31 (pp. 267-281), Springer Berlin Heidelberg.
[28] Wang W, Jiang X, Wang S, Wan M, Sun T, *"Identifying Video Forgery Process using Optical Flow",* In International Workshop on Digital Watermarking 2013 Oct 1 (pp. 244-257). Springer Berlin Heidelberg.
[29] Horn BK, Schunck BG, "Determining Optical Flow", *Artificial Intelligence*, 1981 Aug 1;17(1-3):185-203.
[30] P. U. DIC, "Video forgery data at panjab university, chandigarh," Online, Github Repository, https://github.com/navagg/DIC-PU-Videos-Forgery.git, 8 2016.

BIOGRAPHIES OF AUTHORS

Staffy Kingra is pursuing Masters in Computer Science and Engineering in University Institute of Engineering and Technology, Panjab University, Chandigarh, India. She got her bachelors degree in Computer Science and Engineering from Punjab Technical University, Jalandhar. She is currently working in the digital video forensics domain with special emphasis on video inter-frame tampering detection.

Dr.Naveen Aggarwal is actively working in the area of Computer Vision and Data Mining. He did his Ph.D. from GGSIPU, Delhi in year 2011 and M. Tech. in Computer Science and Engineering from IIT, Kharagpur. Dr. Aggarwal has guided several M. Tech. students. He has over 80 publications in International journals and conferences. He is currently working as an Associate Professor in UIET, Panjab University, Chandigarh, India.

Raahat Devender Singh is a PhD student working in the Department of Computer Science and Engineering in UIET, Panjab University, Chandigarh, India. She obtained her master's degree in Computer Science and Engineering from Punjabi University, Patiala. She is currently working in the digital visual media forensics domain, with primary focus on digital video authentication.