International Journal of Recent Trends in Engineering & Research (IJRTER)
Conference on Recent Trends in Electrical and Electronics Engineering (RTEEE '19)
Special Issue; March- 2019 [ISSN: 2455-1457]
DOI: 0.23883/IJRTER.CONF.20190304.002.VDFJ0

COPY-MOVE FORGERY DETECTION IN VIDEO FORENSICS USING OPTICAL FLOW FOR COARSE-TO-FINE DETECTION

Aiswerya.S.B, P.V.Deepa(Assistant professor)
Department Of Electronics And Communication Engineering (Communication Systems)
Arunachala College Of Engineering For Women
Manavilai, Nagercoil, India.

Abstract—Video copy-move forgery detection is used in multimedia forensics to protect digital videos from malicious use. Based on multiple similarity calculations and unstable image features the detection efficiency, robustness and applicability can be balanced. A novel approach has been proposed to detect frame copy-move forgeries. A coarse-to-fine detection strategy based on optical flow and stable parameters is designed. Coarse detection analyzes OF sum consistency to find suspected tampered points. Fine detection is then conducted for precise location of forgery, including duplicated frames pair matching based on OF correlation and validation checks to further reduce the false detections. The proposed approach is effective and efficient in detecting both unsmooth and common smooth forgery. Also it has high robustness.

Keywords—Copy-move forgery, optical flow, coarse–to-fine detection, video passive forensics.

I. INTRODUCTION

The high speed development and spread of image and video processing software, such as Photoshop, Adobe Premiere and Final Cut Pro, makes it easier to tamper with digital visual media without leaving obvious traces. However, malicious tampering may cause serious legal and social problems. For example, tampered images or videos may be used to provide false evidence in court, or mislead the public about the truth in news reports. Meanwhile, the vast and growing quantity of multimedia information makes itdifficult to detect tampering using only human intuition.

In recent years, researchers have increasingly focused on video forensics, not only because the amount of video data isincreasing at an explosive speed, but also because video tampering is becoming more and easier, to which a wide range of possible alterations can be applied, suchas framedeletion, frame insertion, and video compression. Among them, copy-move forgery to extend or hide specific objects in the same video is one of the common methods.

Based on different operational domains, video copy-move forgeries can be classified into regional forgery and frame cloning.

REGIONAL COPY-MOVE TAMPERING

It changes only parts of the frame images, which is similar to image copy-move, and can be detected by relatively mature image forensic techniques.

THE FRAME COPY-MOVE FORGERY

It occurs in the time domain. It is performed by copying successive video frames and pasting them to another non-overlapping position, aiming to conceal objects, clone regions, or extend the time of some specific activities to forge the event records.

In frame copy-move forgery, cloning and pasting successive frames in the same video improves the imperceptibility and calculation difficulty, making it ineffective to detect the changes of color, shooting parameters, illumination condition, etc., but it leads to abnormal points in the parameter distribution, and creates a high level of correlation between the original and duplicated frames.

METHODS TO DETECT FRAME COPY-MOVE FORGERY

Based on the above idea, different approaches have been developed to detect frame copy-move forgeries, which can be divided into two categories: 1. Image feature based and 2. Video feature based.

Algorithms of the first category extract and explore image features of each frame to detect correlation, including gray values, image texture, color modes, and noise features. In the second category, they exploit the unique features in videos, such as motion features, video compression and coding features (including size, bitrate, and frame type) to analyze the side effect caused by copy-move operation.

DOI: 0.23883/IJRTER.CONF.20190304.002.VDFJ0

Although various detection solutions towards video copy-move forgery have been proposed, current schemes are faced with the following challenges.

High computation complexity: Pixel based or directly correlation based approaches generally suffer from high computational burden. It will be quite time consuming to analyze a large number of frames in videos with a bulk of data far greater than that of still images.

Unstable detection performance: Methods based on image features, including texture, color modes, noise, and pixel gray values, are vulnerable to regular attacks or post-processing on videos, like secondary compression and additive noise. Few of the existing detection approaches take the detection robustness into account, and generally set fixed sensitive parameters for detection.

Limited applicability: Some methods have restrictions to the detected videos in terms of video formats, number of tampered frames, tampering ways (only for unsmooth manipulation) or shooting ways (only with static camera), which limit the practical applicability in video forensics.

These challenges imply that a practical frame copy-move forgery detection scheme is in high demand, which should satisfy three basic requirements: low computation complexity, high accuracy with good robustness, and strong applicability. The proposed work tries to take the above three requirements into consideration, and also propose a new method to detect copy-move forgery.

II. EXISTING WORK

Existing approaches for frame copy-move forgery detection have been presented through analyzing the side effect caused by copy-move operation, namely, the high feature correlation between the original and duplicated frames caused by either frame insertion or replacement, as shown in Fig. 1. Based on the extracted feature type, it can be divided into two categories: Image feature based and Video feature based.

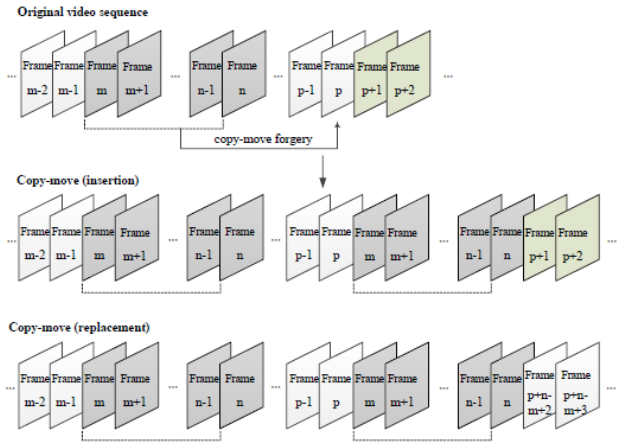


Figure 1. Illustration of frame copy-move forgery

A. *Image Feature Based Methods*

This category of algorithms explores image features of each frame to detect frame correlation, such as pixel gray values, image texture, color modes, and noise features. Wang and Farid earlier proposed a method based on temporal and spatial correlation matrices of pixels in gray images to detect duplication, finding that a high correlation indicates an instance of frame duplication forgery detect video copy-move forgery. Lin and Chang designed a coarse-to-fine approach based on histogram difference of two adjacent frames in the RGB color space to detect video duplication forgery in the temporal domain. However, these methods are usually vulnerable to regular attacks or post-processing on videos, like secondary compression and additive noise. For example, the performance of methods based on singular value decomposition (SVD), gray value, and histogram difference will suffer from noise or filtering, whereas noise-based approaches drops dramatically when the video is compressed by conventional codes, such as MPEG-2 or H.264.

B. *Video Feature Based Methods*

This kind of algorithms generally achieves higher robustness by exploiting the unique features in videos, such as motion features, video compression and coding features (including size, bitrate, and frame type). Chao, Jiang and Sun calculated Optical Flow (OF) consistency to detect video inter-frame forgery. They used a rough detection method and binary searching scheme to achieve good performance. Kingra, Aggarwal and Singh analyzed gradients of prediction residual and OF for the detection of frame-based tampering in MPEG-2 and H.264 encoded videos. However, these methods only analyzed the situation of MPEG-x videos specifically, and mainly focused on static-background videos or videos with no significant motion.

International Journal of Recent Trends in Engineering & Research (IJRTER)
Conference on Recent Trends in Electrical and Electronics Engineering (RTEEE '19)
Special Issue; March- 2019 [ISSN: 2455-1457]
DOI: 0.23883/IJRTER.CONF.20190304.002.VDFJ0

III. PRELIMINARIES

The OF in video sequences, and the influence of frame copy-move forgery on OF correlation and OF sum consistency are explained in this section.

A. *OPTICAL FLOW*

OF is the distribution of apparent movement velocities of brightness patterns in videos, which can give important information about the image spatial arrangement and change rate of objects. Because of its highly descriptive motion information, it has been widely employed in multimedia processing and computer vision field including image segmentation, target tracking, face coding, mosaic construction, etc.

Differential methods are the most widely used techniques for OF computation in image sequences. Among them, the Lucas-Kanade Optical Flow, proposed by B.D. Lucas and T. Kanade, is a local least square calculation to compute OF sparsely for each blob. Because of the rapid computation, simple application, and robustness under noise, OF vectors extracted by Lucas-Kanade algorithm have been widely studied and used. Fig. 2 gives an example of a video sequence and shows the motion change vectors of the corresponding pixel between adjacent frames in Lucas-Kanade OF fields.The OF describes the details of movement changes in each frame and reflects the difference or similarity of frames in video sequences.

Since video copy-move forgeries across the temporal domain always aim to conceal the motion records or change the time of some specific activities, videos recording moving objects are much easier to tamper. Therefore, in videos with copy-move forgery, OFs of adjacent frames can be extracted

to record the detailed difference of frame images; high similarity of OFs between original and duplicated frames created by copy-move operation permits detection.

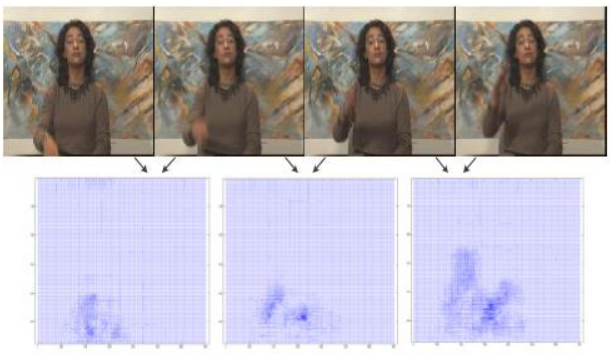


Figure 2. Illustration of motion changes in OF field

B. *OF CORRELATION*

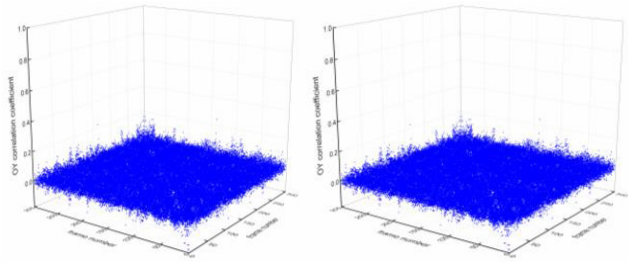
To describe the OF similarity between frame images, the correlation coefficient is taken as a measure. For two adjacent frames *i* and *i*+1, the Lucas Kanade OF vector OFi is decomposed into two figures: OXi in X direction and OYi in Y direction.In a video with *N* frames, *N-1* OF vectors will be extracted and the correlation coefficients between every two OFs can be calculated using two equations.

$$cor(i,j) = \frac{\sum_{m=1}^{wid}\sum_{n=1}^{hei}(OX_i(\mathrm{m,n}) - \overline{OX_i})(OX_j(\mathrm{m,n}) - \overline{OX_j})}{\sqrt{\sum_{m=1}^{wid}\sum_{n=1}^{hei}(OX_i(\mathrm{m,n}) - \overline{OX_i})\sum_{m=1}^{wid}\sum_{n=1}^{hei}(OX_j(\mathrm{m,n}) - \overline{OX_j})}} \quad (1)$$

To demonstrate how copy-move forgery affects the OF correlation, an example originated from a raw YUV sequence is given in Fig. 3 and Fig. 4. The correlation coefficient matrices of both *OX* and *OY* in video sequences are shown after removing the diagonal elements. In Fig. 3(a) and (b), the correlation coefficients between every two OFs are small in an original video because the OF records the motion change details of each corresponding pixel between two adjacent frames; different OFs have a relatively low correlation. But copy-move forgery will result in high correlation between original frame OFs and duplicated frame OFs in videos. From Fig. 4(a), (b), we can see that in a copy-move tampered video sequence, the correlation coefficients between the original frame OFs and the duplicated frame OFs are up to 1, significantly higher than the normal values. Moreover, post-processing on videos may be performed along with copy-move forgery, making the tampering difficult to detect, such as adding noise, filtering, and

In Fig. 3 and 4(a),(b), the correlation coefficients between every two OFs are small in an original video because the OF records the motion change details of each corresponding pixel between two adjacent frames; different OFs have a relatively low correlation. But copy-move forgery will result in high correlation between original frame OFs and duplicated frame OFs in videos. secondary loss compression. As shown in Fig. 4 (c), (d), although the video sequence is subjected to H.264 compression, high correlation between the original frame OFs and the duplicated frame OFs is still apparent, which can be identified by setting a smaller threshold.

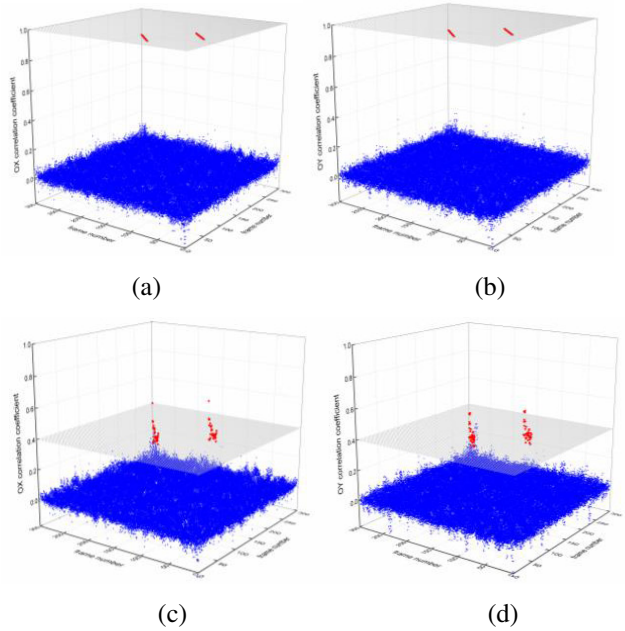
Because of the robustness of OFs, even though additional operation introduces differences between initially identical frame sequences, the motion features will change little. Accordingly, the high OF correlation between original and duplicated frames still exists and can provide evidence for copy-move forgery detection.



(a) (b)

FIGURE 3. OF correlation coefficient matrices of an original video. (a). *OX* correlation coefficient matrix. (b). *OY* correlation coefficient matrix.

DOI: 0.23883/IJRTER.CONF.20190304.002.VDFJ0



(a) (b)

(c) (d)

FIGURE 4. OF correlation coefficient matrices of a copy-move tampered video. (a). *OX* correlation coefficient matrix. (b). *OY* correlation coefficient matrix. (c). *OX* correlation coefficient matrix after video compression. (d). *OY* correlation coefficient matrix after video compression.

C. OF SUM CONSISTENCY

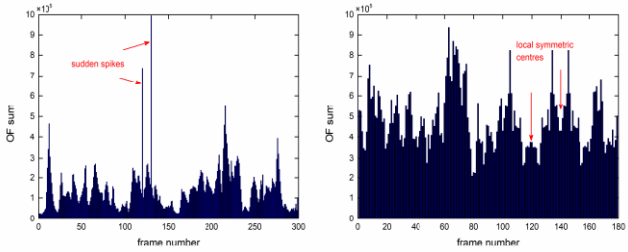
Since the calculation of OF correlation is point by point in frames, the computational cost is high and will increase rapidly as the image size and video length increase. Therefore, the consistency of OFs, as a global feature, is helpful to locate suspected tampered positions, and reduce multiple calculations or comparisons of correlation matrices in forgery detection.

We analyze the OF sum consistency to identify candidate tampered points. In a video with frames, for the i-thframe, the absolute values of OX_i and OY_i in each pixel (m,n) are added with (2) as the OF sum, then the sum sequence composed of N-1values is obtained.

$$sum_{OF_i} = \sum_{m=1}^{wid}\sum_{n=1}^{hei}(|OX_i(\mathrm{m,n})| + |OY_i(\mathrm{m,n})|), i = 1,2,\dots,N-1 \quad (2)$$

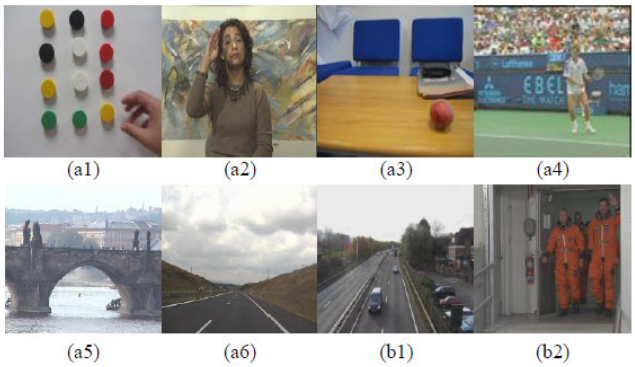
Based on how frame copy-move forgery affects the OF sum consistency, we classify it into two major types. The first type is to directly clone some frames to a different position in videos. The manipulation will generally result in sudden motion spikes in the OF sum sequence, such as inevitably unsmooth insertion because of motion in videos, or manipulation on non-key frames that may aim to change or extend the time of some key frames to obfuscate the event records. Because of the continuity and regularity of the motion in videos, the OF sum sequence will be relatively consistent, meaning no obvious spikes in the sequence. But this type of copy-move forgery will destroy the consistency due to frame replacement or insertion, and bring larger difference between adjacent frames, therefore, leading to anomalies in the OF sum sequence. Fig. 5 (a) shows an example of the OF sum sequence of a copy-move tampered video. There are some small fluctuations in the sequence caused by movement of objects, but these OF sums fluctuate slightly or gradually and have minor differences from the neighboring OF sum values. However, spikes are manifest at the start and end points of the duplicated frames because a copy-move forgery destroys the consistency of the OF sums. These abnormal spikes can be detected to locate the tampered positions.

Another type is the careful manipulation which smoothly integrates the duplicated frames into videos to avoid the abnormal motion spikes. The easiest way is to insert frames in reverse order behind the tampered position, which is difficult to be detected by human eyes. For example, as shown in Fig. 5(b), frames 100 to 119 are inserted in reverse order behind frame 120, and then, frames 101 to 120 are inserted in proper order behind the inserted part. Therefore, the OF sum sequence is smooth at both the start point (the 120_{th} frame) and end point (the 160_{th} frame) of the duplicated frames, making it difficult to detect copy-move forgery based on abnormal spikes. However, there are obvious local symmetries because of the reverse insertion, where the symmetric centres (actually the start or end points of the duplicated frames) can be detected to locate the tampered positions. Note that inserting frames in reverse order is generally effective in videos with less or no direction attributes (see Fig. 6(a1-a6) as examples), but not feasible for videos with moving cars or persons (as shown in Fig. 6(b1-b2)), which can be easily detected by human observation.



(a) (b)

FIGURE 5. OF sum sequence of tampered videos. (a). Tampered video sequence with spikes. (b). Tampered video sequence with symmetries.



(a1) (a2) (a3) (a4)

(a5) (a6) (b1) (b2)

FIGURE 6. Examples of video frames. (a1). Hand movement. (a2). Sitting person. (a3). Moving ball. (a4).

Side-to-side motion. (a5). Remote monitoring. (a6). Moving camera. (b1). Moving car. (b2) Walking person.

IV. Proposed Detection Method

OFs and their high and stable correlation in copy-move tampered videos offer basis for effective detection. For calculation cost reasons, the consistency of OFs is analyzed first to locate suspected tampered positions. This process will help to reduce multiple calculations and comparisons of correlation matrices, but may lead to more false detections. Fine detection based on OF correlation is then proposed to match the duplicated frame pairs, and reduction of false detections based on validation checks will be conducted further for precision. The whole detection process is shown in Fig.7

A. *COARSE DETECTION*

Temporal consistency is ubiquitous in original videos, where temporally adjacent video shots usually share similar visual and semantic content, leading to the similarity of features extracted from adjacent video shots. Therefore, we define the OF sum consistency as a high similarity in OF sums of adjacent video frames.Copy-move forgery will affect the consistency due to frame replacement or insertion, because larger difference of OFs at the start and end points of the duplicated frame sequence will lead to anomalies in OF sum sequences, providing a quantitative measurement for video analysis and forgery detection.

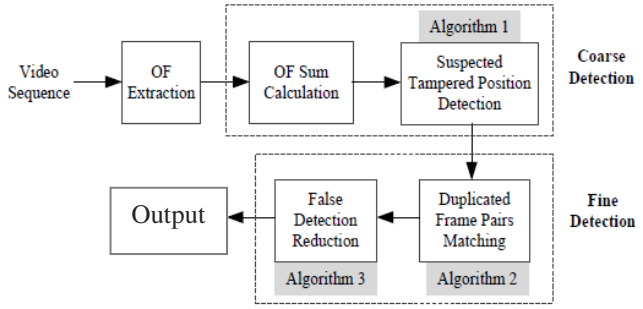


Figure 7. The detection process of the proposed scheme**.**

Therefore, coarse detection based on the OF sum consistency helps to extract abnormal points as suspected tampered positions, avoiding multiple calculations in correlation analysis. The algorithm of abnormities detection is proposed as follows. For a video sequence with N frames, it firstly extracts all individual frames and compute the Lucas Kanade OF for every two adjacent frames i and i+1 (i=1, 2, …, N-1), obtaining OXi matrices in X direction and OYi in Y direction. Then it computes the OF sums with (2) and get the OF sum sequences composed of N-1 values. The mean value of OF sums of its adjacent 2T frames is calculated with (3) to detect whether it is a sudden motion spike.

$$\overline{sum\_OF_i} = \frac{1}{2T}\sum_{k=1}^{T}\left(sum_{OF_{i-k}} + sum\_OF_{i+k}\right) \quad (3)$$

where is the window size for determining the number of adjacent frames. The rate of change β_i is defined to describe the fluctuation extent of the i-th frame and is measured by (4).

$$\beta_i = sum\_OF_i / sum\_OF_i \quad (4)$$

If β_i is larger than a threshold *THR_F*, meaning an abnormal spike in sum_OF_i is manifest, then the i_{th} frame and its adjacent frames,(i-1)th ,(i+1)th frames, are identified as suspected tampered positions.

Meanwhile, we determine whether the i_{th} frame is a local symmetric centre in the OF sum sequence to detect the copy-move forgery of continuous reverse and forward insertion. If the OF sum around the i_{th} frame satisfies

$$sum_{OF_{i+k}} \approx sum_{OF_{i-k-1}}, k = 0,1,\ldots.T \quad (5)$$

In copy-move forgeries, the suspected tampered positions may be the start or end points of the duplicated frame sequences. After the coarse detection, fine detection can find duplicated frame pairs only around the tampered positions, improving detection efficiency with little computation in the OF correlation computing.

B. *FINE DETECTION*

Coarse detection based on rough OF sum features helps to locate suspected tampered positions, but whether the anomalies are caused by copy-move forgery needs fine detection based on more detailed features to identify. In this section, two steps of fine detection are proposed, including duplicated frame pairs matching based on OF correlation and reduction of false alarms based on video inherent features.

1) DUPLICATED FRAME PAIR MATCHING

OF correlation calculation is used to match the duplicated frame pairs after coarse detection. It extracts the OFs around each suspected tampered point, and calculate their correlation coefficients either with all the other OFs or with the OFs of the adjacent frames (for local symmetric centers). Note that OX and OY have the same size with the video frame image, meaning the calculation of the OF correlation coefficients will be heavy. It is necessary to subsample the input OFs to reduce the number of pixels involved in the computation. Meanwhile, as shown in Fig. 3 and Fig. 4 the correlation coefficient matrices for OX and OY in the video sequences are nearly the same. Therefore, it is necessary to only calculate the OF correlation coefficients of OX to reduce the computation load.

Algorithm 2 runs as follows. First, for each suspected tampered frame number i that is detected as a sudden spike, it calculates the OF correlation coefficients cor(i, j) (j=1,2,…,N-1) to find the maximum correlation coefficient cor(i, j)max. The threshold THR_C1, which is always significantly larger than the average value of all the OF correlation coefficients cor(i, j), is used to determine whether the related frame pairs (i, j), (i+1, j+1) of cor(i, j)max have high correlation coefficients. Then, for each suspected tampered frame number i that is detected as a local symmetric centre, it calculates the OF correlation coefficients of the frame pairs before and after i frame. Note that the while loop will be repeated for at most „nt" times, where „nt" is the number of copy-moved frames. The threshold THR_C2 is used to get the successive frames with high correlation coefficients. The final outputs of the

algorithm are the candidate start or end points of tampered frame sequences.

2) REDUCTION OF FALSE DETECTIONS

It is worth noting that fine detection for copy-move forgeries depends on the coarse detection results with abnormal points in OF sum sequences. However, tampering is not the only factor accounting for the outliers in coarse detection phrase. Other factors may also produce spikes or local symmetric centers, leading to false detections. For example, some spikes may come from the weaker OF sum consistency in videos with quickly moving content, while local symmetry may be derived from continuous static scenes or smooth movement in videos. In fine detection based on correlation analysis, adjacent frames with high similarity will also lead to false alarms. Besides, additional operations may be performed after copy-move forgery to cause interference and cover up the abnormities. Therefore, validation checks based on the inherent features of videos will be introduced to reduce the interference frames as further fine detection. Here it defines three inherent features of videos in copy-move forgery detection as follows.

Similarity: Adjacent frames or frames in a short time interval have high similarity because of video consistency. Similarity leads to high correlation between original adjacent frames and may cause false detections in matching duplicated frame pairs. However, it can be distinguished by detecting the frame number differences between the suspected duplicated frame pairs. A small difference means the two frames are close to each other, and the high correlation is caused by video similarity instead of copy-move operation.

Continuity: Videos with continuous multi-frames carry more information, and will be more likely to be tampered than discontinuous or short-length frames with scarce actual meaning. Continuity ensures that the tampered frames are a successive sequence. That is, for a suspected frame pair (i, j), if both (i–1, j–1) and (i+1, j+1) frame pairs have low correlation (i , j) should be found as a false detection. If both (i–1, j–1) and (i+1, j+1) frame pairs have high correlation, then (i, j) should also be found because it is not the end or start point of the tampered frame sequence.

Regularity: The detected duplicated video sequence has the same length with its original sequence, meaning both the intervals of the start points and the end points are equal. Regularity means that the two detected sequences with high correlation (i.e., the duplicated frame sequence and its original sequence) should have the same length, and ensures the integrity of the detection results.

Making use of these features in videos for fine detection after OF correlation calculation, false alarms will be effectively reduced.

V. CONCLUSION AND FUTURE WORK

A practical frame copy-move forgery detection scheme should achieve low computation complexity, high accuracy with good robustness, and strong applicability. In this proposed work, a coarse-to-fine approach based on video OF features and stable parameters to make a tradeoff among the three requirements in frame copy-move forgery detection is proposed. The method on different kinds of videos with two common types of copy-move tampering, i.e. one with unsmooth forgery and one with smooth manipulation are validated.

The future work focuses on evaluating the accuracy and robustness of the algorithm by simulating common attacks as secondary forgery after copy-move forgery.

REFERENCES

[1] W.Wang, and H. Farid, "Exposing digital forgeries in video by detecting double MPEG compression", Proceedings of the 8th workshop on Multimedia and security. ACM, pp.37-47, 2006.
[2] M. Kobayashi, T. Okabe, and Y. Sato, "Detecting Forgery From Static-Scene Video Based on Inconsistency in Noise Level Functions," IEEE Transactions on Information Forensics & Security, vol. 5, no. 4, pp. 883-892, 2010.
[3] S. Milani, M. Fontani, P. Bestagini, et al., "An overview on video forensics," APSIPA Transactions on Signal and Information Processing, 1, 2012.
[4] X. Jiang, W. Wang, T. Sun, et al., "Detection of double compression in MPEG-4 videos based on Markov statistics," IEEE Signal processing letters, vol.20, no.5, pp. 447-450, 2013.
[5] P. Bestagini, S. Milani, M. Tagliasacchi, et al., "Local tampering detection in video sequences," Multimedia Signal Processing (MMSP), 2013 IEEE 15th International Workshop on. IEEE, pp. 488-493, 2013.
[6] J. Chao, X. Jiang, T. Sun. "A novel video inter-frame forgery model detection scheme based on optical flow consistency", The International Workshop on Digital Forensics and Watermarking 2012. Springer, Berlin, Heidelberg, pp. 267-281, 2013.
[7] Q. Wang, Z. Li, Z. Zhang, *et al*. "Video inter-frame forgery identification based on consistency of correlation coefficients of gray values," Journal of Computer and Communications, vol.2, no.04, pp.51, 2014.
[8] C. Feng, Z. Xu, W. Zhang, et al., "Automatic location of frame deletion point for digital video forensics," Proceedings of the 2nd ACM workshop on Information hiding and multimedia security. ACM, pp.171-179, 2014.
[9] Z. Zhang, J. Hou, Q. Ma, *et al*., "Efficient video frame insertion and deletion detection based on inconsistency of correlations between local binary pattern coded frames," Security and Communication Networks, vol.8, no.2, pp.311-320, 2015.
[10] C. S. Lin, C. C. Chen, and Y. C. Chang, "An Efficiency Enhanced Cluster Expanding Block Algorithm for Copy-Move Forgery Detection," Multimedia Tools & Applications, pp. 1-20, 2015.
[11] A. Bidokhti, and S. Ghaemmaghami, "Detection of regional copy/move forgery in MPEG videos using optical flow", International Symposium on Artificial Intelligence and Signal Processing. IEEE, 2015.

DOI: 0.23883/IJRTER.CONF.20190304.002.VDFJ0

[12] J. Yang, T. Huang, L. Su. "Using similarity analysis to detect frame duplication forgery in videos," Multimedia Tools and Applications, vol.75, no.4, pp.1793-1811, 2016.

