Low-Complexity Camera Tamper Detection based on Edge Information

Gil-beom Lee, Youn-chul Shin, Joo-heon Park, Myeong-jin Leeⓒ, *Member, IEEE*
Dept. of Information & Telecommunication, Korea Aerospace University, Korea

***Abstract*--A low-complexity algorithm for camera tamper detection is proposed which can detect various types of tamper attacks based on edge information. The performance of the proposed algorithm is evaluated for three types of tamper attacks and shown to achieve acceptable level of accuracy for all types of tamper attacks.**

I. INTRODUCTION

Recently, video analytics algorithms are introduced to video surveillance systems. Intelligent video analytics algorithm can reduce the cost for video monitoring process by automation. Target events which video surveillance systems target to detect include camera tamper attack, violence, intrusion, fire, etc. Camera tamper attack is the situation when the normal camera capture process is disturbed on malicious purposes, and it would be the first event among surveillance events to be detected by video analytics.

The types of camera tamper attacks in previous studies can be classified as in Table I. Defocused camera event is the case which the focal length of the camera is changed to blur the captured video sequences resulting in the reduction of edge pixels. Saglam detected the camera tamper attacks by using the difference of high frequency components after Discrete Fourier Transform (DFT) and High Pass Filtering (HPF) [1]. Aksay detected Covered and Defocused camera events by using wavelet transform and reduced false alarm rate by using edge data [2]. Ribnick detected Covered camera events by using the histogram of input video frames [3]. However, this algorithm is sensitive to the threshold for decision and has large false alarm rate.

TABLE I
TYPES OF CAMERA TAMPER ATTACK

Type	Feature
Defocused camera event	defocused by spray or rain fall
Covered camera event	camera lens occluded by external objects
Moved camera event	viewing angle of the camera is changed on malicious purpose

Moved camera event is the situation where the viewing angle of a camera is changed to different direction abruptly. Due to the large amount of motion blur in moved camera events, high frequency components are usually decreased in captured video frames. Yi detected Moved camera events by extracting features such as edge and corner with Scale Invariant Feature Transform (SIFT) [4]. Although SIFT algorithm has robust performance for various scales, it requires too much computing resources.

Most of the previous studies on camera tamper detection are limited to specific types of camera tamper attacks or require too much computational resources. In this paper, a novel low-complexity tamper detection algorithm is proposed to detect Defocused, Covered, and Moved camera events simultaneously by using edge information.

II. PROPOSED CAMERA TAMPER DETECTION ALGORITHM

The proposed tamper detection algorithm is shown in Fig. 1. Tamper events are detected by finding the difference between edges of background and current frames. Background frame is generated using Gaussian Mixture Model [5]. For edge detection, Canny edge detection algorithm is used to detect edges for current and background frames.

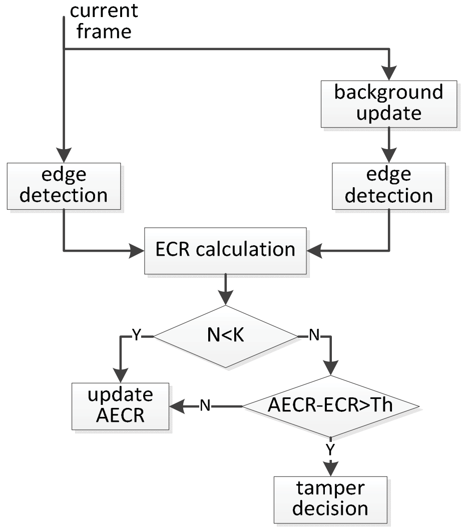

Fig. 1. Proposed tamper detection algorithm

During camera tamper attack, the amount of edge, the high frequency component of video frames, tends to be decreased. Therefore, edge changed rate (ECR) for current frame, the ratio of the number of edge pixels existing in both current and background frames to that of the background frame, is defined as follows.

$$ECR_n = \frac{\sum_p e_{n,p}^{BG} \cdot e_{n,p}^{C}}{\sum_p e_{n,p}^{BG}} \tag{1}$$

where $e_{n,p}^{BG}$ and $e_{n,p}^{C}$ represent the existence of an edge at pixel p in background and current frames with binary code, respectively.

ⓒ Corresponding Author (e-mail : artistic@kau.ac.kr)

This research was supported by Gyeonggi Regional Research Center (GRRC) support program.

978-1-4799-4851-2/14/$31.00 ©2014 IEEE

If the changed ratio of edges in background and current frames are measured by simple edge comparison without using ECR, there is high probability of false alarm from noise occurring over entire frame such as trees trembling in the wind. Moving objects in current frames without tamper attack do not appear in background frames, but their edges may be captured by simple edge comparison between current and background frames. In the proposed algorithm, false alarm caused by foreground objects can be removed by using ECR measure.

In the following procedure, to detect camera tamper attack, difference between average ECR (AECR) and current ECR are compared to a threshold. AECR can be calculated by averaging ECRs of recent frames without camera tamper attack as follows.

$$AECR_n = \frac{\sum_{n=0}^{N_0} ECR_n}{N_0} \quad (2)$$

where N_0 represents the number of successive frames with no tamper attack detected. For initial stage, AECR is calculated over $K (= 50)$ ECRs.

If the difference is larger than the threshold, the proposed algorithm determines that a camera tamper attack occurred. Otherwise, it determines that no tamper attack occurred and current ECR is used for the calculation of AECR. If camera tamper attacks are detected for successive five frames, the proposed algorithm finally makes alert.

If tamper attack continues over long period, the tampered video frames may be used for following background frame update and the changed amount of ECR from that of background frame may go below the threshold. To prevent the detected tamper attack from disappearing due to its long lasting period, considering the background absorption rate of GMM, if a tamper attack detected lasts over 600 frames, the proposed algorithm stops comparing the ECR with that of background and sets a tamper alert for following frames until its reset by operators.

III. Experimental Results

To evaluate the performance of the proposed tamper detection algorithm, video sequences in QVGA (320x240) resolution including three types of tamper attacks are used for experiment. The accuracy of tamper detection algorithm is measured by the following detection rate and false alarm rate with the terms defined in Table II.

TABLE II
Classification of Detection Results

Term	Definition
TP	alert on a tamper attack
FN	no alert on a tamper attack
FP	alert on no tamper attack

$$Detection\ Rate\,(DR) = \frac{TP}{TP + FN} \quad (3)$$

$$False\ Alarm\ Rate\,(FAR) = \frac{FP}{TP + FP} \quad (4)$$

Table III shows the accuracy of the proposed tamper detection algorithm. N is the number of tampering events. For Covered camera event, the proposed algorithm detected all the tamper attacks with false alarm rate of 6.25%. For Moved and Defocused camera events, it detected all the attacks without false alarm. For all kinds of tamper attacks, the proposed algorithm shows 100% of detection rate with false alarm rate of 2.08%. Tamper detection algorithm based on DFT and HPF in [1] showed DR of 95%, 91.7%, and 82.9% for Covered, Moved, and Defocused camera events, respectively. Although this algorithm has zero FAR, the complexity for detection is quite large and the detection rate of Defocused camera event is not acceptable. Tamper detection algorithm based on histogram in [2] showed 95% DR, but more than 20% FAR.

TABLE III
Accuracy of the Proposed Tamper Detection Algorithm

Event	TP	FN	FP	N	DR	FAR
Covered	15	0	1	15	100%	6.25%
Moved	13	0	0	13	100%	0%
Defocused	15	0	0	15	100%	0%

IV. Conclusion

A low complexity camera tamper detection algorithm based on edge information is proposed, which can detect Covered, Moved, and Defocused camera events. Although the computational load in the proposed algorithm is quite low compared to those of conventional tamper detection algorithms adopting DFT and SIFT, the accuracy of the proposed algorithm is shown to be better than those of the algorithms. It is required to be evaluated further for larger set of video sequences with various tamper attacks and to study adaptive thresholds for tamper decision and object removal to improve the FAR.

Reference

[1] A. Saglam and A. Temizel, “Real-time Adaptive Camera Tamper Detection for Video Surveillance,” in *Proc. IEEE Int. Conf. Advanced Video and Signal Based Surveillance*, pp. 430-435, Genova, 2009.

[2] A. Aksay, A. Temizel, and A, E, Cetin, “Camera Tamper Detection using Wavelet Analysis for Video Surveillance,” in *Proc. IEEE Conf. Adv. Video Signal Based Surveillance*, pp. 558-562, 2007.

[3] E. Ribnick, S. Atev, O. Masoud, R. Voyles, N. Papanikolopoulos, “Real-Time Detection of Camera Tampering,” in *Proc. IEEE Int. Conf. Video and Signal Based Surveillance*, pp. 10-15, Nov. 2006.

[4] Hongpeng Yi, Xuguo Jiao, Xianke Luo, Chai Yi, “Sift-based Camera Tamper Detection for Video Surveillance,” *25th Chinese Control and Decision Conference*, pp. 665-668, May 2013.

[5] C. Stauffer, W.E.L Grimson, “Adaptive Background Mixture Models for Real-time Tracking", *IEEE CVPR*, vol. 2, pp. 246-252, 1999.