J. Vis. Commun. Image R. 25 (2014) 1865–1877

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Rapid detection of camera tampering and abnormal disturbance for video surveillance system

Deng-Yuan Huang [a], Chao-Ho Chen [b,*], Tsong-Yi Chen [b], Wu-Chih Hu [c], Bo-Cin Chen [b]

[a] *Department of Electrical Engineering, Dayeh University, 168 University Rd., Dacun, Changhua 515, Taiwan, ROC*
[b] *Department of Electronic Engineering, National Kaohsiung University of Applied Sciences, 415 Chien Kung Rd., Kaohsiung 807, Taiwan, ROC*
[c] *Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, 300 Liu-Ho Rd., Makung, Penghu 880, Taiwan, ROC*

ARTICLE INFO

Article history:
Received 23 October 2013
Accepted 14 September 2014
Available online 23 September 2014

Keywords:
Camera tampering
Camera motion
Camera occlusion
Background subtraction
Video surveillance system
Screen shaking
Defocus
Color cast

ABSTRACT

Camera tampering may indicate that a criminal act is occurring. Common examples of camera tampering are turning the camera lens to point to a different direction (i.e., camera motion) and covering the lens by opaque objects or with paint (i.e., camera occlusion). Moreover, various abnormalities such as screen shaking, fogging, defocus, color cast, and screen flickering can strongly deteriorate the performance of a video surveillance system. This study proposes an automated method for rapidly detecting camera tampering and various abnormalities for a video surveillance system. The proposed method is based on the analyses of brightness, edge details, histogram distribution, and high-frequency information, making it computationally efficient. The proposed system runs at a frame rate of 20–30 frames/s, meeting the requirement of real-time operation. Experimental results show the superiority of the proposed method with an average of 4.4% of missed events compared to existing works.

1. Introduction

Video surveillance systems are widely used in the fields of environmental safety, traffic control, and crime prevention. Important public places such as government agencies, malls, schools, railway stations, airports, military bases, and historical sites are often equipped with digital camera recording systems for video surveillance. However, when cameras are tampered with, the video surveillance system will fail to work properly. Moreover, long-term monitoring of a screen by operators is difficult and many video cameras are frequently left unattended. An intelligent video surveillance system that can automatically analyze live video content, detect suspicious activities, and trigger an alarm to notify operators, is desirable.

Camera tampering is any sustained event which thoroughly alters the image seen by a video camera. Common examples of camera tampering in video surveillance systems are turning the camera lens to point to a different direction (i.e., camera motion) and covering the lens by opaque objects or with paint (i.e., camera occlusion). In general, camera problems are caused by: (1) deliberate actions, such as camera motion and occlusion; (2) weather conditions, such as image blurring due to fogging; (3) abnormal disturbances, such as screen shaking, defocus, color cast, and screen flickering. For automated camera tampering and abnormality detection systems, high reliability and a relatively low false alarm rate are strongly desirable. Most research on the detection of camera tampering and abnormalities has focused on discovering events that move, cover, or defocus the camera [1–6] in a video surveillance system. However, other abnormalities such as screen shaking, fogging, color cast, and screen flickering have received less attention.

Aksay et al. [1] proposed computationally efficient wavelet domain methods for the rapid detection of camera tampering and identified real-life security-related problems. Two algorithms were presented for detecting an obscured camera view and reduced visibility based on a learned background model together with the wavelet transform. However, camera tampering detection based on background modeling often suffers from instability due to varying light source intensity. Ribnick et al. [2] presented an approach to identify camera tampering by detecting large differences between older and more recent frames in video sequences, which are separately stored in two buffers, labeled as the short-term pool and the long-term pool, respectively. Three measures of image dissimilarity are then used to compare the frames to determine whether camera tampering has occurred. However,

* Corresponding author.
E-mail addresses: kevin@mail.dyu.edu.tw (D.-Y. Huang), thouho@kuas.edu.tw (C.-H. Chen), chentso@kuas.edu.tw (T.-Y. Chen), wchu@npu.edu.tw (W.-C. Hu), 1100305149@kuas.edu.tw (B.-C. Chen).

http://dx.doi.org/10.1016/j.jvcir.2014.09.007
1047-3203/© 2014 Elsevier Inc. All rights reserved.

several preset thresholds are required and need to be tuned manually for optimal performance.

Sağlam and Temizel [3] proposed adaptive algorithms to detect and identify abnormalities in video surveillance when the camera lens is defocused, moved, or covered. In their method, background subtraction is utilized to build the absolute background, which is used to determine camera tampering types. In the detection of camera defocus, the discrete Fourier transform is used and then a Gaussian windowing function is applied to eliminate low-frequency content. By comparing the high-frequency components of the current frame image and its background, a defocused camera view can be detected. In the detection of a moved camera, a delayed background image is built and compared with the current background using a preset criterion. The detection of a covered camera is done using the peak histograms of the current frame and its background. However, many thresholds must be set.

Lin and Wu [4] identified camera tampering by detecting edge differences and analyzing the grayscale histograms between current and previous frames. An adaptive non-background model image is compared with both incoming video frames and an updated background image for edge difference detection and abnormality justification. Three types of camera tampering and abnormality, namely occlusion, defocus, and motion, were detected in a timely fashion with an overall recognition rate of 94% in their test scenarios. However, differentiating between camera defocus and motion may be unstable if only edge difference information is used. A detection method for camera tampering was also proposed in [5]. In more recent years, a method that uses an adaptive background codebook model was utilized for classifying camera tampering into displacement and obstruction types [6].

In general, camera tampering may indicate that a criminal act might be happening. Detecting abnormalities and triggering alarms to notify operators may thus decrease crime. This study thus develops a system for the rapid detection of camera tampering and various abnormalities in a video surveillance system. To achieve this goal, a computationally efficient method for the rapid detection of various abnormalities, including screen shaking, fogging, color cast, and screen flickering, is proposed. Camera motion, occlusion, and defocus are also detected, which will be compared with existing works.

The rest of this paper is organized as follows. The proposed method for detecting camera tampering and various abnormalities is introduced in Section 2. Experimental results are provided to demonstrate the performance of the proposed method in Section 3. Finally, concluding remarks are given in Section 4.

2. Proposed method

Fig. 1 shows a flowchart of the proposed method for the detection of camera tampering and other abnormalities, including fogging, defocus, color cast, and screen flickering. Screen shaking is first detected to determine whether the input images can be used to build absolute backgrounds. In this work, two backgrounds with a delay of n frames, i.e., B_t and B_{t-n}, are built when video frames are stable; otherwise, the alarm for screen shaking is triggered. Then, the difference between backgrounds B_t and B_{t-n} is evaluated to determine the types of camera tampering and various abnormalities. If the difference between them is larger than a threshold θ_B, camera motion or occlusion is determined; otherwise, fogging, defocus, color cast, or screen flickering is determined. Finally, a background update is carried out to timely respond to changes in the input video frames.

In Section 2.1, the method of detecting screen shaking is described. Background modeling and updating are introduced in Section 2.2 and 2.3, respectively. Then, the method of evaluating the background (i.e., B_t and B_{t-n}) difference is explained in Section 2.4. Finally, the methods of detecting camera motion, occlusion, and other abnormalities, such as fogging, defocus, color cast, and screen flickering, are given in Section 2.5 and 2.6, respectively.

2.1. Detection of screen shaking

Screen shaking is often caused by wind or vibrations from nearby vehicles. Screen shaking makes the absolute background unstable. As shown in Fig. 2(b) and (d), for shaking frames, the number of pixels with larger gray intensities in a frame-difference image is higher than that of pixels whose gray intensities are smaller. However, for stable frames, the number of pixels with smaller gray intensities in a frame-difference image is higher than that of pixels whose gray intensities are larger. Based on this observation,

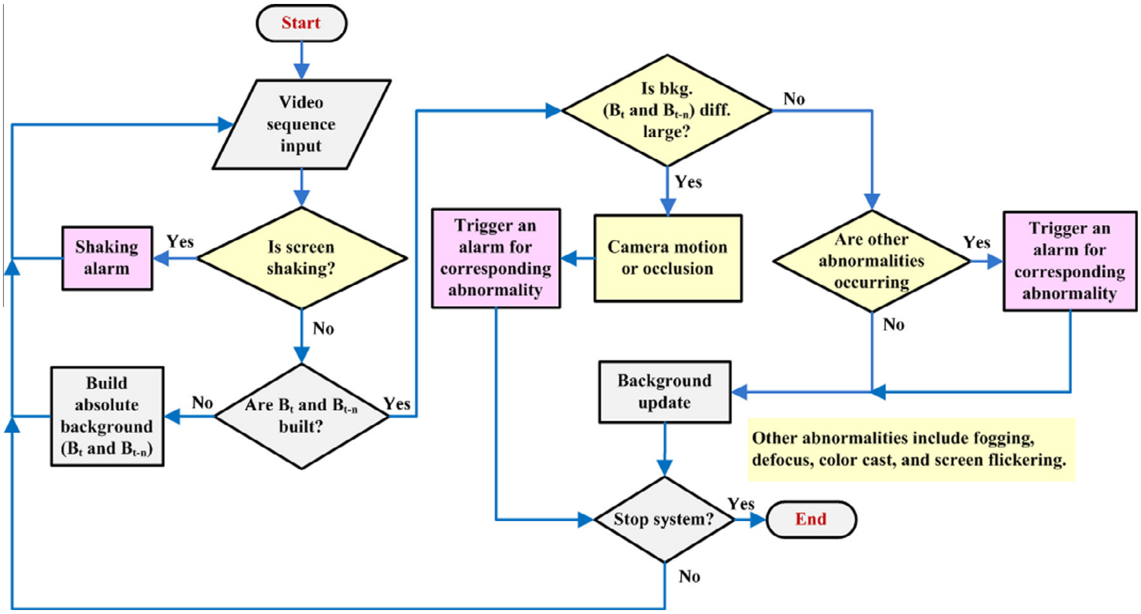
Start
Video sequence input
Is screen shaking?
Yes
Shaking alarm
No
Are B$_t$ and B$_{t-n}$ built?
No
Build absolute background (B$_t$ and B$_{t-n}$)
Yes
Is bkg. (B$_t$ and B$_{t-n}$) diff. large?
Yes
Camera motion or occlusion
Trigger an alarm for corresponding abnormality
No
Are other abnormalities occurring
Yes
Trigger an alarm for corresponding abnormality
No
Background update
Other abnormalities include fogging, defocus, color cast, and screen flickering.
Stop system?
Yes
End
No

Fig. 1. Flowchart of proposed method for the detection of camera tampering and other abnormalities.