IASJ المجلات الاكاديمية العراقية

Tikrit Journal of Pure Science

ISSN: 1813 – 1662 (Print) --- E-ISSN: 2415 – 1726 (Online)

Journal Homepage: http://tjps.tu.edu.iq/index.php/j

Improvement of Alert System against Tampering and Theft in Surveillance Cameras

Furat N. Tawfeeq

National Cancer Research Center, University of Baghdad , Baghdad , Iraq

https://doi.org/10.25130/tjps.v24i2.360

ARTICLE INFO.

Article history:

-Received: 3 / 9 / 2018

-Accepted: 24 / 10 / 2018

-Available online: / / 2019

Keywords: Surveillance camera, Camera tampering, tampering detection, Digital video recorder, system abolition

Corresponding Author:

Name: Furat N. Tawfeeq

E-mail: Furatnidhal@yahoo.com

Tel:

ABSTRACT

Use of Surveillance cameras in houses and markets became common, that resulted to minimize theft and make it a difficult task because it let recording and viewing what is going around. The wide application of these cameras, pushed thieves to seek new ways for abolition of the surveillance system and digital recording of events, such as cutting the signal wire between the camera and Digital video recorder or changing the direction of the camera away from the focus spot or damaging the camera or steal the device which means the loss of the recorded media. This paper focuses on such abolitions and fixed it by suggesting a way to notify the administrator immediately and automatically by Email about any violation of the system using MATLAB, which allow fast action by the administrator to fix such tampering. The results show that selecting of threshold equal to two was fair in detecting motion and value of five, in case of changing the camera direction through testing of fast and slow motions.

Introduction

One of the main problems in camera surveillance system is the detection of camera abolition and tampering, in this situation, the action may be intentional by thieves and should be detected and alerted by the system [1]. The tampering is defined as any disconnection among the three main parts of the surveillance system, (which are cameras, Digital Video Recorder (DVR) and the administrator), and turning the camera away from the area to be monitored (the angle) which assigned previously by the administrator.

Hagui M., et. al. [2] made a comparative study between several algorithms to detect camera tampering and suggests a combination of these algorithms to enhance the detection of a various type of camera tampering. Saglam A. and Temizel A. [3] used the adaptive background subtraction method of video surveillance and monitoring system to detect camera moving, defocusing and covering camera view. Hebbalaguppe R., et. al. [4] suggested a novel effective method detect false alarms caused by spider/spider web using computer vision technique by distinguishing between alarms caused by a spider and those caused by real motion. Veena G.S, et. al. [5] created a smart application for the camera by adding of face recognition based on a principal component analysis. If the object is misplaced, or an unauthorized user is in the extreme vicinity of the object, an alarm signal is raised.

In this paper, any disconnection among these three end-parts will be detected and alerted by email. This approach is based on comparing two sequenced images (frames) in live video stream provided by camera, which will detect any suspicious movements regarding to selected detection threshold, but in case of changing the direction of the camera, the situation is different, here the comparing of the two sequenced frames is not efficient, so instead, the comparison is performed between reference frame k (which will be changed simultaneously) and frame (k+15), this because sometimes the thief try to move the direction of the camera slowly to prevent the system from detecting them, but the approach presented in this paper will set another threshold to accomplish such tampering.

Equation (1) shows how to compare two frames after preparation [6].

$$D_{(x,y)} = I_t(x,y) - I_{t-n}(x,y) > \mathrm{DT} \quad \ldots..(1)$$

Where $D_{(x,y)}$ represents the difference between two frames in pixel(x,y), $I_t(x,y)$ is the intensity of pixel

(x, y) in grayscale, $I_{t-n}(x, y)$ is the intensity of pixel (x, y) according to n in grayscale, DT is the detection threshold and n value defined as in Equation 2.

$$n = \begin{cases} 1, & two\ sequence\ frames, default\ motion\ detection \\ 15, & in\ case\ of\ changing\ the\ direction\ of\ camera \end{cases} \quad \text{.....(2)}$$

Proposed Method

As mentioned before, the tampering according to our system is defined as:

1. Camera tampering
2. The Disconnection between DVR and camera
3. The Disconnection between DVR and user
4. Changing the direction of the camera

All these types of tampering will be discussed later. Basically, the connection in surveillance camera system could be summarized in figure (1).

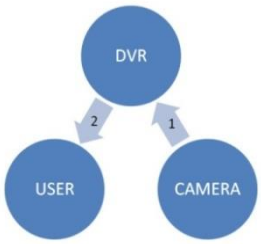

Figure 1: The main parts of surveillance camera system

Figure 1 shows the link 1 and 2, which is the connection between DVR, camera, and user.

In case number one and two, the link one stopped carrying signal or down by a thief, in this approach an email will be sent immediately to the user notifying him that the camera stopped from working properly or the links between the system were damaged, also the email will contain long data and time format of the event. Of course, this action may be intentional sabotage or unintentional. Figure 2 shows the overall algorithm steps, where the inputs are images representing frames recorded by a camera and the outputs are emails if the system detects any suspicious event.

```
01  Start
02  Setting threshold error for normal detection=2 and for camera moving=5
03  Input frame image (n)
04    If      there is no frame
05    Then  send email about disconnection, go to step 15
06    Else
07          image pre-processing (conversion to gray scale & erosion process)
08          find the difference between two successive frames =frame(n) - (n-1)
09           If      difference> threshold error for normal detection
10          Then   send email (suspicious movement)
11          Else
12                  find the difference between the two frames =frame(n) - (n-15)
13                 If      difference> threshold error for camera moving
14                 Then   send email (changing camera angle)
15            get next frame (n+1), go to step 02
16  End
```

Figure 2: The overall algorithm steps

The difference is the dissimilarity between two images, while the threshold error is the criterion between triggering an alarm or not which was selected using try and test to find the optimum values and will be further discuss later in details.

By default, the system will continue sending an email with attached image to the administrator about any suspicious movements, but in some cases, the thief reaches to the DVR and steals it, leads to losing all recorded media, which is case number 3, where the link between DVR and user was down. As in case 1 and 2, an email will be sent to the user telling them that the DVR is power off or damaged.

Turning camera away is another type of tampering (type 4); in this paper, such problem is detected by spatial comparison process. Basically, every video (which in our case is the video recorded by a camera), consists of series of images frames, which are fundamentally the same with each other, the main contrast between them is the status of moving objects [7]. When an unauthorized person changes the angle of the camera to move the focused area away, the default sequenced frames comparison (as shown in figure 3) may be missed, because the comparison takes place between two successive frames, and if intruder try to move the camera slowly, these frames will be very similar to each other; so the alarm will not be triggered. To solve such failure, the dissimilarity will be calculated between two frames away from each other by 15 frames as shown in figure 4, and by this, absolutely it will not be similar regardless of the motion is slow or fast.

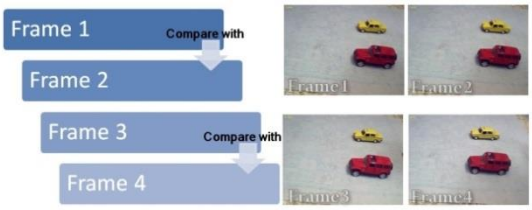

Figure 3: Sequenced of frames comparison in default case

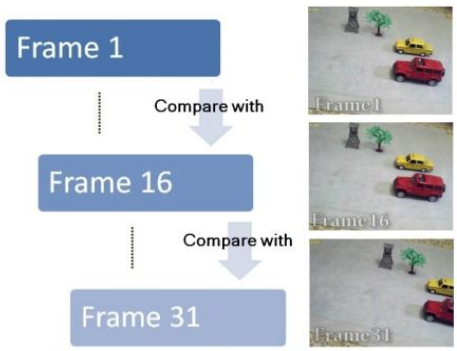

Figure 4: Sequenced of frames comparison in case of a camera moving

Comparison Process

As mentioned before, the dissimilarity takes place between two frames. [6] But first; the frames should be pre-processed to make the comparison more accurate, and this performed by using erosion process. The basic effect is to erode away the boundaries of regions of foreground pixels. Thus areas of foreground pixels shrink in size, and holes within those areas become larger. Grayscale erosion

with a flat disk-shaped structuring element will generally darken the image. Bright regions surrounded by dark regions shrink in size, and dark regions surrounded by bright regions grow in size. Small bright spots in images will disappear as they are eroded away down to the surrounding intensity value, and small dark spots will become larger spots. [8] The pre-processing stages are shown in the overview of the system in figure 5.

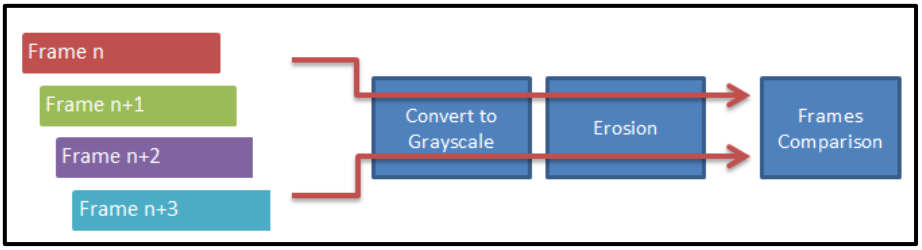

Figure 5: Frame pre-processing

Setting Detection Threshold

The detection threshold of the frames comparison should be set to a proper value to ensure minimum error and right movement detection. Setting high value will lead to reducing error in detection but may neglect many real motions, on the other hand, small value detect all movements but with some false alarms. Hints, a trade-off between false alarms and missing events should be considered. A group of tested values will be examined, but the presented values that will display in the experimental results are selected and near to the proper value.

Experiment Results

As mentioned previously, every frame will convert to a grayscale, and then compare with the next frame, if the value of pixel intensity in the first frame is not equal to the intensity of pixel for the next frame in the same location (x,y), then this leads to a dissimilarity. The counter of this dissimilarity divided by the total number of pixels in a frame will generate the differences between frames.

In this paper, two values of threshold were calculated (for successive frames and moving camera detection) in different illumination cases and events.

For normal detection, six threshold values were tested to find the optimum one, and the percentage of true alarms, false alarms, and missed events were recorded for each case, as shown in Table 1. Every recorded alarm means that the frame error is greater than the selected threshold as mentioned previously in equation 1 and 2, where n=1.

Table 1: Results of different values of threshold in the normal detection process

Thresholds	% of True Alarms	% of False Alarms	% of Missed Events
0.5	20	70	10
1	50	40	10
1.5	60	20	20
2	70	10	20
2.5	60	0	40
3	50	0	50

The true alarm indicates that there is a real event occurred during surveillance and detected by the system correctly or what we call it true positive (TP) and true negative (TN), the false alarm indicates that there is no event required to assign it but the system considered it as a suspicious movement or by other words false negative (FN), while missed event represents the system failure from detecting a real event that should be alarmed or what we call it false positive (FP). Figure 6 shows the relationship between threshold values and percentage of true, false alarms and missed events in the normal detection process.

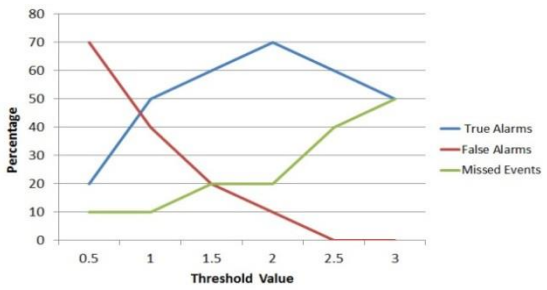

Figure 6: The relationship between threshold values and percentage of true, false alarms and missed events in the normal detection process

According to the results shown in Table 1 and Figure 6, we can easily notice that when threshold value increase, the percentage of false alarm decrease, and percentage of missed events increase also. This occurs because of many real events will passed by the system due to selecting high threshold as shown previously in equation one. The accuracy were calculated which is in our case is the ability to differentiate the occurrence of events and the absences. The accuracy of each threshold taken from table 1 is equal to percentage of true alarms mentioned before, because the equation of accuracy will divides the correctness of alarms by the total number of cases as shown below:

$Accuracy = (TP + TN)/(TP + TN + FP + FN)$ ….(3)

Also the sensitivity was calculated which is in our case, the ability to determine the suspicious events correctly and specificity which is the ability to determine the absence of events correctly, the equations of the two above standards are shown below:

$Sensitivity = TP/(TP + FN)$ ….(4)

$Specificity = TN/(TN + FP)$ ….(5)

Now from table one, we can calculate accuracy, sensitivity and specificity to find the optimum value of the threshold, from table two we can assign two as the optimum threshold, where there is a balance between the number of true alarms, false alarms, missed events, accuracy, sensitivity and specificity.

Table 2: Accuracy, sensitivity and specificity of different values of threshold in the normal detection process

Thresholds	Accuracy	Sensitivity	Specificity
0.5	20	22.2	66.6
1	50	55.5	83.3
1.5	60	75	75
2	**70**	**87.5**	**77.7**
2.5	60	100	60
3	50	100	50

As mentioned before, detection of changing camera direction has a different way of comparison in our paper. Again, another set of thresholds were examined to find an accurate detection threshold.
Five thresholds were tested, also the percentage of true alarms, false alarms, and missed events were calculated for each threshold as shown in Table 3. The changing of camera direction was applied in slow and fast motion. Every recorded alarm means that the frame error is greater than the selected threshold as mentioned previously in equation 1 and 2, where here n=15.

Table 3: Results of different values of threshold in case of changing the camera direction

Thresholds	Motion	% of True Alarms	% of False Alarms	% of Missed Events
3	slow	50	30	20
	fast	65	20	15
4	slow	73	10	17
	fast	85	10	5
5	slow	98	1	1
	fast	99	0	1
6	slow	85	7	8
	fast	92	4	4
7	slow	63	2	35
	fast	77	3	20

Motion refers to the speed of changing the direction or the angle of the camera, here, true alarm indicates that there is a real changing in camera direction and detected by the system correctly or there is no changing in direction and the system did not triggered as changing (TP and TN), false alarm indicates that there is no changing in camera direction but the system considered it as a changing (FN), while missed event represents the system failure from detecting a real changing in camera direction (FP). Figure 7 and 8 shows the relation between threshold values and percentage of true, false alarms and missed events for slow and fast motion respectively in case of changing the camera direction.

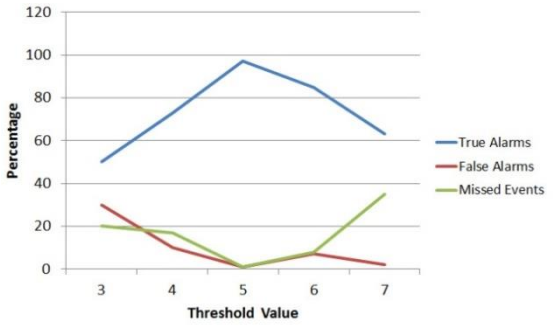

Figure 7: The relationship between threshold values and percentage of true, false alarms and missed events in case of changing the camera direction slowly

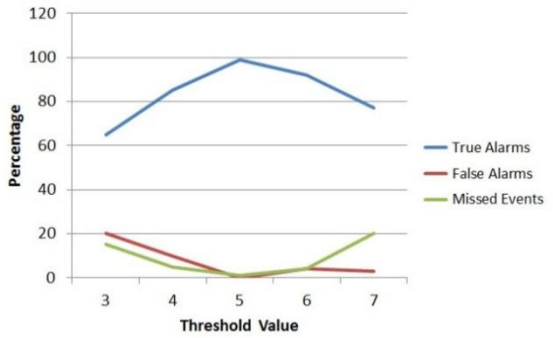

Figure 8: The relationship between threshold values and percentage of true, false alarms and missed events in case of fast changing in camera direction.

As shown in Table 3, Figure 7 and 8; when threshold value equal to three, too many numbers of false alarms were recorded, because many little movements considered as camera moving. Increasing the threshold values will decrease the number of false alarms but at the expense of missed events.
Again, we calculate the accuracy, sensitivity and specificity for each threshold value and motion speed to find the optimum one as shown in table four.

Table 4: Accuracy, sensitivity and specificity of different values of threshold in case of changing the camera direction

Thresholds	Motion	Accuracy	Sensitivity	Specificity
3	slow	50	62.5	71.4
	fast	65	76.4	81.2
4	slow	73	87.9	81.1
	fast	85	89.4	94.4
5	**slow**	**98**	**98.9**	**98.9**
	fast	**99**	**100**	**99**
6	slow	85	92.3	91.3
	fast	92	95.8	95.8
7	slow	63	96.9	64.2
	fast	77	96.2	79.3

The value of five gave an accurate percentage of true and false alarms and missed events. Additional to varying the threshold value, slow and fast motion in changing the direction of camera playing a great role, because if the motion is slow, then the threshold in some cases will not detect it due to small differences between sequenced frames, for this reason, one can easily notice for table 4 that slow-motion recorded higher percentage of missed events comparing with fast motion.

From table four, we can assign five as the optimum threshold, where there is a balance between the number of true alarms, false alarms, missed events, accuracy, sensitivity and specificity.

Figure 9 and 10 show the final outputs which are emails send by the system to the administrator to alarm him that there is a suspicious movement or changing in camera direction respectively, the emails contain the time of event with an attached image clarify the situation.

Figure 9: An example of an email that notifies a suspicious movement

Figure 10: An example of an email that notifies camera moving

Conclusion

In this paper, an enhancement of camera tempering detection was proposed, where tempering was defined as any disconnection between system parts or changing the direction of the camera. The results found a good tempering threshold that improves the system performance through detecting real motions, also highlight the importance to assign another threshold to detect camera moving. An email is an excellent way that notifies the user in case of camera tempering immediately.

References

[1] Ribnick, E.; Atev, S.; Masoud, O.; Papanikolopoulos, N. and Voyles, R. (2006). Real-Time Detection of Camera Tampering. AVSS '06. IEEE International Conference on Video and Signal Based Surveillance, IEEE, Nov. 2006.

[2] Hagui, M.; Boukhris A. and Mahjoub, M.A. (2016). Comparative study and enhancement of Camera Tampering Detection algorithms. 13th International Conference Computer Graphics, Imaging and Visualization, IEEE 2016: p. 226-231.

[3] Saglam, A. and Temizel, A. (2009). Real-time Adaptive Camera Tamper Detection for Video Surveillance. Conference paper: Advanced Video and Signal Based Surveillance, Sep. 2009: p. 430-435.

[4] Hebbalaguppe, R. et al. (2016). REDUCTION OF FALSE ALARMS TRIGGERED BY SPIDERS/COBWEBS IN SURVEILLANCE CAMERA NETWORKS. IEEE International Conference on Image Processing (ICIP) August 2016.

[5] Veena G.S.; Chandrika P. and Khaleel K. (2013). AUTOMATIC THEFT SECURITY SYSTEM (SMART SURVEILLANCE CAMERA). Computer Science & Information Technology (CS & IT), Natarajan Meghanathan et al. (Eds): ITCSE, ICDIP, ICAIT 2013: 75–87.

[6] Tawfeeq, F.N. (2013). Real Time Motion Detection in Surveillance Camera Using MATLAB. *International Journal of Advanced Research in Computer Science and Software Engineering*, **3 (9)**:622-626.

[7] Yao, Y.; Shi, Y.; Weng, S. and Guan, B. (2018). Deep Learning for Detection of Object-Based Forgery in Advanced Video. *symmetry*, **10 (3)**, doi:10.3390/sym10010003.

[8] Gonzalez, R.C. and Woods, R.E. (2006). Digital Image Processing. 3rdedn., Pearson Education International.

تطوير نظام الانذار في كاميرات المراقبة ضد عمليات التخريب والسرقة

فرات نضال توفيق

المركز الوطني الريادي لبحوث السرطان ، جامعة بغداد ، بغداد ، العراق

الملخص

ان استخدام كاميرات المراقبة في المنازل والمحال التجارية قد اصبح امراً شائعاً، وقد ادى الى تناقص عمليات السرقة وجعلها بالغة الصعوبة من خلال عمليات التسجيل والمراقبة، ان التطبيقات الواسعة لهذه الكاميرات قد اجبرت اللصوص على اللجوء الى طرق جديدة لايقاف التوثيق الرقمي للاحداث، مثال ذلك هو اللجوء الى قطع التوصيلات الممتدة بين الكاميرات وجهاز التسجيل الفديوي او ازاحة اتجاه الكاميرة بعيداً عن مركز العمل او اتلاف الكاميرات او سرقة جهاز التسجيل الفديوي والذي يؤدي الى فقدان المادة المسجلة. تم التركيز في هذا البحث على مثل هكذا عمليات تخريب وكيفية تجاوزه من خلال اقتراح طريقة لاشعار الشخص المسؤول عن المراقبة بصورة فورية وتلقائية بواسطة البريد الالكتروني حول أي اختراق للنظام باستخدام المحاكي MATLAB والتي تتيح للشخص المسؤول العلم الفوري لاصلاح مثل هكذا تخريب. اضهرت النتائج ان اختيار الحد اثنان كان مناسباً لكشف عمليات التسلسل للمنطقة المراقبة والحد خمسة بالنسبة لكشف تحريك الكاميرا اوابعادها عن المنطقة المراد مراقبتها من خلال التجريب على الحركة البطيئة والسريعة.