A Signal Detection Theory Approach for Camera Tamper Detection

Pranav Mantini
Department of Computer Science
University of Houston
pmantini@cs.uh.edu

Shishir K. Shah
Department of Computer Science
University of Houston
sshah@central.uh.edu

Abstract

Camera tamper detection is the ability to detect faults and operational failures in video surveillance cameras by analyzing the video. Researchers have increasingly focused on such techniques attributing to the ubiquitous deployment of large scale surveillance systems. In this paper, a signal detection theory approach is proposed to quantitatively analyze the information being captured by the camera and to detect tampers. Signal activity is used as a feature to measure the amount of information in the image. The distribution of features representing the normal operation of a camera are modeled as a Gaussian mixture model (GMM). The GMM is trained using synthetic data. To reduce the effects of noise, a Kalman filter is used to model changes in signal activity in the video. Experimental results show that the proposed approach out performed the state-of-the-art [13] in detecting tampered images with higher accuracy while generating lower false alarms.

1. Introduction

Surveillance cameras have become an integral part of public and private infrastructures in recent years. The availability of cheap sensors along with their numerous security benefits have contributed to the deployment of large scale surveillance systems. Systems ranging from hundreds of cameras at a school to thousands of cameras at an airport is a common configuration size. Surveillance systems are typically deployed over a large physical area with a centralized control point. Such wide distributions often require rigorous maintenance and continual review processes to ensure that each camera within the system is functioning as required. Reviewing thousands of cameras manually to ensure functionality is a tedious task and prone to human error. Moreover, high-level computer vision algorithms like tracking [17], re-identification [18] and motion prediction [16, 19] are designed with an implicit assumption of properly functioning cameras. Non-functionalities in cameras generally lead to erroneous results in these high-level algorithms. Hence, automatic camera tamper detection is a critical low-level task to ensure uninterrupted operation of surveillance systems and to ensure public safety.

Camera tamper detection can be defined as persistent deviation in the image quality or expected scene information captured by a camera's video. Such deviations could be a result of natural events (like strong winds in outdoor cameras) or due to intentional malicious activity (like a perpetrator changing the view of the camera). Camera tampers in existing literature has typically been classified as: a) Covered, b) Defocused and c) Moved. Covered tamper occurs when the view of the camera is blocked using an opaque object. Defocused tamper occurs when a camera lens is out of focus resulting in a blurred image. Finally moved tamper occurs when the viewing direction of the camera is changed.

We propose a signal detection theory approach for camera tamper detection. A signal is a function that conveys information about the behavior and attributes of some phenomenon [20]. We leverage the idea that a properly functioning camera captures a certain amount of discernible and useful information. A tamper alert can be triggered when there is a considerable decrease or change in the amount of information being captured. In most cases of a covered tamper, certain region of pixels change to uniform intensity, and in defocused tampers, the pixel representation is blurred and the individual objects cannot be discerned. In either case, a sharp decrease in the amount of information captured is noticed. In most cases of a moved tamper, there is a persistent change in the characteristics of the information being captured. We leverage these variation for detecting tamper in cameras. The contributions of this paper can be summarized as:

1. Using **signal activity** [31] as a feature to represent the measure of information in an image and estimate it using Kalman filtering.
2. Modeling the distribution of signal activity of normal operating view of the camera as a **Gaussian mixture model** trained over synthetic images.
3. A **signal detection theory approach** for camera tamper detection.

2. Related Work

Camera tamper detection techniques have gained a fair share of attention over the last decade [13, 12, 25, 5]. It can be considered as a sub problem of video change detection, where the objective is to detect changes in the scene as video progresses. More recently with the ubiquitous deployment of low cost cameras for surveillance, research has been dedicated for robust automatic detection of camera tampers.

Existing literature has classified camera tampers under three categories [7]: a) Covered, b) Defocused, and c) Moved. Majority of the solutions proposed to detect camera tamper, have addressed each of the tampers individually, while very few have developed a unified algorithm to detect all three tampers at the same time. Unified tamper detection algorithms can have considerably low complexity at the expense of the inability to classify the type of tamper. Independent tamper detection algorithms are designed to detect each individual tamper. However, the algorithms might have common preprocessing and training stages. The choice of one over the other can be driven by the application and computational resources available. In this paper, we propose a unified approach for camera tamper detection.

Taking inspiration from research in image quality assessment, Wang *et al.* [30] categorized tamper detection methods as full-reference, reduced-reference and no-reference techniques. Full-reference methods usually assume that a normal (untampered) image of the camera is available and can be used to perform a pixel-wise comparison. The difference between the reference image and incoming image is assessed to detect tampers. Reduced-reference techniques map images into a lower dimension feature space and learns a model representation for normal operating view of the camera. An estimate of the likeliness of the incoming image belonging to the learned reference model is used to detect tampers. Finally, no-reference techniques do not have a reference image or model to compare with. An inference is made based on the characteristics of incoming video frames. In this paper, we propose a reduced reference method for camera tamper detection.

Covered tamper detection algorithms in general identify the stable regions in an image and constantly checks for loss in density or distribution in these regions due to occlusions. Some methods have chosen to model the background to establish stable regions. In order to compute or identify large deviation, Jimenez *et al.* [7] and Ellwart *et al.* [4] computed the entropy and compared it to the incoming frames. Another common approach is to compute the histogram of the background [2, 23, 14, 26, 1] and compare it to the incoming image. Tung *et al.* computed a codebook model for the background for covered tamper detection [27]. Some methods have proposed to compute key point features like Scale Invariant Feature Transform (SIFT) [33, 15] and Speeded Up Robust Features (SURF) [9] and track changes amongst these points to detect covered tamper. Wang *et al.* [30, 29] proposed a set of reduced-reference features, namely pixel based edge entropy for covered tamper detection. While no-reference methods are not so common, Jiao *et al.* [10] proposed an application specific method to detect occlusions from banners using corner detection and line fitting techniques.

Defocused tamper detection methods can also be organized under full, reduced and no-reference techniques. Distinct edges and corners are the most commonly used indicators to detect defocussing. Defocussing results in a degradation of the edge content. Key features extracted include stable edges [15] and SURF [9] features, which are used as a reference to detect defocussing. Another common method is to conduct an analysis in the frequency domain. A degradation in the edges would result in a loss of high frequency components. Image transformations like Fourier transform [23], discrete cosine transform [1], and wavelet transform [2] are used to analyze edge details. Gaiboti *et al.* [5] used average norm of the gradient as a measure to detect defocussing. Wang *et al.* [30, 29] proposed a reduced-reference technique for covered tamper detection which was also used for detecting defocused tampers. Ganguli *et al.* [6] proposed a no-reference technique for defocused tamper detection using a blur metric that quantifies the extent of blurring.

Moved tamper detection methods can also be organized similar to the other two tamper detection methods. Most methods have leveraged a form of image spatial matching algorithm to estimate translations so as to detect moved tampers. Commonly used algorithms include block matching, background pixel matching and static object matching. Saglem *et al.* [23] proposed a method using corresponding pixel matching. If the number of matching pixels between the reference and incoming image falls below a threshold, a moved tampers is detected. Block matching between the reference frame and incoming frame was conducted to detect large displacements [8, 7, 4, 14, 1] and histogram difference was used as a measure to detect moved tampers. Spatial location of static objects was also used as a reference to detect moved tampers. Raghavan *et al.* [21] used traffic signals as static objects for detecting moved tampers in traffic cameras.

As this paper proposes a unified method for camera tamper detection, we review these methods in detail. Ribnik *et al.* [22] proposed a unified method by measuring dissimilarity between the reference and incoming images. Three different measures were calculated (histogram chromaticity, histogram L1R difference and histogram gradient). These dissimilarity measures were individually thresholded to detect tampers. Shih *et al.* [24] proposed a two stage scene matching algorithm for tamper detection. The first stage is used to detect tampers and the second stage to reduce false

alarms. Stable edges were obtained using Sobel operator and Otsu's voting method by counting the frequency of the edge points. The obtained stable edge pixels were modeled as a GMM. The portion of non-background points are measured, and later thresholded to detect tampers. Lee *et al.* [13] proposed a unified tamper detection approach based on edge information. Tamper events were detected by measuring the difference between the edges of background and current frame. The background frame was generated using a GMM and the edges were extracted using Canny edge detector. Edge change rate of the current frame compared to the background is used as a measure. The average change rate computed over a series of frames was thresholded to detect a tamper. Lee *et al.* [12] later used a similar approach by quantifying the edge disappearance rate. However, they accounted for the foreground objects and excluded them from the edge comparison for robust detection.

Our proposed approach is a reduced-reference unified method for camera tamper detection. Images are discretized 2D signals, and we take inspiration from signal detection theory to model the characteristics of the image. We propose to use signal activity as a measure of information in the image. Signal activity is a image quality measure that can quantify the extent and type of image degradation and correlates closely with human perception of image quality. Objective image quality measures that are consistent with perceptual image quality can reliably predict perceived quality. Many objective image quality measures have been proposed [3]. We build on the signal activity measure proposed in [31]. Camera tamper detection techniques suffer heavily from false positives. Most literature has identified false positives to arise from either sudden illumination changes or due to a large object passing in front of the camera. Ribnick *et al.* [22] showed that 80% of the false alarms were a result of sudden illumination changes in their dataset. This can be attributed to the sudden change in measurement that occur in the two scenarios. Existing work has handled these using temporal suppression in the post processing stages [2, 23]. We propose to use Kalman filter to estimate signal activity to reduce false alarms due to illumination changes.

3. Framework

Figure 1 describes the framework for proposed camera tamper detection approach. The process involves two stages beginning with a training phase and then followed by a detection phase. The training phase captures a reference model to represent the view of the normal operation (not tampered) of the camera. The training phase begins by generating synthetic data that is required for training. The synthesis captures variations in the view of the camera due to illumination changes, which otherwise are tedious to collect manually. The feature extraction phase captures the characteristics of the training images in a reduced feature space.

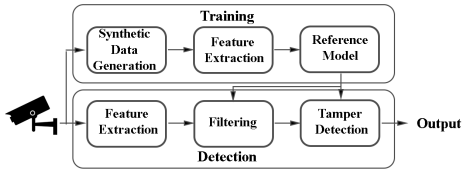

Figure 1. Camera Tamper Detection Framework

Then a reference model is created using the features to represent the normal operating view of camera. The second phase leverages the reference model from the training phase to detect tamper in the incoming images from the camera. The images from the camera are transformed to the lower feature space similar to the one in training phase. The reference model is leveraged to initialize a filter. The features undergo filtering to reduce the effects of noise due to illumination changes. Finally in the tamper detection step, the estimated features using the filter are compared to the reference model to detect tampers.

4. Methodology

4.1. Problem Formulation

We propose a **signal detection theory** approach for camera tamper detection. In the field of electronics, signal detection theory is a means to quantify the ability to discern information bearing patterns from random patterns that distract from the signal [32]. Images obtained from the camera is a signal representing the information being captured. Normal images (not-tampered images) can be considered as information bearing patterns and tampered images (covered, blocked and moved) can be considered as random and noise induced patterns in signals. Let y be an observation of the signal, a representation of the amount of information in the image. Let H_{tamp} be the hypothesis that the observation y is tampered and H_{nor} that the image is normal. Following a Maximum-a-Posterior approach, H_{nor} is chosen if $p(H_{nor}|y) > p(H_{tamp}|y)$ and H_{tamp} is chosen otherwise, where $p(.)$ is a probability function. Using Bayes' theorem, the posteriors can be expressed as:

$$\begin{aligned} \frac{p(y|H_{nor})p(H_{nor})}{p(y)} &> \frac{p(y|H_{tamp})p(H_{tamp})}{p(y)} \\ \implies p(y|H_{nor})\pi_{nor} &> p(y|H_{tamp})\pi_{tamp} \end{aligned} \tag{1}$$

where $p(y|H_i), i = \{nor, tamp\}$ are the likelihood probabilities and π_i are the priors. $p(y) = \Sigma_i p(y|H_i)p(H_i)$ is the total probability of the observation y. Assuming that the image belongs to one of the two hypothesis we have $p(y|H_{nor}) = 1 - p(y|H_{tamp})$, therefore

$$\begin{aligned} p(y|H_{nor})\pi_{nor} > (1-p(y|H_{nor}))\pi_{tamp} \implies \\ p(y|H_{nor}) > \frac{\pi_{tamp}}{\pi_{nor}+\pi_{tamp}} \implies \ln p(y|H_{nor}) > \delta. \end{aligned} \tag{2}$$

We define an image y to be normal if the log likelihood, $\ln p(y|H_{nor})$, is above a threshold δ, or alternatively to be tampered if it falls below the threshold. In the following subsection 4.2, we describe **signal activity** as a measure of information in the image. We describe our approach to learn a reduced reference likelihood model for $p(y|H_{nor})$, representing the normal operating view of a camera. We describe our method for estimating signal activity of an incoming image and detecting tampers.

4.2. Proposed Methods

Feature Extraction {Signal Activity as a Measure of Information in the Image}: We represent the information in the image using **Signal Activity** as defined in [31]. If the image is represented by $I(i,j)$, where i,j denotes a particular pixel position, then signal activity is given by $A = \frac{A_h + A_v}{2}$: where,

$$A_h = \frac{1}{m(n-1)} \sum_{i=1}^{m} \sum_{j=1}^{n-1} |d_h(i,j)|$$
$$A_v = \frac{1}{(m-1)n} \sum_{i=1}^{m-1} \sum_{j=1}^{n} |d_v(i,j)| \quad (3)$$

where, $d_h = I(i,j+1) - I(i,j)$, and $d_v = I(i+1,j) - I(i,j)$. Signal Activity can be computed over the entire image or sub regions of the image. An image I can be represented in a reduced feature space $Y_I = \{A_I^1, ...A_I^n\}$ where A_I^n is the signal activity of the region n in image I.

Filtering {Estimating Signal Activty using Kalman Filter:}: We propose to use linear quadratic estimator like the Kalman filter to estimate signal activity of the images over time for a robust representation of the scenario. Let $X_{t-1} = \{A_{t-1}\}$ be the internal state of the image, where A_{t-1} is the signal activity. The signal activity is estimated recursively as a prediction and correction step using Kalman filter. Let the estimated signal activity of an image or region I at time $t-1$ be $\hat{X}_{t-1}$. An estimate of signal activity for next step $\hat{X}_t$ is estimated using Kalman filter as:

$$Predict - step:$$
$$\hat{X}_{t|t1} = F_t \hat{X}_{t1|t1} + B_t u_t$$
$$P_{t|t1} = F_t P_{t1|t1} F_t^T + Q_t$$
$$Correct - step: \quad (4)$$
$$\hat{X}_{t|t} = \hat{X}_{t|t1} + K_t(y_t H_t \hat{X}_{t|t1}$$
$$K_t = P_{t|t1} H_t^T (H_t P_{t|t1} H_t^T + R_t)^{-1}$$
$$P_{t|t} = (I K_t H_t) P_{t|t1}$$

Where, $\hat{X}$ is the estimated state, F is the state transition matrix (i.e., transition between states), u are the control variables, B is the control matrix (i.e., mapping control to state variables), P is the state variance matrix (i.e., error of estimation), Q is the process variance matrix (i.e., error due to process), y is the measurement variables, H is the measurement matrix (i.e., mapping measurements onto state), K is the Kalman gain, and R is the measurement variance matrix (i.e., error from measurements). The subscripts $t|t$ is the current time period, $t1|t1$ is the previous time period, and $t|t1$ are intermediate steps. Kalman filter provides a robust estimate of the signal activity for the images being captured by the camera.

Reference Model{Modeling Likelihood Probabilities as a Mixture of Gaussian:}: The distribution of signal activity is modeled as a GMM. The likelihood, $p(y|H_i) = \sum_{j=0}^{n} \omega_i^j \eta_i^j(\mu_i^j, \sigma_i^j)$, where $\eta(\mu_i^j, \sigma_i^j)$ represents Gaussian distributions corresponding to different scenarios. In case of H_{nor}, $\{\eta_{nor}^1, \eta_{nor}^2 ...\}$ corresponds to different naturally occurring illumination variations like day, night and overcast sky among normal images and ω_i^j are the weights corresponding to each scenario such that $\sum_j \omega_i^j = 1$.

Tamper Detection{Abnormality Detection using a Moving Average of Log-Likelihood:}: One could follow a simplistic approach and detect tampers using the estimated value from the Kalman filter. A tamper could be detected if $\hat{X}_t \pm \sigma$ does not fall within a confidence interval. However, this simple approach could result in a large number of false positives. We follow a similar approach to Knorn *et al.* [11] by thresholding a moving average of log-likelihood of the estimated values over time. The likelihood of an estimated value $\hat{X}_t$ can be readily calculated as $p(\hat{X}_t|H_{nor}) = \sum_{j=0}^{n} \omega_{nor}^j \eta_{nor}^j(\mu_{nor}^j, \sigma_{nor}^j)$. Similar to [11], we use a moving average (or low pass) filter on the log likelihoods of past measurements. This can provide a significantly robust tamper detector.

$$z_t = \alpha_z z_{t-1} + (1 - \alpha_z) \log p(\hat{X}_t|H_{nor}) \quad (5)$$

Where, α_z is a smoothing factor. A suitable threshold for z_t is used to detect tamper at step t.

5. Experiments

5.1. Implementation

Synthetic Data Generation{Learning Model Parameters from Synthetically Generated Image Variants:}: Parameter estimation of the likelihood distributions require a dataset consisting of samples representing natural illumination variations in $p(y|H_{nor})$. Capturing such variations from actual observations is a time consuming and arduous task. We propose to initially model these variations synthetically from a limited number of observations of a normal image. Natural illumination variations were modeled by inducing variation in the brightness and contrast of the image (Figure 2). The illumination varied images ($I^{'}$) were created from the original image (I) by applying linear transformations ($I^{'} = \alpha * I + \beta$). To induce contrast variations $\alpha = \{.75, .80, .85, .90, .95, 1., 1.05, 1.1, 1.15, 1.2, 1.25\}$

values were used, and to induce brightness variations $\beta = \{-60, -40, -20, 0, 20, 40, 60\}$ were used.

These image variants were used to estimate the parameters for the Gaussians $\eta_{nor}(\mu_{nor}, \sigma_{nor})$, where $\mu_{nor} = mean(A(I'))$ and $\sigma_{nor} = stdev(A(I'))$, where I' were the synthetic images generated for the natural illumination variants and $A(I')$ was the signal activity of image I'.

(a) (b) (c)

Figure 2. Synthetic image variants (a) normal image; (b) brightness intensity lowered by 60; (c) contrast increased by 0.25.

Kalman Filter{Implementation Details:} A static Kalman filter model was used to estimate signal activity. Therefore, we have $x_{t+1} = x_t$, and signal activity ($A = 0$) and $F_t = 1$, for any $t \geq 0$. Control variables B and u were not used. The computed signal activity was used as a measurement $y_t = A_t$. Kalman Filter was initialized using the mean(μ_{nor}) of the sufficient statistics calculated using synthetically generated images. The estimated error was initialized to σ_{nor}.

Tamper Detection{Implementation Details:} The image was subdivided into a $3X2$ grid and signal activity was calculated for each region. A Kalman filter was initialized for each region and the signal activities were estimated individually. The threshold δ was set to $ln(0.1)$, i.e. a tamper was detected if the $p(y|H_{nor}) < 0.1$. If for at least three regions z_t fell below the threshold (δ) simultaneously, a tamper was detected at t.

5.2. Evaluations

Two sets of real world video data are used in the evaluation of the proposed camera tamper detection approach.

Change Detection Dataset [28]: This dataset is aimed at understanding the performance with respect to a variety of scenarios that are likely to generate false positives. This dataset does not contain any tampered images. We use the change detection dataset [28] that represent a wide variety of scenarios that are ambiguous and more likely to generate false positives. The algorithm is evaluated over hundred thousand frames consisting of scenarios from bad weather, night video, turbulence, baseline, and others.

Surveillance Video Dataset: This dataset is aimed at understanding the performance with respect to tampered images and the detection of true positives. This dataset is captured from various indoor and outdoor surveillance cameras located within our infrastructure. Covered tamper is created by blocking the camera view with a rigid object. Defocused tamper is obtained from cameras that have naturally gone out of focus over time. Scenarios include day and night videos from outdoor cameras and over-saturated images due to sunlight. A total of 25,000 frames consisting of 9,500 tampered images were used in the evaluation.

Dataset	Lee *et al.* [13]		Proposed	
	Accuracy	FPR	Accuracy	FPR
Bad weather	0.3910	0.6089	0.9932	0.0067
Baseline	0.3436	0.6563	0.6539	0.3460
Camera Jitter	0.4917	0.5082	0.7685	0.2314
Dynamic Background	0.9226	0.0773	0.9107	0.0892
Intermittent Object Motion	0.3619	0.6380	0.8464	0.1535
Low Frame rate	0.4034	0.5965	0.6577	0.3422
Night Videos	0.5197	0.4802	0.9902	0.0097
Shadow	0.4310	0.5689	0.8899	0.1100
Turbulence	0.4096	0.5903	0.8064	0.1935
Average	0.4936	0.5063	0.8532	0.1467

Table 1. Change detection dataset

Dataset	Lee *et al.* [13]			Proposed		
	Accuracy	TPR	FPR	Accuracy	TPR	FPR
Covered	0.5266	0.7201	0.4764	0.9003	0.7236	0.0329
Defocused	0.7378	0.5550	0.1541	0.7338	0.7249	0.0
Moved	0.5077	0.4985	0.4727	0.6447	0.7202	0.5082
Average	0.5735	0.6096	0.3947	0.7789	0.7299	0.1732

Table 2. Video surveillance dataset

The proposed method is evaluated and compared against the state-of-the-art unified tamper detection method proposed in [13]. Accuracy ($\frac{TP+TN}{TP+FP+TN+FN}$), true positive rate ($TPR = \frac{TP}{TP+FN}$) and false positive rate ($FPR = \frac{FP}{FP+TN}$) are measured to compare the performance of the two methods, where TP are true positives, FP are false positives, TN are true negatives and FN are false negatives. TPR is not measured for the change detection dataset as it does not have any tampered images.

The evaluation results for change detection dataset are shown in table 1 and the evaluation results for surveillance dataset are shown in table 2. With respect to change detection dataset, the proposed method out performed [13] in all the scenarios except for dynamic background. Lee *et al.* [13] performed with higher accuracy in scenarios with dynamic background. The proposed method performed slightly poorly in scenarios with low frame rate. Overall the proposed method generated 15% false positive as opposed to [13], which produced 50% false alarms. With respect to video surveillance dataset, the proposed method detected all three types of tampers with a higher accuracy while generating considerably low false alarms. The proposed method detected covered tampers with 90% accuracy, followed by defocused tampers with 73% accuracy and finally moved tampers with 65% accuracy . However, [13] generated lower false alarms with respect to moved tampers than the proposed method. Overall with respect to video surveillance dataset, the proposed method generated 17% false positive as opposed to [13], which produced 40% false alarms.

6. Conclusion

We have proposed a signal detection theory approach for detecting tampers in video surveillance cameras. Signal activity was used as a feature to measure the amount of information in the image. The distribution of signal activity representing the normal operation of a camera were

modeled as a Gaussian mixture model, and trained using synthetically generated data. A Kalman filter was used to estimate the signal activity of the images, to reduce the effects of sudden illumination changes. We have compared the proposed method with state-of-the-art unified tamper detection method [13] over a change detection dataset and a video surveillance dataset. Experimental results show that the proposed approach out performed the state-of-the-art in detecting tampered images with higher accuracy while generating lower false alarms.

References

[1] Rapid detection of camera tampering and abnormal disturbance for video surveillance system. *Jour. of Visual Communication and Image Representation*, 2014.

[2] A. Aksay, A. Temizel, and A. E. Cetin. Camera tamper detection using wavelet analysis for video surveillance. In *2007 IEEE Conf. on Adv. Video and Signal Based Surveillance*.

[3] I. Avcibas, B. Sankur, and K. Sayood. Statistical evaluation of image quality measures. *Jour. of Electronic Imaging*, 2002.

[4] D. Ellwart, P. Szczuko, and A. Czyżewski. *Camera Sabotage Detection for Surveillance Systems*.

[5] A. Gaibotti, C. Marchisio, A. Sentinelli, and G. Boracchi. *Tampering Detection in Low-Power Smart Cameras*.

[6] A. Ganguli, A. Raghavan, V. Kozitsky, and A. Burry. Automated fault detection in violation enforcement cameras within electronic toll collection systems. In *ITSC 2013*.

[7] P. Gil-Jiménez, R. López-Sastre, P. Siegmann, J. Acevedo-Rodríguez, and S. Maldonado-Bascón. *Automatic Control of Video Surveillance Camera Sabotage*.

[8] S. Harasse, L. Bonnaud, A. Caplier, and M. Desvignes. Automated camera dysfunctions detection. In *6th IEEE Southwest Symp. on Image Analysis and Interpretation, 2004.*

[9] M. S. Javadi, Z. Kadim, H. H. Woon, M. J. Khairunnisa, and N. Samudin. Video stabilization and tampering detection for surveillance systems using homography. In *I4CT 2015*.

[10] Y. Jiao, L. Chen, X. Xu, and J. Tian. Banner occlusion detection in security surveillance video. In *ICSPCC '15*.

[11] F. Knorn and D. J. Leith. Adaptive kalman filtering for anomaly detection in software appliances. In *IEEE INFOCOM Workshops '08*.

[12] G.-b. Lee, M.-j. Lee, and J. Lim. Unified camera tamper detection based on edge and object information. *Sensors*, 2015.

[13] G.-b. Lee, Y.-c. Shin, J.-h. Park, and M.-j. Lee. Low-complexity camera tamper detection based on edge information. In *ICCE-TW '14*.

[14] Z. Li and Q. Li. Protection of regional object and camera tampering. In *2013 IEEE 4th International Conference on Software Engineering and Service Science*.

[15] D. T. Lin and C. H. Wu. Real-time active tampering detection of surveillance camera and implementation on digital signal processor. In *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*.

[16] P. Mantini and S. K. Shah. Human trajectory forecasting in indoor environments using geometric context. In *Proc. of the 2014 Indian Conf. on Computer Vision Graphics and Image Processing*.

[17] P. Mantini and S. K. Shah. Multiple people tracking using contextual trajectory forecasting. In *Technologies for Homeland Security (HST), 2016 IEEE Symposium on*.

[18] P. Mantini and S. K. Shah. Person re-identification using geometry constrained human trajectory modeling. In *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*.

[19] P. Mantini and S. K. Shah. Camera placement optimization conditioned on human behavior and 3d geometry. In *Proceedings of the 11th Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - Volume 3: VISAPP*, 2016.

[20] R. Priemer. *Introductory signal processing*. 1991.

[21] A. Raghavan, R. Price, and J. Liu. Detection of scene obstructions and persistent view changes in transportation camera systems. In *2012 15th International IEEE Conference on Intelligent Transportation Systems*.

[22] E. Ribnick, S. Atev, O. Masoud, N. Papanikolopoulos, and R. Voyles. Real-time detection of camera tampering. In *2006 IEEE International Conf. on Video and Signal Based Surveillance*.

[23] A. Saglam and A. Temizel. Real-time adaptive camera tamper detection for video surveillance. In *AVSS 2009*.

[24] C. C. Shih, S. C. Chen, C. F. Hung, K. W. Chen, S. Y. Lin, C. W. Lin, and Y. P. Hung. Real-time camera tampering detection using two-stage scene matching. In *2013 IEEE International Conference on Multimedia and Expo (ICME)*.

[25] K. Sitara and B. M. Mehtre. *Real-Time Automatic Camera Sabotage Detection for Surveillance Systems*.

[26] T. Tsesmelis, L. Christensen, P. Fihl, and T. B. Moeslund. Tamper detection for active surveillance systems. In *AVSS 2013*.

[27] C.-L. Tung, P.-L. Tung, and C.-W. Kuo. Camera tamper detection using codebook model for video surveillance. In *2012 International Conference on Machine Learning and Cybernetics*.

[28] Y. Wang, P.-M. Jodoin, F. Porikli, J. Konrad, Y. Benezeth, and P. Ishwar. Cdnet 2014: an expanded change detection benchmark dataset. In *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2014.

[29] Y.-K. Wang, C.-T. Fan, and J.-F. Chen. Traffic camera anomaly detection. ICPR '14.

[30] Y. K. Wang, C. T. Fan, K. Y. Cheng, and P. S. Deng. Real-time camera anomaly detection for real-world video surveillance. In *2011 International Conference on Machine Learning and Cybernetics*.

[31] Z. Wang, H. R. Sheikh, and A. C. Bovik. No-reference perceptual quality assessment of jpeg compressed images. In *ICIP 2002*, 2002.

[32] T. H. Wilmshurst. *Signal recovery from noise in electronic instrumentation*. CRC Press, 1990.

[33] H. Yin, X. Jiao, X. Luo, and C. Yi. Sift-based camera tamper detection for video surveillance. In *2013 25th Chinese Control and Decision Conference (CCDC)*.