PRNU-based Source Identification for Network Video Surveillance System

Sai-Chung Law and Ngai-Fong Law, senior member, *IEEE*
Dept. of Electronic and Information Engineering, The Hong Kong Polytechnic University
ennflaw@polyu.edu.hk

***Abstract*—Photo response non-uniformity (PRNU) noise has been proven instrumental for camera source identification in image forensics. The paper proposes a signal-based detection system using PRNU for source verification in video surveillance systems. The effects of different aspects such as video resolutions, frame types and environmental conditions on the accuracy and reliability of the system have been tested. Our results show that the signal-based approach is effective to verify the video source.**

I. Introduction

Video surveillance cameras are now increasingly connected through the network/Internet for remote viewing of live scenes via mobile apps or web-based applications. On one hand, such flexibility of access to the videos provides people much convenience. On the other hand, the same system becomes more prone to cyber-attacks at vulnerable points of networks. Hackers may break into the network and modify video data.

To verify the source of the security video, we can inspect the video to see if there are any visual discontinuities among consecutive frames. However, this method is both unreliable and tedious. Instead, current video systems often rely on network intrusion detection methods. In this paper, we propose an alternative signal-based method for verifying the source of the video. Particularly, we will analyze the video in signal level with a sensor pattern noise called photo response non-uniformity (PRNU) as the camera signature [1].

There is a growing trend of migrating from traditional network/Internet video security systems to Cloud-based counterparts [2]. In such cases, the conventional network-based detection approach is no longer useful, because video users and owners do not have much control on the cloud's infrastructures. Consequently, the proposed signal-based detection approach would become vital to verify the source, especially if the reliability of the video data in the cloud is of utmost business or legal importance.

II. Proposed Method

A typical video surveillance system consists of several components such as a set of cameras, video monitor, data storage devices, video management/analytic software and network equipment. A workstation with numerous functions including camera and monitor control is also needed. Video compression formats for these systems are usually H.264 and MPEG4. The resolutions mostly encountered can be HD 1920x1080 and 1280x720, or lower sizes such as 640x480. Fig. 1 shows the proposed signal-based detection system for video source verification. There are two main steps involved.

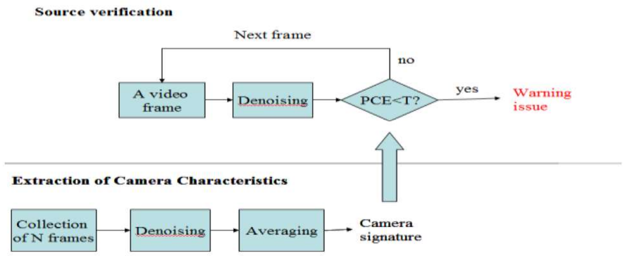

Fig. 1. Proposed signal-based source verification system.

Step 1: Camera signature construction: For each camera, a set of frames with smooth content is obtained to estimate the features of the security video camera. These frames will undergo denoising and averaging to obtain the PRNU as the camera signature. Finally, this camera signature will be stored in the system for source verification later.

Step 2: source verification: When a live video is received, and displayed in the monitor, its source will be verified. Frames are extracted from the live video stream. They will undergo denoising to obtain the noise residues which are then correlated with the stored camera signatures to find out their similarity. When the peak to correlation energy (PCE) value [3,4] for similarity test is large, then the video source matches the camera registered in the system. Otherwise, the video source cannot be verified.

The source verification is based on one tested frame in which its noise residue will be compared with the camera signature. The quality of the noise residue is thus important. Good results can be obtained from the scene which contains mostly smooth content. In video surveillance, however, various types of scenes are monitored. We devise two ways to improve the reliability of the detection. The first approach requires M consecutive video frames to have low PCE values before a warning is issued. In a typical video structure, we have I-, B- and P-frames in which B- and P-frames depend on I-frames for decoding. The accuracy of B- and P-frames is thus lower than that of I-fames in source verification. By using this approach, we can improve the reliability. The second approach is used to enhance the quality of noise residues. Rather than using one noise residue from one frame, noise residues from a group of frames are averaged to produce the resultant noise residue for more reliable source verification.

III. Experimental Results

Our proposed signal-based source verification system is evaluated on videos taken by three camera devices: Samsung Galaxy A7 (A7), Samsung Galaxy C7 Pro (C7) and Samsung SM-N7505 (SM). Videos from these three devices were merged to form a combined video that contains scenes from them. Three different sizes are tested, namely *L*:1920x1080, *M*:1280x720 and *S*:640x480. Video frames used to construct the camera signatures contain smooth content only.

Experiment 1: effect of resolutions: The combined video sequence contains 200 frames from A7, 200 frames from C7 and 200 frames from SM. Table 1 shows the average PCE values for different sections of the video sequence. For example, in the first row, using the camera signature of A7, the first 200 frames have an average PCE of 294.9, the next 200 frames have an average PCE of -0.10. Thus, the first 200 frames can be deduced to come from A7, while the next 200 frames are unlikely to be taken by A7. From frame sizes of 1920x1080 and 1280x720, we can see that the average PCE values give a reliable source verification for different scenes under test. However, the performance drops when the frame size becomes 640x480. In general, we can see that high peaks of PCE values occur periodically as well. It may be due to the frame structure of the video sequence.

Experiment 2: effect of frame structure: As I-frame uses only intra coding, it should be more reliable than B- or P-frames in source verification. Table 1 also shows the average PCE values for testing I-frames only. We can see that the PCE values for the positive cases increase while those values for the negative cases remain about the same. For example, for the camera SM, the average PCE value increases from 1.5 to 7.8 for same scene with 640x480 image size. Hence, the verification can be performed only on the I-frames without affecting the accuracy while reducing the false positive rate. Moreover, the computational complexity is also reduced.

Experiment 3: effect of outdoor environment: The video surveillance system may need to monitor outdoor scenes. Video scenes containing heavy rains have been collected. In these videos, visibility in some shots is not clear. We found that the heavy rain does not have much effect on the verification accuracy. This could be due to the blurring effect which tend to smooth out the texture pattern in the scene.

TABLE 1. Average PCE Values

Camera signature	Frame size	Consider all types of frames in video			Consider I-frames only in video		
		A7	C7	SM	A7	C7	SM
A7	*L*	**294.9**	-0.1	-0.05	**307.6**	-0.1	0.1
	M	**155.6**	-0.4	0.3	**434.2**	-0.1	0.2
	S	**12.7**	-0.1	-0.1	**24.9**	-0.4	-0.4
C7	*L*	-0.2	**3.7**	-0.0	-0.1	**22.6**	-0.2
	M	-0.1	**11.7**	-0.2	0.3	**35.8**	-0.3
	S	**1.4**	0.2	0.0	-0.5	**3.3**	0.4
SM	*L*	0.0	-0.4	**19.3**	0.3	0.0	**95.0**
	M	-0.1	-0.3	**70.7**	0.2	0.2	**195.1**
	S	-0.7	0.1	**1.5**	0.1	-0.9	**7.8**

Experiment 4: For 1920x1080 and 1280x720 cases, we can see that the verification is very reliable. PCE values for the positive cases and negative cases have essentially no overlap. However, there are overlaps for the 640x480 cases. To prevent this worst case of overlapping, two approaches have been proposed to reduce the false positive rates. Table 2 shows the results for requiring a number of frames having PCE values exceeding a threshold value *T* before issuing a warning. False positive (FP) case is the case where the video frame comes from the particular camera but the system cannot verify that. False negative (FN) case means that the video frame does not originate from the particular camera, but the system has wrongly classified it to be coming from the camera. The threshold *T* can be estimated based on the average values observed from the video signals produced by the particular camera. In this case, *T* is equal to 0.8*average PCE value. The results show that if we check for more number (M) of frames, both FP and FN can be reduced significantly. This can therefore enhance the reliability of the proposed system.

TABLE 2. FP and FN for Video Size of 640x480

		Approach 1			Approach 2	
		M=1	M=2	M=3	No=3	No=5
A7	FP	43%	18%	3%	0%	0%
	FN	0%	0%	0%	0%	0%
C7	FP	52%	11%	8%	23.3%	5%
	FN	7.5%	1%	0%	3.3%	0%
SM	FP	49%	14%	5%	6.7%	0%
	FN	4%	0.5%	0%	3.3%	5%

The quality of the noise residue from the test frame is critical to the reliability of the detection system. Instead of using just one frame for testing, an average for a number of noise residues can be used so that the additive noise in the video frames can be smoothed out. Table 2 shows the results for combining different number (No) of noise residues. It is found that there is a noticeable improvement of the system performance, when more number of frames in a video is used to produce the noise residues.

IV. Conclusions

We have proposed a signal-based source verification system for video surveillance. Reliability of the system under different aspects of video frame nature and environmental condition of scenes taken by cameras has been tested. The obtained results show a reliable system with promising application in the future. This signal-based system using PRNU can be integrated to video surveillance systems, so that the cyber security for important video data can be enhanced. Further works can include a larger dataset, various camera devices, and the system integration project.

References

[1] J. Lukas, J. Fridrich and M. Goljan, "Digital camera identification from sensor pattern noise", *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 205-214, June 2006.

[2] "Schneider Electric now offers Cloud-based video surveillance service", Security Distribution & Marketing, vol. 43(6), pp. 103, June 2013.

[3] M. Chen, J. Fridrich and M. Goljan, " Source digital camcorder identification using sensor photo response non-uniformity", Proc. of SPIE electronic imaging, steganography, security, and watermarking of multimedia contents IX, vol. 6505, pp. 1G-1H, 2007.

[4] L.H. Chan, N.F. Law and W.C. Siu, "A Confidence Map and Pixel-based Weighted Correlation for PRNU-based Camera Identification", Digital Investigation, 10(3), 2150-22, 2013.