Hybrid G-PRNU: Optimal parameter selection for scale-invariant asymmetric source smartphone identification

Reepjyoti DEKA, Chiara GALDI, Jean-Luc DUGELAY - Digital Security Department, Eurecom, Sophia Antipolis, France

Abstract

The ease in counterfeiting both origin and content of a video necessitates the search for a reliable method to identify the source of a media file - a crucial part of forensic investigation. One of the most accepted solutions to identify the source of a digital image involves comparison of its photo-response non-uniformity (PRNU) fingerprint. However, for videos, prevalent methods are not as efficient as image source identification techniques. This is due to the fact that the fingerprint is affected by the post-processing steps done to generate the video. In this paper, we answer affirmatively to the question of whether one can use images to generate the reference fingerprint pattern to identify a video source. We introduce an approach called "Hybrid G-PRNU" that provides a scale-invariant solution for video source identification by matching its fingerprint with the one extracted from images. Another goal of our work is to find the optimal parameters to reach an optimal identification rate. Experiments performed demonstrate higher identification rate, while doing asymmetric comparison of video PRNU with the reference pattern generated from images, over several test cases. Further the fingerprint extractor used for this paper is being made freely available for scholars and researchers in the domain.

Introduction

In forensic investigation of criminal cases like child pornography, movie piracy and other cases of frauds involving digital media, one of the significant challenges is to detect the origin of the media. Photo-response non-uniformity (PRNU) of digital sensors proposed by Lukas *et al.* [1] can be used as a unique fingerprint for digital cameras and hence is a key technology available for identification of smartphones from images. Researchers have tried to identify video sources by treating video frames as images. Forensic experts compare the fingerprint obtained from a video with the reference fingerprint extracted from a set of videos from a device. However the quality of the PRNU fingerprint obtained from a video is questionable. This is firstly due to the manufacturer specific video post-processing, and further due to the fact that unlike image capture, only a scaled (at a different size and/or a different aspect ratio), cropped or zoomed portion of the total sensor area is used for videos - a portion of the actual fingerprint of the device. In this paper, we present an approach called the "Hybrid G-PRNU" that uses reference PRNU fingerprints from images for video source identification and demonstrates its superior performance. Firstly, we establish that one can use image reference PRNU fingerprint, known to be of superior quality, to identify its source. Secondly, through our experiments, we find the optimal parameters for identification and show that hybrid methods are preferable over approaches which generate the reference PRNU patterns from video frames. The name of our technique is inspired by the works of Al-Athamneh *et al.* [2] and Iuliani *et al.* [3].

Related works

Researchers have proposed multiple techniques to tackle the important problem of source identification in digital image forensics [4]. Lukas *et al.* [1] present a digital source camera identification technique based on Sensor Pattern Noise (SPN). The latter is a pattern generated by the imperfections of the sensor silicon wafer, unique for each camera sensor, extracted from still images. In their scheme, each camera is identified by a Reference Sensor Pattern Noise (RSPN) estimated from a pool of captured images. The camera whose RSPN has the highest correlation with the SPN of the image in trial, is assigned as the source. Chen *et al.* [5] extend the PRNU technique to identify digital camcorders from video clips. Chuan *et al.* [6] state that strong compression lowers the accuracy of PRNU estimation, with performance being the highest when only I-frames are used. Galdi *et al.* [7] also demonstrate better estimation using only I-Frames and adopt Li's [8] PRNU enhancement. Sansone *et al.* [9] used PRNU to blindly cluster images in databases according to their source device. Houten and Geradts [10] tackle compression effects on *Youtube.com* videos by comparing the total correlation summed over all colour channels. Al-Athamneh *et al.* [2] present a "G-PRNU" approach by using only the green channel of the frames for computing PRNU and show its improved performance in camera identification for videos. Akshatha *et a.* [11] illustrate a feature based identification approach where the PRNU is extracted from images using a wavelet based denoising method and is represented by higher-order wavelet statistics (HOWS). Mcloskey [12] introduces a different enhancement technique to reduce the negative impact of the presence of edges in video frames while computing the pattern noise.

The overall consensus of the aforementioned work is that digital camera recognition from videos is still an open problem. The mentioned papers do not experiment with using still images to generate the reference fingerprint to verify a video source: we refer to this kind of approach as "hybrid" or "asymmetric". The drastic drop in performance of asymmetric comparison (i.e. image ref. vs. video and vice versa) is illustrated by Galdi *et al.* [13]. Asymmetric techniques has gained interest in other fields as well. For example, Galdi *et al.* [14] discuss improved user authentication using a combination of source camera identification and biometric recognition. Iuliani *et al.* use a "hybrid" approach that determines a geometric relation between images and the video frames of a smartphone, to identify a video source [3]. A major limitation however is that, a brute force search for determining the manufacturer specific cropping and scaling factors (and, in the case of devices acquiring stabilized videos, rotation) is required for the identification.

Contribution

In this paper, a novel hybrid approach for source identification is presented, namely "Hybrid G-PRNU", to extract and correctly identify a video source from an image-based reference PRNU fingerprint extracted from the green channel only. The proposed approach is independent of the geometric relation between the image and the video fingerprints, and thus invariant to crop and scaling factors, including different size and different aspect ratio. Unlike the work of Al-Athamneh *et al.* [2], our method is asymmetric as it does not use video frames as references. Further, both the image reference and the test video G-PRNUs are resized to 256×256px using bilinear interpolation. This is more efficient compared to the hybrid approach of Iuliani *et al.* [3] where a brute-force scheme is used for the determination of crop and scale parameters.

The experimental results provide the optimal parameters for a higher identification rate, using images and videos from the VISION dataset [15]. The "Hybrid G-PRNU" Forensic Tool [16] is available under an open source license. The updated green channel photo-response non-uniformity (G-PRNU) fingerprint extractor is based on the work of Muammar [17]. The current version allows customization by selecting different sizes and interpolation methods along with a variety of filters. Li's PRNU enhancement [8] method for image and noise handling is also incorporated in the tool.

The rest of the paper is organized as follows. The next section discusses the mathematical foundation of PRNU and of G-PRNU and the source identification algorithm. In Section "Experiments", the experimental setup of the "Hybrid G-PRNU" method, as well as the experiments conducted to determine the optimal parameters and the test results, are described. Finally, Section "Conclusion" summarizes our work and provides directions of future work.

From PRNU to G-PRNU

Photo-Response Non-Uniformity (PRNU) is an unique identification fingerprint for digital cameras. Imaging sensors are known to introduce noise in the pixel values [4]. This noise is the result of three main components, i.e. pixel defects, fixed pattern noise (FPN), and Photo-Response Non-Uniformity (PRNU). Pixel defects – point defects, hot point defects etc. – reasonably vary across different sensors, independently of the specific camera model. FPN and PRNU are the two components of the so-called pattern noise, and depend on dark currents in the sensor and pixel non-uniformities, respectively. These arise as a result of material and manufacturing imperfections of CCD and CMOS sensors and vary even for different devices of the same smartphone model. Lukas *et al.* [1] firstly proposed to analyze the sensor pattern noise (SPN) for camera identification and showed that noise extracted from images from the same camera are more correlated than from those extracted from different sensors/cameras. The noise can be estimated by subtracting the image from its denoised version. Denoising can be performed using different techniques. The "Hybrid G-PRNU" Forensic Tool allows users to choose one of the following filters for denoising: 'mihcak', 'sigma', 'gaussian', and 'bm3d'. We have chosen the wavelet-based technique proposed by Mihcak et al [18] for our experiments as it has been intensively used for denoising purposes and calculation of PRNU [19]. Considering $F()$ as the denoising filter, and W and I to be the SPN and the image respectively, we have that

$$W = I - F(I)$$

The reference SPN W_{ref} is calculated by averaging the SPN extracted from a sufficiently large number of images or frames (I-frames in our case) from a video.

$$W_{ref} = \frac{1}{m}\sum_{i=1}^{m} W_i$$

Where m is the number of reference images. Chen *et al.* [20, 21] acknowledge the fact that the pattern noise W is a combination of the PRNU signal IK and other sources of noise Ξ (e.g. CFA interpolation or compression quantization).

$$W = IK + \Xi$$

For a camera model c, the reference $\hat{K}^c$ can be estimated through maximum likelihood using

$$\hat{K}^c = \frac{\sum_{k=1}^{d} W_k I_k}{\sum_{k=1}^{d} (I_k)^2}$$

where, $k = 1, 2 \ldots d$ are the number of images used to calculate the reference PRNU factor. If the correlation between W^c_{ref} calculated for a camera device c and the pattern noise calculated for an individual image I is high (above an empirically determined threshold per device), we can establish that image I, was captured by the camera c. In practice, normalized cross correlation (NCC) of the reference and the test PRNU factors are calculated and for further confirmation Peak-to-Correlation Energy ratio (PCE), a measure of similarity for two discrete signals, is used. PCE is especially suitable for 2-dimensional camera fingerprints because of the presence of hidden periodic patterns (a latent source of false identification) [22]

$$\begin{aligned} corr(X,Y) &= \frac{(X-\bar{X}) \odot (Y-\bar{Y})}{\|X-\bar{X}\| \cdot \|Y-\bar{Y}\|} \\ PCE &= \frac{corr[U_{peak}, V_{peak}]^2}{\frac{1}{mn-|N_{peak}|}\sum_{(u,v)\notin N_{peak}} corr[u,v]^2} \end{aligned} \tag{1}$$

As mentioned in an article from the Stanford Center for Image Systems Engineering (SCIEN) [23], the relationship between PRNU responsivity and exposure time is approximately linear. Among the three channels, the green channel has the highest PRNU responsivity followed by red and blue. Employing this information, Al-Athamneh *et al.* [2] provide the "G-PRNU approach" and show that it is a more reliable approach than ordinary PRNU for source camera identification with videos as test and references. In their experiments, they used 350 frames per video. Their method extracts the green channels, resizes them to 512×512 pixels, performs denoising and calculates the average G-PRNU over the video frames. The identification uses 2-D correlation coefficient as similarity metric to identify the source camera. Unlike [2], the proposed approach is hybrid, that is it matches videos to the reference fingerprint extracted from still images. It uses the "G-PRNU" where only the green channel of the images is considered for the reference computation. Optimal parameters are selected, resizing to 256×256 pixels using bilinear interpolation, in order to increase the identification rate. Next Section details a suite of experiments for the selection of the optimal parameter values.

Experiments and results

Setup

Our Method is tested on a benchmark dataset of 35 devices, namely VISION [15], released for the evaluation of image and video forensic research. For computing the image-based reference SPN of a device, flat images are used. The reference SPN from videos is extracted by averaging the SPN from the I-frames of flat-still videos. The media files used as test images and test videos are randomly picked from the "natural" media folder in VISION. For test video SPN estimation, only i-frames were used to generate the fingerprint using our method. For test images (and test videos), Li's PRNU enhancement [8] has been applied to suppress information derived from high frequencies (e.g. edges) of the test images (and test video i-frames). For extracting and correlating the G-PRNUs, the Hybrid G-PRNU Forensic Tool [16] is used, that is configurable to different scaling factors and interpolation methods. The tool is made open source for the research community.

A reliability score is then computed by normalizing all correlation values between 0 and 1 to determine the confidence of the matches, by applying the formula:

$$\text{Reliability Score} = \frac{(\text{rank 2 score} - \text{rank 1 score})}{(\text{rank 3 score} - \text{rank 1 score})}$$

The results are presented as cumulative match characteristic (CMC) curve, where rank describes how many top correlated scores are considered to declare a match and identification rate is the percentage of devices that are correctly identified.

Please note that the terms sensor pattern noise (SPN), PRNU and fingerprint are used interchangeably in this paper. For clarity, in the following sections, the following abbreviations below will be adopted:
IMG-RSPN - Reference PRNU fingerprint or Sensor Pattern Noise computed from flat field images;
IMG-SPN - Sensor Pattern Noise computed from images;
VID-RSPN - Reference Sensor Pattern Noise computed from flat field videos (i-frames);
VID-SPN - Sensor Pattern Noise computed from video i-frames.
For all experiments, the SPN/RSPN is computed using only the green channel of the media files. The resizing values and the interpolation methods are abbreviated in the paper as follows:
XXX BL = $XXX \times XXX$px Bilinear Interpolation
XXX BC = $XXX \times XXX$px Bicubic Interpolation
XXX NN = $XXX \times XXX$px Nearest Neighbour Interpolation

Baseline Experiments

As a baseline experiment on the devices from the VISION dataset, the IMG-RSPN and IMG-SPN are computed and compared at different sizes. This experiment confirms that sensor identification using images achieves 100% accuracy even if we extract and compare the G-PRNU at 256 BL, 512 BL or 640 BL. This could be beneficial considering that the computation of the G-PRNU at lower sizes is much faster than extracting the fingerprint at a higher resolution.

The "Hybrid G-PRNU" approach is based on asymmetric comparison of video vs. image fingerprint. Whereas, G-PRNU was firstly proposed by Al-Athamneh *et al.* [2] for video vs. video PRNU matching. The experiment was repeated, using video I-frames to generate the fingerprint, as another baseline experiment. The VID-SPN is compared with the VID-RSPN computed from the videos in VISION dataset. Two set of parameters from the methods being compared are tested: the one proposed in by Al-Athamneh *et al.* [2], that is 512 BL, and the one proposed by this work, that is 256 BL. Please note that for our experiments only i-frames are used. The results of the experiment are summarized in Figure 1. The experiment confirms that the best scaling size for video vs. video comparison, that is symmetric matching, is 512 BL, as found by Al-Athamneh *et al.* [2]. In the following, it is demonstrated that for asymmetric comparison the optimal set of parameters is 256 BL instead.

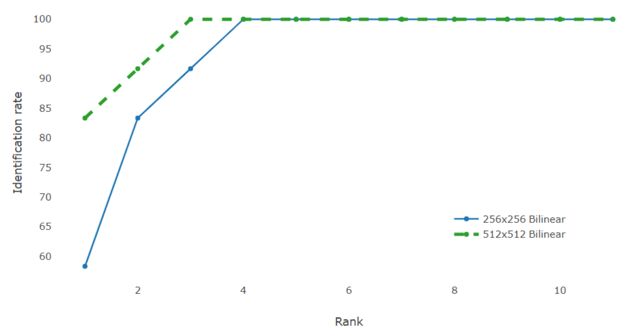

Figure 1. *Baseline - Cumulative Match Curve for VID-RSPN vs VID-SPN matching - Non-Stabilized Videos*

The following subsections describe the method and its performances. Please note that the experiments are performed separately on the devices acquiring stabilized videos and those without digital stabilization.

Hybrid G-PRNU

The steps of the proposed "Hybrid G-PRNU" method are summarized below:

1. Extract green channel i-frames of the video;
2. Perform Mihcak wavelet-based denoising on the green channel i-frames.
3. Resize the sensor pattern noise obtained to 256×256px using bilinear interpolation.
4. Compute the G-PRNU for the device by averaging the noise pattern over the green channel i-frames.
5. Apply Li's enhancement algorithm on the pattern noise extracted on step 4.
6. Using a pool of images (possibly flat), extract the reference G-PRNU at size 256×256 to compute the reference fingerprint.
7. Compute the 2D cross correlation between the reference G-PRNU and the fingerprint extracted in steps 1-5.
8. The device of the image reference which shows highest correlation with the test video fingerprint is the source of the

Table 1: Image and Video frame sizes of 4 devices from the VISION dataset.

Device	D03	D04
Image resolution	3968×2976	3264×2448
Video frame resolution	1920×1080	800×480
Device	**D07**	**D20**
Image resolution	4784×2704	2592×1936
Video frame resolution	1280×720	1920×1080

video in question.

9. Validate the results by calculating the reliability score.

A flowchart representing the Hybrid G-PRNU approach is illustrated in figure 2.

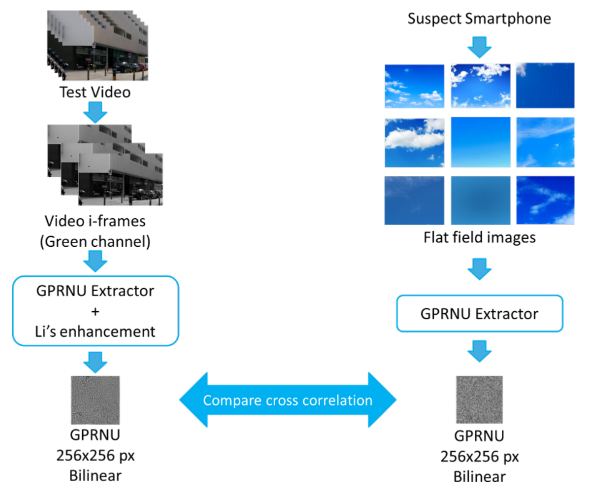

Figure 2. Flowchart of the proposed method

Finding Optimal Parameters

In smartphones, not only the resolution changes when capturing pictures and while recording videos with the same sensor, but also the scene is usually cropped and scaled for videos compared to still images. This leads to false positives during source identification. Table 1 shows a glimpse of the different resolutions of media files available in the VISION dataset.

To tackle the changes in aspect ratio between the fingerprint extracted from videos and the one obtained from images and to mitigate the matrix dimension mismatch problem, both G-PRNU fingerprints are scaled to a predefined size. The following experiment is intended to determine which scaling parameters perform the best for asymmetric PRNU comparison.

To show the difference in quality of a fingerprint, patterns extracted from images and video I frames of device D09 of the VISION dataset, at different sizes and interpolation methods, is shown in Figure 3 and Figure 4. For the optimal parameters selection, the G-PRNU was extracted and compared using flat-field videos and images at 64×64px, 128×128px, 256×256px, 512×512px, 640×640px and at the video I-frames size, each with bilinear (BL), bicubic (BC) and nearest neighbour (NN) interpolation methods. Among all, G-PRNUs extracted at 256 BL and 256 BC correlated better compared to the other settings for all devices. For stabilized video acquiring devices however, the correlation scores were lower and comparable to the ones obtained using the other parameters. Among the interpolation methods, at a particular size, the highest correlation is empirically observed to be shown by bilinear, followed by bicubic and nearest neighbour. Scaling to a smaller dimension reduces G-PRNU computation time drastically but highly increases the number of false positives as in the cases of 64×64px and 128×128px.

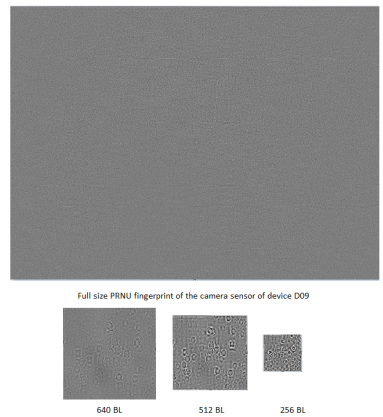

Figure 3. IMG-RSPN (extracted from images) for Device D09. Top to Bottom, Left to Right: PRNU of D09 extracted from images, GPRNU extracted at 640 BL, GPRNU at 512 BL, GPRNU at 256 BL. The sizes are scaled for better viewing.

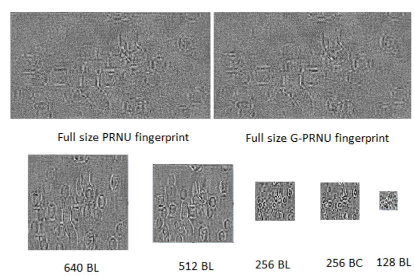

Figure 4. VID-RSPN (extracted from video I-frames) for Device D09. Top to Bottom, Left to Right: PRNU (all channels) of D09 extracted at video iframe size (resized), GPRNU extracted at video iframe size, GPRNU at 640 BL, GPRNU at 512 BL, GPRNU at 256 BL, GPRNU at 512 BC, GPRNU at 128 BL. The sizes are scaled for better viewing.

Figure 5 and Figure 6 show the identification rates obtained by the optimal set of parameters for devices acquiring non-stabilized and stabilized videos, respectively. The CMC curves show that there is an overall higher accuracy for 256 BL for non-stabilized videos. The latter is then selected as the scaling parameter for the proposed approach. In the case of stabilized videos, 256 BL and 256 BC perform better than the rest at lower ranks, however, the identification rate is much lower compared to non-stabilized videos. 512 BL performs better than the rest after rank 6 with 73.33% identification rate, reaching 80% at rank 11.

Performance of Optimal parameters

For testing the approach using the selected optimal parameters, the VID-SPNs from test video are extracted. SPN extraction

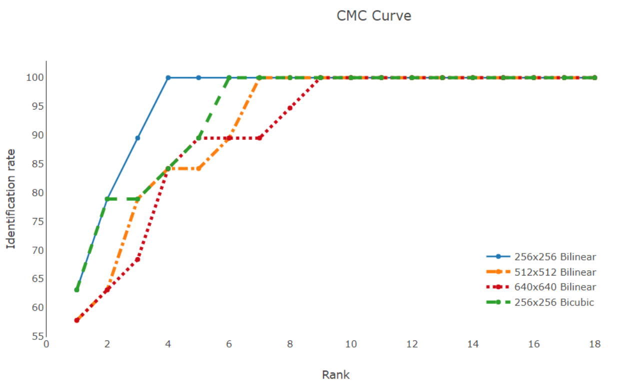

Figure 5. *Non-Stabilized Videos: Finding optimal parameters - Cumulative Match Curve for asymmetric matching using flat field images and videos*

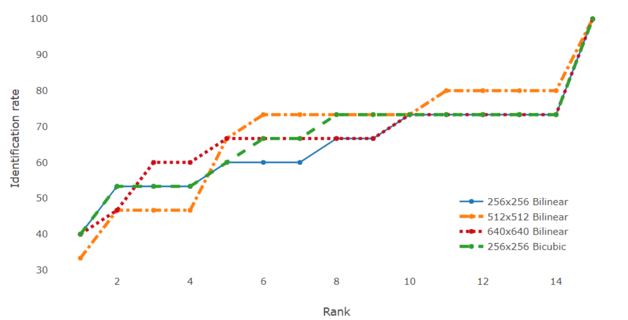

Figure 6. *Stabilized Videos: Finding optimal parameters - Cumulative Match Curve for asymmetric matching using flat field images and videos*

and Li's PRNU enhancement are applied on randomly selected natural videos from each device from the VISION dataset. We used the IMG-RSPN as reference fingerprint for the identification.

For non-stabilized videos, 100% accuracy is achieved in identifying the source devices using "Hybrid G-PRNU" approach with the optimal parameters (256 BL). Figure 7 describes the performance of the optimal parameters compared to Al-Athamneh *et al.* [2] and to other comparative parameter sets. Please note that we performed the experiments using only I-frames of the video. The reliability scores of each device identified are presented in the Table 2. The results show that not only our approach achieves optimal performances for asymmetric PRNU comparison, but also that our method outperforms symmetric comparison VID-RSPN vs. VID-SPN. This confirms the observation that given the superior quality of the reference fingerprint extracted from still images, asymmetric comparison is to be preferred over symmetric comparison for video source identification.

While searching for optimal parameters for stabilized videos, we observed that the Hybrid G-PRNU approach was not as effective as for non-stabilized videos. This can be attributed to the fact that in the case of stabilized videos, post-processing has a rotational affect on the fingerprint, which the "Hybrid G-PRNU" method does not account for. Not much performance variance is observed upon changing the parameters and 20-30% of the devices were never identified, even when IMG-RSPN and VID-

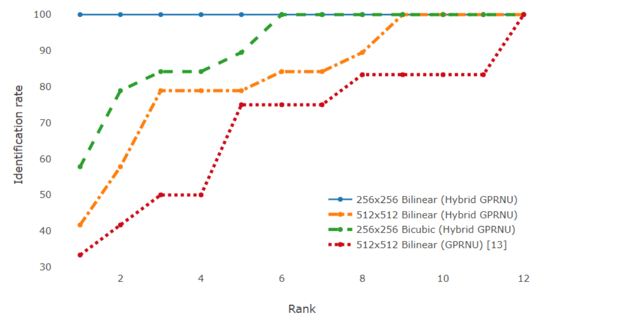

Figure 7. *Performance of optimal parameters on test videos - Cumulative Match Curve for Image Reference vs Test Video. In this plot, the superior performance of the proposed Hybrid G-PRNU method, compared to the parameters used by Al-Athamneh* et al. *[2], is established, demonstrating asymmetric comparison being more dependable than symmetric matching for video source identification.*

Table 2: Reliability Scores of Successfully Identified Sources of Non-Stabilized Videos

Device	**D03**	**D07**	**D09**	**D11**	**D16**	**D17**
Score	.9806	.9640	.9972	.9718	.9384	.9810
Device	**D21**	**D22**	**D24**	**D27**	**D28**	**D30**
Score	.9831	.9508	.8895	.9940	.9114	.6945

RSPN were compared as shown in Figure 6. However, as listed in the Table 3 except device D18, 5 out of 6 devices are correctly identified at rank 1 at 256 BL and show a very high reliability score.

For non-stabilized devices, even though the VID-SPN seem to highly correlate with the IMG-RSPN of the same device, we notice the presence of certain "imposter" devices where their IMG-RPSN has a higher correlation with most of the VID-SPNs, including two where it showed a higher correlation than the image reference of the source itself.

Conclusion

Identifying the origin of a digital media file is still an open research area. State-of-the-art methods have achieved good performance on detecting the source of an image, however there is room for improvement considering the increase in number and type of capturing devices. For videos, research is mostly based on the application of image-based techniques on video frames, performance of which is not at par with that of image source detection.

In this paper, we have experimentally verified that asymmetric comparison of G-PRNU extracted from images successfully identifies video source. In particular, we show that for videos source identification, using the G-PRNU of the image at 256×256 pixels using bilinear interpolation gives the best results for non-stabilized videos, specifically, much better than the original i-frame size. Our approach named "Hybrid G-PRNU" is built

Table 3: Reliability Score of Successfully Sources of Stabilized Videos

Device	**D04**	**D14**	**D15**	**D18**	**D25**	**D34**
Score	.9887	.9983	.9920	.3589	.9917	.9980

on the most efficient research in this field and is tested on the benchmark dataset VISION for forensic research. The tool used in the project is licensed as open source and made available for the research community to use and enhance it.

The "Hybrid G-PRNU" method does not require to find the different scaling and cropping parameters for each device as in [3]. Also, the method acknowledges the fact that the aspect ratio of a video is different than the one of the still images from the same device. This enables an unaffected detection process despite the fact that a single camera can produce a range of videos with different frame size. The reliability score increases with the increase in number of i-frames and the reference pattern noise is stronger if a larger number of flat-field images is used. Due to the rotational affect on the fingerprint for devices acquiring stabilized videos, the accuracy of the method decreases. For non-stabilized videos however, we achieve 100% accuracy in identification even for devices with less number of media files (80 images and 60 i-frames for device D30).

As future work, we plan to analyze methods to identify the source of digitally stabilized videos and also to further investigate imposter devices reported in section 3.5.

References

[1] J. Lukas, J. Fridrich, M. Goljan. Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics and Security, June 2006, 205-214

[2] M. Al-Athamneh, F. Kurugollu, D. Crookes, M. Farid. Digital Video Source Identification Based on Green-Channel Photo Response Non-Uniformity (G-PRNU). September 2016 DOI 10.5121/csit.2016.61105

[3] M. Iuliani, M. Fontani, D. Shullani, A. Piva. A Hybrid Approach to Video Source Identification. 4 May 2017) - arXiv:1705.01854 [cs.MM]

[4] J. A. Redi, W. Taktak, JL Dugelay. Digital image forensics: a booklet for beginners. Multimedia Tools and Applications-January 2011, Volume 51, Issue 1, pp 133162

[5] M. Chen, J. Fridrich, M. Goljan, J. Lukas. Source Digital Camcorder Identification Using Sensor Photo Response Non-Uniformity. Proc. SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX, 65051G, 1 March 2007

[6] W. Chuan, H. Su, M. Wu. Exploring Compression Effects For Improved Source Camera Identification Using Strongly Compressed Video. 2011 - DOI 10.1109/ICIP.2011.6115855

[7] C. Galdi, M. Nappi, JL. Dugelay, Secure User Authentication on Smartphones via Sensor and Face Recognition on Short Video Clips, International Conference on Green, Pervasive, and Cloud Computing, 15-22

[8] C.-T. Li, Source camera identification using enhanced sensor pattern noise. IEEE Trans. Inf. Forens. Secur., 5 (2) (2010), pp. 280-287

[9] F. Marra, G. Poggi, C. Sansone and L. Verdoliva, "Blind PRNU-Based Image Clustering for Source Identification," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 9, pp. 2197-2211, Sept. 2017.

[10] W. Houten, Z. Geradts. Using Sensor Noise to Identify Low Resolution Compressed Videos from Youtube. 2009 - IWCF 2009, LNCS 5718, pp. 104115

[11] K.R. Akshatha, A.K.Karunakar, H. Anitha, U. Raghavendra, D. Shetty. Digital Camera Identification using PRNU: A feature based approach. Digital Investigation Volume 19, December 2016 https://doi.org/10.1016/j.diin.2016.10.002

[12] S. Mcloskey. Confidence Weighting for Sensor Fingerprinting. 15 July 2008 DOI: 10.1109/CVPRW.2008.4562986

[13] C. Galdi, F. Hartung, JL. Dugelay, Videos versus still images: Asymmetric sensor pattern noise comparison on mobile phones, Electronic Imaging 2017 (7), 100-103

[14] C. Galdi, M. Nappi, JL. Dugelay, Y. Yu, Exploring New Authentication Protocols for Sensitive Data Protection on Smartphones, IEEE Communications Magazine 56 (1), 136-142, 2018

[15] D. Shullani, M. Fontani, M. Iuliani, O.A. Shaya, A. Piva. VISION: a video and image dataset for source identification. EURASIP Journal on Information Security (2017) 2017:15

[16] Github page: https://goo.gl/SEjzDB

[17] H. Muammar. Source Camera Identification Using Image Sensor PRNU Pattern. London: Communications And Signal Processing Research Group, 2014. Imperial College Communications And Signal Processing Research Group. Web. 29 Feb. 2016.

[18] M.K. Mihcak, I. Kozintsev, K. Ramchandran: "Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising," Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Phoenix, Arizona, vol. 6, pp. 32533256, March 1999.

[19] J. Lukas, J. Fridrich, M. Goljan. Detecting digital image forgeries using sensor pattern noise. In SPIE Electronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents VIII, volume 6072, pages 362U372, San Jose, CA, USA, Jan. 2006.

[20] M. Chen, J. Fridrich, M. Goljan (2007) Digital imaging sensor identification (further study). In: Proc SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX 6505(1) marking of Multimedia Contents. San Jose, CA, USA

[21] M. Chen, J. Fridrich, M. Goljan, J. Lukas (2008) Determining image origin and integrity using sensor noise. IEEE Trans Inf Forensics Secur 3(1):7490

[22] Binghamton.edu page: https://goo.gl/p7XxME

[23] Stanford.edu (Archive.org) page: https://goo.gl/MGhaiD