Provenance Analysis for Instagram Photos

Yijun Quan[1], Xufeng Lin[2], and Chang-Tsun Li[1,2]

[1] University of Warwick, Coventry, UK
Y.Quan@warwick.ac.uk
[2] Charles Sturt University, Wagga Wagga, Australia

Abstract. As a feasible device fingerprint, sensor pattern noise (SPN) has been proven to be effective in the provenance analysis of digital images. However, with the rise of social media, millions of images are being uploaded to and shared through social media sites every day. An image downloaded from social networks may have gone through a series of unknown image manipulations. Consequently, the trustworthiness of SPN has been challenged in the provenance analysis of the images downloaded from social media platforms. In this paper, we intend to investigate the effects of the pre-defined Instagram images filters on the SPN-based image provenance analysis. We identify two groups of filters that affect the SPN in quite different ways, with Group I consisting of the filters that severely attenuate the SPN and Group II consisting of the filters that well preserve the SPN in the images. We further propose a CNN-based classifier to perform filter-oriented image categorization, aiming to exclude the images manipulated by the filters in Group I and thus improve the reliability of the SPN-based provenance analysis. The results on about $20,000$ images and 18 filters are very promising, with an accuracy higher than 96% in differentiating the filters in Group I and Group II.

Keywords: Digital image forensics, sensor pattern noise, social media, provenance analysis

1 Introduction

The provenance of a digital image constitutes the most essential information about the history of the image, thus its determinability is crucial for any successive forensic investigation to be conducted on the image. For instance, forensic investigators are often faced with the challenge of analyzing a large corpus of images of unknown provenance, e.g. downloaded from the social media sites. If the image provenance information can be recovered, the forensic investigators will be able to focus on the images of the same provenance and conduct more effective investigations, e.g. associating the images to the cameras or cellphones belonging to a suspect. Occasionally, the provenance information of an image can be extracted from the attached metadata, e.g. EXIF header, but this only grants limited reliability as the metadata can be easily edited or erased. A more reliable way would be to infer the provenance from the image data itself. It has

been shown that some artifacts introduced by the in-camera processing components, either hardware or software, of the acquisition pipeline can be used to "fingerprint" the source camera. One such artifact is sensor pattern noise (SPN) [1], which mainly arises from the manufacturing imperfections of imaging sensors. The same SPN is left in every image taken by the same source camera, therefore, the images of the same provenance can be identified by examining the similarities between their SPNs, which are usually approximated as the noise residuals of the images.

Various SPN-based methods have been proposed to identify the source device of images [2–7] or group images of the same provenance [8–11]. However, almost all of these methods were evaluated on the high-quality images straight out from the camera without undergone any off-camera post-processing. With the rise of social networks, digital images have been continuously uploaded from computers or portable devices and shared through social media platforms. The increasingly rich built-in photo-editing features on social media platforms, e.g. the photo filters on Instagram or camera effects on Facebook, allow users to produce visually attractive photos at the tap of a finger. Consequently, the images downloaded from social networks may have gone through a series of manipulations, most of which are unknown, before they are handed to forensic investigators. In view of these facts, it is reasonable to question the trustworthiness of SPN in determining the provenance of images downloaded from social media sites. In this paper, we are particularly interested in the provenance analysis of the images posted on Instagram, which is one of the most popular photo-sharing platforms and offers a number of pre-defined photo filters. Using the performance of SPN-based provenance-oriented image clustering as an indicator, we intend to investigate the effects of Instagram filters on SPN-based image provenance analysis.

The rest of this manuscript is organized as follows: Section 2 briefly introduces the background and related works. Section 3 describes the details of the evaluation methodology. Section 4 presents the experimental results while Section 5 draws the conclusion and outlines the future work.

2 Background and Related Works

SPN, as its name indicates, is the fixed noise pattern that originates from the imaging sensor. The dominant component of SPN is the photo response non-uniformity (PRNU) noise, which is due to the variation of pixels' capabilities in converting photons into electrons. Such pixel-to-pixel discrepancy is very unique and commonly presents in every image captured by a sensor, making SPN a feasible choice for source device fingerprinting from images. Given an image $\boldsymbol{I}$, its SPN $\boldsymbol{n}$ can be approximated by the noise residual [1]:

$$\boldsymbol{n} = \boldsymbol{I} - \hat{\boldsymbol{I}}, \tag{1}$$

where $\hat{\boldsymbol{I}}$ is the denoised image. To see if the image is taken by a camera C, the normalized cross-correlation (NCC) similarity is examined:

$$\rho = corr(\boldsymbol{n}, \boldsymbol{r}) = \frac{(\boldsymbol{n} - \bar{\boldsymbol{n}}) \cdot (\boldsymbol{r} - \bar{\boldsymbol{r}})}{\|\boldsymbol{n} - \bar{\boldsymbol{n}}\| \|\boldsymbol{r} - \bar{\boldsymbol{r}}\|}, \tag{2}$$

where $\boldsymbol{r}$ is the reference SPN constructed by averaging the SPNs of multiple images captured by C to suppress other random interferences. $\boldsymbol{I}$ is deemed to be taken by C if ρ exceeds a predefined threshold. This task is referred to as source camera identification (SCI) in the literature. Similarly, for any two single images, if they are captured by the same camera, they should share the same SPN and have a relatively larger similarity. Based on the similarities, we are able to cluster the images of the same provenance. We will refer to this task as provenance-oriented image clustering, which is more challenging due to the unavailability of reference SPN and the necessity of examining the similarities of SPNs pairwise.

SPN has been proven to be effective for identifying the provenance of images [12]. However, most of the techniques based on SPN were evaluated on the images coming directly out of cameras, ranging from various private datasets to the widely used Dresden image database [13]. Nowadays, with the popularization of social media, the amount of digital images uploaded to and shared through social networks has explosively increased. Conducting forensic investigations on images downloaded from social networks will thus become increasingly common in the foreseeable future. The manipulations, usually unknown, that different social media platforms apply to images may attenuate the SPN signal in the image and thus are casting doubt on the trustworthiness of SPN in determining the provenance of digital images.

Despite the above problem, few studies have actually tried to evaluate the effectiveness of SPN on images from social media. Goljan *et al.* [12] conducted a large-scale test of camera identification from SPN on images downloaded form Flickr. Experiments on over one million pictures showed a false rejection rate < 0.0238 at a false acceptance rate $< 2.4 \times 10^{-5}$, which is a very promising result given that the images were taken by 6896 cameras covering 150 camera models. But it should also be noticed that Flickr allows the uploaded images to be stored in their original resolution with no or very little compression, so the results on Flickr are not representative compared to other social media platforms which may apply a series of manipulations on images.

In [14], Satta and Stirparo used SPN for linking a photo to social network accounts belonging to the person that has shot the photo. A probe photo P is considered to be taken by the account containing the image with the highest matching score to P. Evaluated on 2896 images from Flickr, Facebook, Google+ and personal blogs belonging to 30 different accounts, the method gave a correction recognition rate of $\sim 50\%$. Though it may not be high enough for accurate identification, such a performance shows the feasibility of using SPN for provenance analysis of images on social media. However, the rapidly evolving new tools and techniques constantly being deployed on social media platforms leave a huge gap for further studies.

Recently, it has been shown in some works, e.g. [15, 16], that the image manipulations applied by each social network will leave some distinctive traces that can, in turn, be used to trace back to the social network origin of the image. This opens up new possibilities to associate an image with its social network provenance, but it also poses new challenges for tracing back to an image's acquisition device provenance via SPN, which may have been attenuated or removed after the image is uploaded. In this paper, we intend to investigate the effects of the photo filters of Instagram on the task of SPN-based provenance-oriented image clustering, the performance of which is a good indicator of how well the SPN is preserved after the filters are applied. Note that we did not evaluate the performance of SPN-based source camera identification because in many real-world scenarios, especially for social network data analysis, the reference SPN is not easy or impossible to obtain, but we believe that the performance of SPN-based source camera identification on Instagram photos should exhibit similar patterns and trend as the results presented in this paper.

3 Methodology

In this work, we sought to answer the following three closely related questions:

1. Would the filtering operations affect the SPN significantly and whether directly clustering the Instagram photos irrespective of the applied filters is possible?
2. How different filters affect the SPN?
3. Is it possible to identify the applied filter so that more reliable provenance analysis can be conducted with the information of the identified filters?

To answer the above three questions, a series of evaluations will be conducted. We will first blindly cluster a collection of images manipulated by different filters without knowing what filters have been applied. The clustering results of this experiment should give us an answer about to what extent the SPN can be affected by Instagram filters. Different image filters may have different impacts on the SPN, so in the second experiment, we will investigate the effects of different filters on SPN by performing SPN-based image clustering on images processed by individual filters. As can be expected, some filters may severely attenuate or remove the SPN in the images. So for the reliability of the provenance analysis, identifying and excluding the images manipulated by such filters is important. This requires us to be able to identify the filter applied to an image. For this purpose, in the third experiment, we will train three photo filter classifiers with Convolutional Neural Network (CNN), using the unprocessed images (with filters applied), denoised images and noise residuals, respectively.

Network Design The design of the network is inspired by the well-known VGG-network [17] and the work in [18], where the VGG-net is used to extract the perceptual artistic styles from artworks. A main feature of VGG-net is that

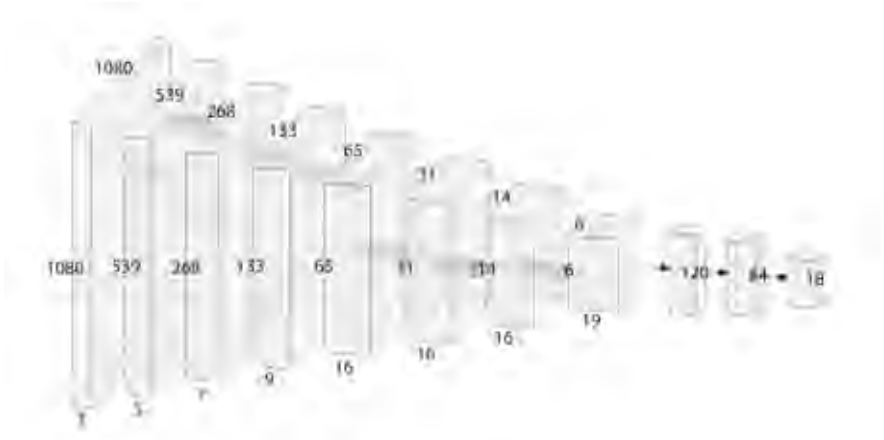

Fig. 1: The network architecture of the filter classifier. For brevity, only the convolutional and fully-connected layers are shown. The red pyramid represents the combination of convolution and max-pooling operations. The blue cuboid represents the receptive field of each convolutional filter, which has a size of 3×3 throughout the network. The dimensions of each layer are labeled by the numbers on the edges.

it uses convolutional layers with a small receptive field (e.g. 3×3) combined with a large depth of the network. The layers in the convolutional neural network can be considered as a set of different image filters and each filter extracts certain features of the image. While including higher layer information can lead to a finer representation of the artistic style, the artistic style can be mostly represented by the lower layers of a neural network. It indicates that a shallower network might be able to capture the features to classify the Instagram filters without compromising too much performance. To further reduce the computational cost, in this work, we use a network with 7 convolutional layers followed by 3 fully connected layers (Fig. 1), which is more compact than the shallowest VGG-net architecture (11 layer VGG-net) in [17] and the 19 layer VGG-net used in [18]. All the convolutional layers have a receptive field size of 3×3 and all the hidden layers are equipped with the rectification non-linearity (ReLU) and batch normalization. Each convolutional layer is followed by a max-pooling layer, which is performed over a 2×2 pixel window. The network takes 3-channels (RGB) images of size 1080×1080 pixels (the maximum allowable image resolution on Instagram at the time being) as input and returns a vector of length 18 to accomplish an 18-class classification (to classify 17 different Instagram filters tested in this work and the original image).

Network inputs Since we can consider the Instagram filters as the artistic styles of the images as a whole, removing the noise can reduce the pixel-wise

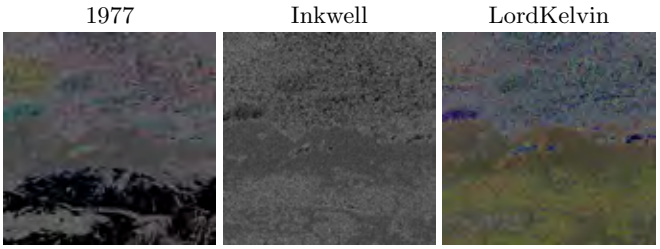

Fig. 2: The noise residuals extracted from the three images shown in Fig. 3.

disturbance and may improve the training of the classifier. However, on the other hand, we notice that the filters can not only change the visual style in the images but also alter the noise residuals of the images in very different manners. For example, some filters have high contrast level which can suppress the noise at both ends of histogram. So the filtered images tend to have more flattened regions of noise, as exemplified by the image manipulated by filter '1977' in Fig. 2. As another example, some filters can have different color profiles, so the noise behavior may vary considerably across different color channels (e.g. comparing Inkwell and LordKelvin in Fig. 2). These significant differences introduced by different filters in the noise residuals motivate us to use noise residuals as the input for constructing the filter classifier. Given all these facts, we train three classifiers of the same neural network architecture using three different inputs: the unprocessed images $\boldsymbol{I}$ (with filters applied), denoised images $\hat{\boldsymbol{I}}$ and image noise residuals $\boldsymbol{n}$. For simplicity, we call the three networks as $\boldsymbol{I}$-net, $\hat{\boldsymbol{I}}$-net and $\boldsymbol{n}$-net, respectively.

4 Experiments

4.1 Dataset

The experiments were conducted on the images from 25 different mobile devices in the VISION dataset [19], with each device accounting for more than 200 JPEG images. These images were first cropped to a size of 1080×1080 pixels. For each image, we then applied 17 different filters with the Instagram app on iOS. We consider the filters as black boxes without knowing the details of how the images are manipulated. The list of the filters applied can be found in Fig. 3, where one example image is shown for each filter while the original image is labeled as 'Normal'. Thus, together with the original image, we have 18 different versions for each image from the VISION dataset, which results in $96,660$ images in total. The whole set or a subset of these $96,660$ images will be used in the following experiments.

Fig. 3: Example images of the 17 Instagram filters together with the original image (Normal) used in our experiment.

4.2 Evaluation Matrix

As can be noticed in Fig. 3, to produce different artistic visual effects, each filter may alter each color channel in very different manners. For this reason, we will evaluate the clustering performance with the noise residuals extracted from all three color channels (RGB) using BM3D denoising algorithm [20]. The fast clustering algorithm in [21] will be used to cluster the images and the clustering quality is measured by F1-measure, which is defined as:

$$\mathcal{F} = 2 \cdot \frac{\mathcal{P} \cdot \mathcal{R}}{\mathcal{P} + \mathcal{R}} \tag{3}$$

where $\mathcal{P}$ and $\mathcal{R}$ are the average precision and recall rate respectively. They can be calculated as:

$$\begin{cases} \mathcal{P} = \sum_i |c_i \cap \psi_{j^*}| / \sum |c_i| \\ \mathcal{R} = \sum_i |c_i \cap \psi_{j^*}| / \sum |\psi_{j^*}| \end{cases} \tag{4}$$

$|c_i|$ is the size of the cluster c_i, and $|\psi_{j^*}|$ is the size of the class ψ_{j^*} (i.e. the number of images captured by camera j^*) corresponding to the largest sub-cluster in cluster c_i, i.e. $j* = \text{argmax}_j\{|c_i \cap \psi_j|\}$.

4.3 Results and Analyses

Is it possible to blindly cluster the Instagram photos? We randomly selected 1800 images filtered by 18 different filters (including the 'Normal' class),

each responsible for 100 images. As can be seen in Table 1, the low recall rates indicate the failure of the clustering as many small or singleton clusters are produced. If we assume that the filters do not affect the SPN at all, there will be 72 images from each camera on average. Given the results reported in [21], clustering such a dataset is an easy task and a high $\mathcal{F}$ should be expected for the clustering algorithm described in [21]. However, the rather contradictory results presented in Table 1 imply that the photo filters severely affect the SPN and make direct clustering on Instagram photos infeasible.

Color channel	$\mathcal{F}(\%)$	$\mathcal{R}(\%)$	$\mathcal{P}(\%)$
Red	7.78	4.16	60.28
Green	7.59	4.06	58.67
Blue	7.63	4.08	58.56

Table 1: Clustering results on unclassified images.

How different filters affect the SPN? We then investigate the effect of individual filters on the performance of SPN-based image clustering. We randomly selected 1000 images from the 25 cameras for each filter. To make sure the comparison of clustering performance between the filters is representative and unbiased, images selected for each filter are generated from the same set of the original images. Table 2 shows the clustering results based on the noise residuals from R, G, B channels for different filters. The highest F1-measure among the three color channels is highlighted in bold for each filter. Based on the performance difference relative to the 'Normal' class, we divide the 17 filters into two groups:

- Group I (filters highlighted in the violet background in Table 2). The clustering on the images processed by the filters in this group fails completely, with an F1-measure of 12.38%. Further investigation reveals that the clustering algorithm produces a singleton cluster containing all the images processed by each filter, which indicates the filters in this group greatly damage the SPN in the image. The 1000 test images for each filter are selected randomly from 25 cameras. The most common source camera for the test images contributes 66 images, which accounts for the F1-measure of 12.38% in a singleton cluster of 1000 images.

- Group II (filters highlighted in the green background in Table 2). The highest $\mathcal{F}$ among different color channels is comparable to that of the 'Normal' class. So for the images processed by the filters in this group, SPN-based techniques are still effective for analyzing the provenance. Furthermore, the clustering performance stays quite stable across different color channels, with the exception of 'LordKelvin' filter, which applies radical adjustments to the blue channel.

For all the filters we have tested in this paper, it might be a little surprising to see that the green channel delivers a better (or at least comparable) performance

than the other two color channels. So, without any prior information about the applied filters, the best bet would be to apply analysis on the SPN extracted from the green channel.

Filters	$\mathcal{F}(\%)$		
	Red	Green	Blue
Normal	85.83	**85.96**	86.4
1977	77.45	**85.90**	72.21
Amaro	12.38	**12.38**	12.38
Brannan	85.05	**85.61**	83.84
Earlybird	**87.06**	85.96	82.62
Hefe	12.38	**12.38**	12.38
Hudson	12.38	**12.38**	12.38
Inkwell	85.75	**85.75**	85.75
Lomofi	84.7	**87.07**	82.39
LordKelvin	82.08	**86.58**	36.71
Nashville	82.97	**85.75**	81.99
Rise	12.38	**12.38**	12.38
Sierra	12.38	**12.38**	12.38
Sutro	12.38	**12.38**	12.38
Toaster	12.38	**12.38**	12.38
Valencia	84.43	85.13	**85.65**
Walden	85.17	**86.27**	80.22
XproII	84.76	**85.29**	83.71

Table 2: Clustering results for different Instagram filters using SPNs extracted from different color channels.

Is it possible to identify the applied filter? We have seen that for the filters in Group I, the clustering fails completely for all three color channels. Therefore, for the reliability of forensic investigations, the images processed by those filters should be identified beforehand and excluded in the subsequent provenance analysis. For this purpose, we train three photo filter classifiers with the same network architecture depicted in Fig. 1, using the unprocessed images (with filters applied), denoised images and noise residuals, respectively. We train each network for 50 epochs using the cross-entropy loss function and a learning rate of 0.002. $96,660$ images in the dataset are split into training, validation and test sets with a ratio of $60\% : 20\% : 20\%$.

We evaluate the trained classifiers on $19,332$ test images and show the detailed classification results for individual filters in terms of $\mathcal{P}$ and $\mathcal{R}$ in Table 3. On average, the $\boldsymbol{I}$-net, $\hat{\boldsymbol{I}}$-net, and $\hat{\boldsymbol{I}}$-net achieve an accuracy of 79.91%, 86.93% and 88.38%, respectively. It shows that by training with the de-noised images or noise residuals, a better overall classification performance can be achieved.

Though $\boldsymbol{I}$-net and $\hat{\boldsymbol{I}}$-net have seemingly good overall classification accuracy, they may be problematic in some cases. Taking the 'Normal' class as an example, the recall and precision rates of $\boldsymbol{I}$-net and $\hat{\boldsymbol{I}}$-net are considerably lower compared to $\boldsymbol{n}$-net, which makes $\boldsymbol{I}$-net (52.89%) and $\hat{\boldsymbol{I}}$-net (66.76%) unsuitable for identifying the images with no filter applied at all. For an original natural image, although no filter is applied, it may look like as if a specific filter has been applied just because its content tends to be similar to the filter's artistic style. So as pointed out in [18], the image content and artistic style always co-exist in natural images, which makes it difficult to classify different filters (or artistic styles) for the original images. In contrast, the precision rate of $\boldsymbol{n}$-net (98.53%) on classifying original images is nearly perfect because by using the noise residuals as the input data, the network is less affected by the image content and focuses more on the features that can differentiate the original images from other filtered images.

Filters	$\mathcal{R}$(%)			$\mathcal{P}$(%)		
	$\boldsymbol{I}$-net	$\hat{\boldsymbol{I}}$-net	$\boldsymbol{n}$-net	$\boldsymbol{I}$-net	$\hat{\boldsymbol{I}}$-net	$\boldsymbol{n}$-net
Normal	65.55	67.69	**93.48**	52.89	66.76	**98.53**
1977	79.14	**92.36**	92.09	86.47	**91.68**	89.75
Amaro	69.55	83.33	**84.17**	**83.74**	79.27	73.80
Brannan	**94.41**	87.62	91.24	72.90	**91.72**	82.35
Earlybird	85.85	95.16	**96.00**	84.90	**88.03**	72.61
Hefe	**85.94**	85.01	84.08	83.00	87.79	**94.55**
Hudson	91.90	95.07	**98.70**	87.58	90.11	**98.15**
Inkwell	56.42	94.88	**98.60**	94.10	90.66	**95.66**
Lomofi	69.46	68.53	**73.09**	58.88	69.50	**90.54**
LordKelvin	94.97	92.55	**95.44**	90.19	93.86	**97.53**
Nashville	85.57	**94.04**	80.26	81.76	**92.24**	89.60
Rise	64.62	**77.28**	72.16	80.32	**86.82**	80.31
Sierra	77.09	81.01	**95.53**	72.44	80.04	**98.65**
Sutro	88.27	**92.74**	92.55	87.21	**95.22**	90.12
Toaster	92.27	96.00	**97.21**	**98.21**	97.45	94.90
Valencia	69.55	77.37	**78.21**	66.11	78.40	**82.27**
Walden	88.83	94.04	**96.09**	91.47	**95.92**	80.56
XproII	78.96	**90.13**	71.88	87.78	90.21	**91.69**

Table 3: Classification performance of $\boldsymbol{I}$-net, $\hat{\boldsymbol{I}}$-net, and $\hat{\boldsymbol{I}}$-net, which are trained with three different types of data: the unprocessed images $\boldsymbol{I}$ (with filters applied), denoised images $\hat{\boldsymbol{I}}$ and image noise residuals $\boldsymbol{n}$, respectively.

As the images manipulated by the filters in Group I are not suitable to be used in SPN-based provenance analyses, we need to move one step further to differentiate the filters from the two groups, so we further conduct a binary group-wise classification to classify the images into two groups corresponding to the Group I and II in Table 2. The confusion matrix for the group-wise

classification by the three classifiers is shown in Table 4. We can see that the $\boldsymbol{n}$-net clearly outperforms the other two classifiers with higher true positive rates and lower false rates. It shows that by applying the $\boldsymbol{n}$-net to classify the images before provenance analysis, we will be able to identify and exclude the majority (96.83%) of the images in Group I and only discard a very small portion (1.61%) of the images with reliable SPN in Group II. This will greatly help the forensic investigators to reduce the size of data to be analyzed and make the results from SPN-based techniques more trustworthy.

Actal/Predicted	$\boldsymbol{I}$		$\hat{\boldsymbol{I}}$		$\boldsymbol{n}$	
	Group I	Group II	Group I	Group II	Group I	Group II
Group I	0.8889	0.1111	0.9258	0.0742	**0.9683**	**0.0317**
Group II	0.0468	0.9532	0.0416	0.9584	**0.0161**	**0.9839**

Table 4: Confusion Matrix for the classification of the Group I and Group II Instagram filters.

5 Conclusions and Future Work

In this work, we have shown that some Instagram filters, i.e. the filters in Group I, can significantly attenuate or modify the SPN signal in the images and thus hinder the SPN-based image provenance analysis, while some other filters, i.e. the filters in Group II, well preserve the SPN in the images. Furthermore, due to the varying quality of the preserved SPNs across different image filters, separate treatments are needed for the images processed by different filters when we conduct SPN-based provenance analysis on Instagram photos. We also show that it is possible to identify the filter applied to an image by training a CNN-based classifier. We trained three classifiers of the same network architecture with three different types of inputs: the unprocessed images (with filters applied), the denoised images and the noise residuals. We found that the classifier trained with the noise residuals clearly outperforms the other two classifiers, with an accuracy of more than 96% in identifying the filters in Group I and II. We believe this work can help the forensic investigators to pre-process the images and facilitate the reliable SPN-based provenance analysis for Instagram photos. As the future work, we will conduct a larger-scale evaluation to cover more Instagram filters and extend this work to the analysis of the data on other social media platforms.

Acknowledgment

This work is supported by the EU Horizon 2020 Marie Sklodowska-Curie Actions through the project entitled Computer Vision Enabled Multimedia Forensics and People Identification (Project No. 690907, Acronym: IDENTITY)

References

1. Lukas, J., Fridrich, J., Goljan, M.: Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensics Security 1(2), 205–214 (2006)
2. Chen, M., Fridrich, J., Goljan, M., Lukás, J.: Determining image origin and integrity using sensor noise. IEEE Trans. Inf. Forensics Security 3(1), 74–90 (2008)
3. Hu, Y., Yu, B., Jian, C.: Source camera identification using large components of sensor pattern noise. In: Proc. Int. Conf. Computer Sci. its Appl. pp. 291–294 (2009)
4. Li, C.T.: Source camera identification using enhanced sensor pattern noise. IEEE Trans. Inf. Forensics Security 5(2), 280–287 (2010)
5. Kang, X., Li, Y., Qu, Z., Huang, J.: Enhancing source camera identification performance with a camera reference phase sensor pattern noise. IEEE Trans. Inf. Forensics Security 7(2), 393–402 (2012)
6. Lin, X., Li, C.T.: Preprocessing Reference Sensor Pattern Noise via Spectrum Equalization. IEEE Trans. Inf. Forensics Security 11(1), 126–140 (2016)
7. Lin, X., Li, C.T.: Enhancing sensor pattern noise via filtering distortion removal. IEEE Signal Process. Lett. 23(3), 381–385 (Mar 2016)
8. Bloy, G.J.: Blind camera fingerprinting and image clustering. IEEE Trans. Pattern Anal. Mach. Intell. 30(3), 532–534 (2007)
9. Li, C.T.: Unsupervised classification of digital images using enhanced sensor pattern noise. In: Proc. IEEE Int. Symp. Circuits Syst. pp. 3429–3432 (May 2010)
10. Caldelli, R., Amerini, I., Picchioni, F., Innocenti, M.: Fast image clustering of unknown source images. In: Proc. IEEE Int. Workshop Inf. Forensics Security. pp. 1–5 (Dec 2010)
11. Lin, X., Li, C.T.: Large-scale image clustering based on camera fingerprints. IEEE Transactions on Information Forensics and Security 12(4), 793–808 (Apr 2017)
12. Goljan, M., Fridrich, J., Filler, T.: Large scale test of sensor fingerprint camera identification. In: IS&T/SPIE Electronic Imaging. pp. 72540I–72540I. Int. Society for Optics Photonics (2009)
13. Gloe, T., Böhme, R.: The dresden image database for benchmarking digital image forensics. J. Digital Forensic Practice 3(2-4), 150–159 (2010)
14. Satta, R., Stirparo, P.: On the usage of sensor pattern noise for picture-to-identity linking through social network accounts. In: International Conference on Computer Vision Theory and Applications (VISAPP). vol. 3, pp. 5–11 (Jan 2014)
15. Caldelli, R., Becarelli, R., Amerini, I.: Image origin classification based on social network provenance. IEEE Transactions on Information Forensics and Security 12(6), 1299–1308 (June 2017)
16. Amerini, I., Uricchio, T., Caldelli, R.: Tracing images back to their social network of origin: A cnn-based approach. In: 2017 IEEE Workshop on Information Forensics and Security (WIFS). pp. 1–6 (Dec 2017)
17. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556 (2014)
18. Gatys, L.A., Ecker, A.S., Bethge, M.: A neural algorithm of artistic style. arXiv preprint arXiv:1508.06576 (2015)
19. Shullani, D., Fontani, M., Iuliani, M., Shaya, O.A., Piva, A.: Vision: a video and image dataset for source identification. EURASIP Journal on Information Security 2017(1), 15 (Oct 2017)
20. Dabov, K., Foi, A., Katkovnik, V., Egiazarian, K.: Image denoising by sparse 3-d transform-domain collaborative filtering. IEEE Trans. Image Process. 16(8), 2080–2095 (Aug 2007)

21. Li, C.T., Lin, X.: A fast source-oriented image clustering method for digital forensics. EURASIP J. Image Video Process.: Special Issues on Image and Video Forensics for Social Media analysis 1, 69–84 (Oct 2017)