Picture-to-Identity linking of social network accounts based on Sensor Pattern Noise

Riccardo Satta* **and Pasquale Stirparo*+**

* Institute for the Protection and Security of the Citizen,
Joint Research Centre (JRC), European Commission, Ispra (VA), Italy
+Royal Institute of Technology (KTH), Stockholm, Sweden
{riccardo.satta, pasquale.stirparo}@jrc.ec.europa.eu

Keywords: social network, Sensor Pattern Noise, identity, linking, digital image forensics

Abstract

The widespread diffusion of digital imaging devices fuelled a growing interest on photo sharing through social networks. Nowadays, Internet users continuously leave visual "traces" of their presence and life on the Internet, which can constitute precious data for forensic investigators. *Digital Image Forensics* tools are used to analyse such images and collect evidences. One of such tools is the Sensor Pattern Noise (SPN), that is, an unique "fingerprint" left on a picture by the source camera sensor. In this paper, we propose and experimentally test a novel usage of SPN, to find social network accounts belonging to a person of interest, who has shot a given photo. We name this task *Picture-to-Identity linking*, and believe it can be useful in a variety of forensic cases, e.g., finding stolen camera devices, cyber-bullying, or on-line child abuse. We evaluate two methods for Picture-to-Identity linking based on two existing SPN comparison techniques, on a benchmark data set of publicly accessible social network accounts collected from the Internet. The reported results are promising and show that such technique has a practical value for forensic practitioners.

1 Introduction

Digital imaging devices have gained a prominent role in everyone's life. The general availability of affordable mobile smart-phones, tablets, digital cameras and camcorders has indeed contributed to this, and has fuelled a growing interest for sharing life moments using social networks (e.g., Facebook, Flickr) and Internet in general. As a consequence, many people continuously leave visual "traces" of his/her presence and life on the Internet. Unfortunately, often these traces can be easily accessed by others outside the network of friends/contacts: in fact, many social networks do not implement the privacy-by-default principle (i.e., default settings do not guarantee user privacy). On the other hand, under the proper legal framework law enforcement bodies and forensic investigator can access this data (e.g., in undercover operations) in case it is relevant for investigations.

The task of analysing digital images for forensic purposes is usually referred to as *digital image forensics*. In this field, recently introduced techniques able to extract a unique "fingerprint" of the camera that shot a picture [4, 9, 14] have set the way for a series of useful tools for the forensic investigator. In particular, the Sensor Pattern Noise (SPN) left in a picture by the device sensor has been exploited in various forensic tasks, e.g., source device identification [14], forgery detection [10], source device linking [5], or clustering of images with respect to the source camera [10].

In this paper, we propose a novel usage of the SPN for digital image forensic purposes. We exploit SPN fingerprints to find social network accounts belonging to a certain individual of interest, who has shot a given, known photo. We name this task *Picture-to-Identity linking*, and believe it can be useful in a variety of forensic cases, e.g., on-line child abuse, cyber-bulling, finding stolen camera devices. To the best of our knowledge, this application of the SPN has never been proposed in the literature so far. We developed two implementation of Picture-to-Identity linking that extract the SPN using the method proposed by [14], and based on two different SPN comparison methods, Normalised Cross-Correlation ([14]) and Peak to Correlation Energy ([6]). We tested them on a benchmark data set of social network accounts collected from the Internet. We report promising results that show evidence of the practical usefulness of such technique for forensic investigators.

The rest of the paper is structured as follows. First, in Sect. 2 we review previous works on source camera identification, with particular regard to SPN. We then focus in greater detail on the usage of SPN for Picture-to-Identity linking in Sect. 3, providing an overview of the possible concrete applications and of the challenges that must be expected. Sect. 4 describes and formalises a method for Picture-to-Identity linking, that is then experimentally tested on a benchmark data set in Sect. 5. Finally, Sect. 6 draws up conclusions and suggests possible directions for further research on this topic.

2 Related Work

Digital images are usually associated to various kinds of useful *metadata*. Examples are Exif data, image tags, or text as-

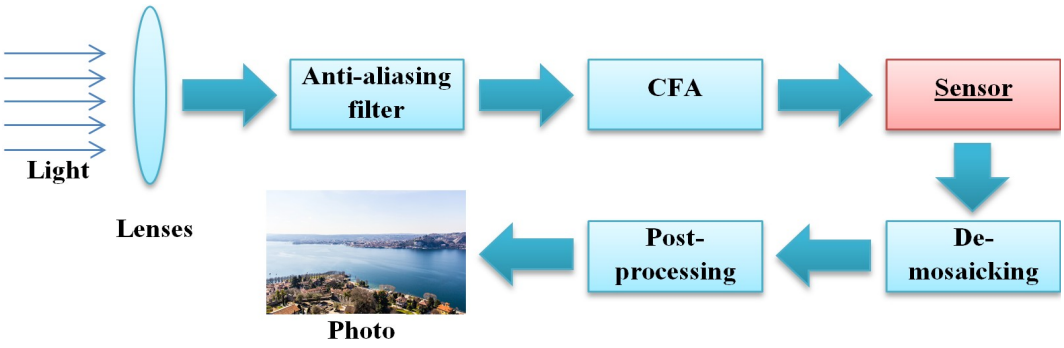

Figure 1: Image acquisition pipeline in typical camera devices.

sociated to the image (e.g., contained in the same web page), etc. Exif metadata has in particular received much attention by forensic investigators, as it stores various useful information about the device (e.g., camera model, serial number, etc.) that produced the content. However, from a forensic viewpoint, this information must be taken into account with extreme care; in fact, it is fairly easy to modify or remove it with image processing software (e.g., Photoshop) as well as with free tools available on the Internet (e.g., ExifTool). A robust cue, which can be used in place of Exif data to identify the source camera of a picture, is the noise pattern left by the sensor element of the camera (usually referred to as Sensor Pattern Noise or SPN) [14]. In fact, such noise pattern is univocal of a camera sensor, and can be seen as an unique fingerprint that identifies an individual device.

To understand how the SPN can be used as a fingerprint, it is worth to take a closer look at how a digital picture is typically produced by a camera [9] (refer to Fig. 1 for a clarifying scheme). The light coming from the scene arrives first to the camera lens. Then, it passes through an anti-aliasing filter, and reaches a Colour Filter Array (CFA), placed just over the sensor and used to capture one colour channel per pixel. The light finally reaches the sensor; essentially, it is a matrix of elementary sensitive elements, each corresponding to a pixel, that converts light into a digital representation. The subsequent steps, de-mosaicking and post-processing, are respectively in charge of interpolating the missing two colours of each pixel, and of carrying out image processing operations (e.g., white balancing, de-noising, etc.) to increase the perceived image quality. Each step of this pipeline leaves artefacts on the image, which can be used as a *signature* of the camera device.

Much research has been conducted in this direction, exploiting SPN [8, 9, 10, 14], interpolation artefacts caused by de-mosaicking filter [1, 13, 15] and JPEG compression [16], traces of dust in the sensor [4], or lens aberrations [3, 17], as possible fingerprints. Out of them, de-mosaicking and JPEG compression artefacts depend on the algorithms chosen by the manufacturer, which are usually specific of the model; therefore, they can be used only as a signature of the camera model (not of individual cameras). Dust traces affect mainly professional reflex cameras with interchangeable lens (dust may enter inside the camera when the photographer changes the lens) and constitute a fingerprint of the single device, that however exhibits a low stability over time (i.e. new dust particles may be deposited into the sensor). Regarding lens aberrations, their use as device fingerprint has been tested in a limited extent [3, 17] and its actual potential is still to be explored.

Differently to the aforementioned techniques, the Sensor Pattern Noise has the desired characteristics of uniqueness and stability, and has been studied and tested in various forensic tasks, e.g.: source device identification [8, 9, 10, 12, 14], forgery detection [10], source device linking [5], clustering of images with respect to the source camera [10].

Most techniques extract the SPN by exploiting the additive noise model first presented by [14], that models the SPN as an additive, high frequency noise. In the wavelet domain, this can be formulated as:

$$n_P = DWT(P) - F\big(DWT(P)\big) \tag{1}$$

where P is a picture, n_P is the SPN of P, $DWT(\cdot)$ is the Discrete Wavelet Transform, and F is a de-noising filter which extracts the low-frequency (non-noise) components of P. The de-noising filter F used indeed plays a crucial role. An effective one is the wavelet-based filter described in Appendix A of [14], which has been used in many other works [9, 10, 12].

In order to compare two SPNs n_{P1} and n_{P2} from two images $P1$ and $P2$, a common approach [9, 10, 12] is to evaluate the Normalised Cross-Correlation, which is defined as

$$\rho(n_{P1}, n_{P2}) = \frac{(n_{P1} - \bar{n}_{P1}) \cdot (n_{P2} - \bar{n}_{P2})}{\|n_{P1} - \bar{n}_{P1}\| \cdot \|n_{P2} - \bar{n}_{P2}\|} \tag{2}$$

where $\bar{n}_{P1}$ and $\bar{n}_{P2}$ are the means of n_{P1} and n_{P2}, respectively. The value of $\rho(n_{P1}, n_{P2})$ can be taken as a *matching score* between n_{P1} and n_{P2}.

In case of misalignment of the two SPNs n_{P1} and n_{P2} (e.g., due to cropping), a better approach, as proposed by Goljan et al. [6], is to evaluate the correlation on a range of possible shifts between the two images, and take the maximum:

$$\hat{\rho}(n_{P1}, n_{P2}) = \max_{s_1, s_2} \rho(s_1, s_2; n_{P1}, n_{P2}) \tag{3}$$

where s_1 and s_2 are the horizontal and vertical shifts respectively, and $\rho(s_1, s_2; n_{P1}, n_{P2})$ is the Normalised Cross-Correlation (NCC) between n_{P1} and n_{P2} when a shift (s_1, s_2) is applied to n_{P2}. The similarity value between n_{P1} and n_{P2}

is then defined as the Peak to Correlation Energy (PCE) ratio, that is, the ratio between $\hat{\rho}(n_{P1}, n_{P2})$ and the average correlation (the reader is referred to [6] for further details).

3 Picture-to-Identity Linking using SPN

Most social networks (e.g., Facebook, Google Plus) offer users the possibility to upload pictures to enrich their profile. Some social networks, like Flickr and Ipernity, are entirely devoted at sharing photos. Indeed, from a forensic viewpoint, these personal accounts may offer useful information for investigations.

Finding social networks accounts that belong to a certain person of interest (e.g., who is relevant for a case) can be therefore very valuable. The task is non-trivial, even if one knows identity details. In fact, one should expect to find several homonyms, and the person of interest may use a pseudonym or a nick name. Nevertheless, from the perspective of digital forensics investigations, being able to go back to the person who shot a certain picture(s) is important in several scenarios. Here we mention three of them, varying from lower to higher level of seriousness.

The first one is the case of a stolen smart-phone. After the theft, the thief will possibly start using the smart-phone, taking pictures and sharing them on-line on social platforms. Having already pictures taken by the victim as sample, using the methodology we propose in this paper it would be possible to find the social network account of the thief and consequently identify him/her. Another scenario is the case of defamation torts. Once they mainly used to happen verbally (e.g. during public speeches) or in a written form (e.g. releasing interviews to the newspaper), nowadays in the Internet era they are often perpetrated posting on websites/social networks pictures of which the targeted person may be ashamed of, maybe because taken without he/she being aware of it. A clear example of this is cyber-bullying. With a Picture-to-Identity linking technique, these defaming images could be linked to an account of the creator. Finally, another crime that heavily involves digital forensics, is the on-line abuse of children, where the perpetrators often record moments of the ongoing crime by different means, taking videos or photos to later share them over the Internet (On-line Child Abuse). In such cases, being able to identify the perpetrator as soon as possible is important due to the serial habit of this type of criminals in committing such crimes. Again, our proposed technique could be conveniently used to find a social network account of the perpetrator (even if it contains legal images only), using the offending images as query.

In this work, we propose to use the SPN signature as a mean to find social network accounts belonging to the person that has shot a given photo. In other words, we aim at answering the question: *Given a picture P^*; how can I find an account belonging to the person who shot P^*?* We name this task *Picture-to-Identity Linking* (see Fig. 2), and propose to address it by using the SPN. To the best of our knowledge, the task above has never been presented in the literature so far. The rationale behind our proposal is that social network accounts might contain pictures taken with the digital imaging device(s) of the

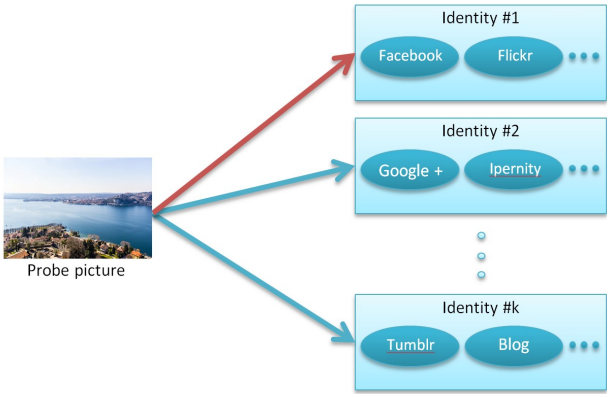

Figure 2: Picture-to-Identity Linking.

account owner. Given a *probe* picture P^*, one can extract its SPN and compare it against the SPNs of the pictures from a social network account. If a match is found, this means that the account contains a picture taken by the same camera of P^*; in turn, the owner of the account is likely to be the person who shot P^*.

Picture-to-Identity linking via SPN poses several challenges. Among them we highlight:

- **Differences in image size**. The size of the probe image P^* and of the social network images can differ, e.g. because images uploaded to the social network are automatically resized (this is the case, for instance, of Facebook). In turn, SPN sizes will differ and will not be directly comparable.

- **SPN misalignment**. The probe image P^* and/or the social network images might have been cropped by the author; consequently, the SPNs might be misaligned.

- **JPEG compression**. Most images taken with digital imaging devices are compressed using JPEG. Some social networks might further compress them automatically after uploading. JPEG compression degrades the SPN as it attenuates or destroys high frequency image components.

- **Image alteration**. Images can be altered for artistic purposes (e.g., contrast enhancement, HDR processing, or other visual effects). Any such image alteration in turn modifies the SPN.

- **Different ISO settings**. Images shot in low light conditions will have a higher ISO, and thus show a stronger noise. On the contrary, images taken in good lighting conditions will have a low ISO and less noise.

Despite the challenges above, we will show that the Picture-to-Identity linking via SPN is feasible, and could be used as a tool for forensic investigations. A practical implementation of our proposal is presented in the next Section.

4 Method Overview and Implementation

In this Section, we describe our method to perform Picture-to-Identity linking via SPN. We formalise the problem as follows. Let P^* be a probe (target) image, and let us define $\mathbf{I} = \{\mathsf{A}_i\}$, $i = 1,m$ the set of m social network accounts A_i that belong to the person/identity $\mathbf{I}$. Let then $\mathbb{I} = \{\mathbf{I}_j\}$, $j = 1,k$ be a set of k candidate identities, each associated with her own set of accounts $\mathbf{I}_j$.

The problem of Picture-to-Identity linking can be formulated as finding the identity $\mathbf{I}^*$ which owns the account containing the image with highest matching score to P^* (Fig. 2). Formally:

$$\mathbf{I}^* = \arg\max_{\mathbf{I}_j} S(P^*, \mathbf{I}_j) \, , \mathbf{I}_j \in I \tag{4}$$

where $S(P^*, \mathbf{I})$ is the *identity score*, i.e., the maximum SPN matching score between the SPN extracted from P^* and each image of each account own by identity $\mathbf{I}$:

$$S(P^*, \mathbf{I}) = \max_{\mathsf{A} \in \mathbf{I}} \max_{P \in \mathsf{A}} \text{score}(\mathrm{n}_{P^*}, \mathrm{n}_P) \tag{5}$$

and $\text{score}(\mathrm{n}_{P^*}, \mathrm{n}_P)$ can be computed either by means of NCC or PCE ratio (see Sect. 2).

In practice, due to the problems stated in Sect. 3, the probability of wrong identification may be high (see next Sect. 5). Thus, in a practical implementation of the above technique, for a given probe P^* it is better to show an *ordered list* of the candidate identities $\{\mathbf{I}^*_1, \mathbf{I}^*_2, \ldots, \mathbf{I}^*_k\}$, ranked with respect to their score $S(P^*, \mathbf{I}*_j)$.

For the extraction of the SPN, we used the additive model of Eq. (1) with the Wavelet-based filter proposed by Lukas et al. [14]. Since the reliability of the SPN is usually better in the central portion of the image [11, 12], before extracting it the image is cropped by taking a 256×256 pixels window in the image centre.

5 Experimental Results

We evaluated the performance of the method presented above in the task of Picture-to-Identity Linking, on a data set of 2896 images, taken from social network accounts and/or personal blogs belonging to 15 different identities. For each identity, we found two social network accounts. All the accounts were publicly accessible (i.e., not restricted to friends only). The number of images per account, and the account type, are listed in Table 1. Images vary in size and are mostly small. In fact, in many social networks (e.g., Facebook) pictures are automatically scaled to a small size to fit better to the web page layout. Other social networks (e.g., Flickr) offer a low resolution preview of the image, and bigger versions of the same picture can be accessed by clicking on the preview. In these cases, we took the preview image only. Before extracting the SPN, and in order to make them comparable, each image is (i) rotated so that it has a landscape orientation (if necessary) and (ii) resized so that the long side has a length of 4096 pixel, keeping the aspect-ratio.

Identity	Accounts (Nr. of images)	Total nr. of images
#1	Flickr (158), Personal blog (83)	241
#2	Facebook (105), Flickr (118)	223
#3	Flickr (91), Facebook (73)	164
#4	Facebook (104), Personal blog (79)	183
#5	Flickr (74), Google Plus (36)	110
#6	Facebook (101), Flickr (144)	245
#7	Flickr (159), Facebook (43)	203
#8	Facebook (56), Flickr (113)	169
#9	Flickr (98), Personal blog (21)	119
#10	Google Plus (99), Flickr (112)	211
#11	Flickr (109), Facebook (184)	293
#12	Facebook (62), Flickr (39)	101
#13	Flickr (172), Facebook (32)	204
#14	Facebook (51), Flickr (133)	184
#15	Flickr (193), Facebook (100)	293

Table 1: Composition of the data set used for benchmark. For each social network account, the number of images is shown in brackets.

		Estimated identity														
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15
Real identity	#1	**130**	16	5	5	8	3	7	5	3	2	6	4	1	37	9
	#2	28	**95**	11	5	6	11	13	6	5	10	3	7	2	10	11
	#3	3	19	**68**	1	2	41	2	4	0	4	2	1	2	13	2
	#4	3	18	0	**131**	0	2	2	8	2	4	1	4	1	3	4
	#5	4	6	2	1	**111**	3	3	3	5	4	14	4	1	1	1
	#6	4	20	44	1	2	**124**	6	2	3	1	6	6	2	6	18
	#7	10	18	5	4	7	5	**79**	11	5	3	15	6	6	8	20
	#8	11	7	5	2	4	13	12	**54**	16	7	9	4	6	8	11
	#9	7	11	3	3	13	3	8	12	**29**	3	10	6	2	5	4
	#10	3	7	1	4	1	0	2	2	1	**184**	0	2	0	2	2
	#11	8	10	2	2	14	9	17	10	16	4	**74**	9	8	4	6
	#12	8	11	3	5	2	5	5	2	7	2	8	**35**	5	1	2
	#13	2	3	1	2	4	3	2	4	1	1	7	3	**157**	11	3
	#14	34	14	6	1	6	2	9	12	5	1	4	2	13	**58**	17
	#15	24	21	2	16	3	20	28	16	3	5	8	4	2	29	**112**

Table 2: Picture-to-Identity confusion matrix using NCC.

		Estimated identity														
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15
Real identity	#1	**141**	13	1	1	7	2	4	8	3	0	7	3	1	28	22
	#2	30	**96**	14	7	4	10	12	8	1	4	2	4	5	9	17
	#3	4	8	**74**	1	2	43	0	4	1	4	3	2	3	9	6
	#4	2	8	0	**143**	0	2	0	5	1	1	1	4	4	1	14
	#5	6	6	0	2	**114**	3	7	3	4	3	9	1	3	2	0
	#6	4	3	42	2	1	**149**	0	2	3	0	11	2	6	6	14
	#7	13	9	2	0	5	2	**72**	15	6	3	21	5	11	10	28
	#8	14	8	5	0	2	9	9	**62**	10	5	14	3	6	10	12
	#9	14	1	4	0	9	4	9	15	**32**	2	12	2	4	8	3
	#10	4	2	1	0	1	1	0	3	1	**190**	1	0	1	0	6
	#11	12	4	2	1	12	11	17	7	14	1	**73**	9	12	4	14
	#12	9	3	2	3	4	6	1	2	8	1	12	**35**	9	3	3
	#13	3	2	2	0	3	2	1	5	0	0	9	1	**159**	14	3
	#14	39	13	9	0	4	3	5	8	2	0	5	3	14	**50**	29
	#15	27	16	3	8	3	21	12	13	1	2	11	1	1	27	**147**

Table 3: Picture-to-Identity confusion matrix using PCE.

Experiments have been carried out as follows. Each image of the data set was taken out from its source account and used as query image P^*; then, the identities were ranked with respect to the identity score, computed by means of Eq. (5), using the NCC and the PCE.

In Table 2 and Table 3 we show the identification performance, respectively using NCC and PCE to compute the identity score, in terms of confusion matrix. The (i, j)-th element of the matrix is the number of images coming from an account belonging to the identity i that has been classified as belonging to the identity j. The ranking performance, instead, has been assessed by means of Cumulative Matching Characteristic (CMC), and of Synthetic Recognition Rate (SRR) curves. The former is the cumulative probability of finding the correct identity within the first n ranks; the latter is the probability of

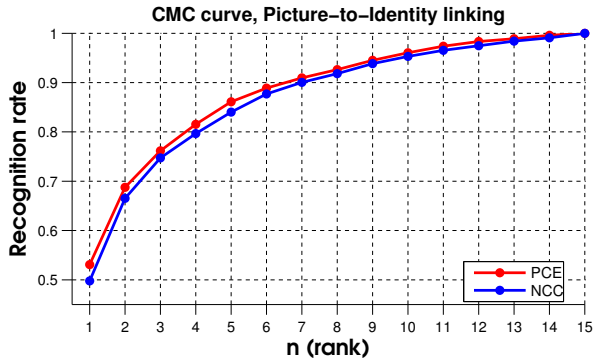

Figure 3: Picture-to-Identity linking performance, in terms of Cumulative Matching Characteristics curve, in a benchmark data set of 2896 images (see the text for details).

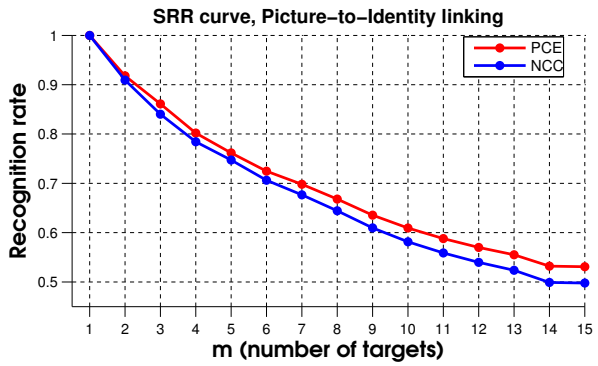

Figure 4: Picture-to-Identity linking performance, in terms of Synthetic Recognition Rate curve, in a benchmark data set of 2896 images (see the text for details).

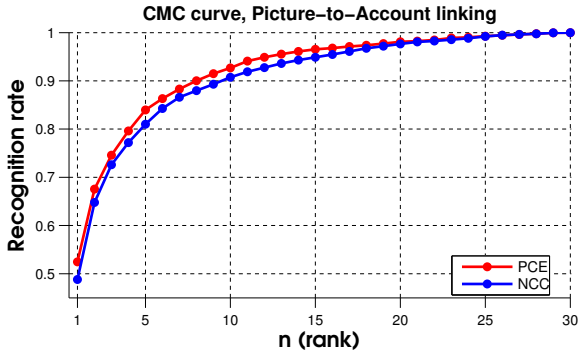

Figure 5: Picture-to-Account linking performance, in terms of Cumulative Matching Characteristics curve, in a benchmark data set of 2896 images (see the text for details).

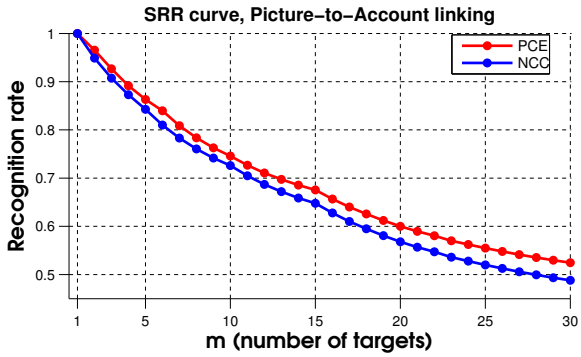

Figure 6: Picture-to-Account linking performance, in terms of Synthetic Recognition Rate curve, in a benchmark data set of 2896 images (see the text for details).

a correct recognition given m target identities. The SRR curve can be obtained from the CMC (hence the term *synthetic*) as $SRR(m) = CMC(k/m)$ where k is the number of identities [7]. The resulting plots are shown in Fig. 3 and Fig. 4, respectively.

Both NCC and PCE show a probability of correct recognition at the first rank of about 50%, with PCE showing a slightly better performance. This was expected, as the PCE technique is more robust than NCC to image cropping.

Such a performance is obviously not enough for a precise identification. One could argue that these scoring results do not qualify data as evidence for its admissibility in court. It is correct to state that an evidence as such shall be 100% attributable, as level of accuracy, to a subject (e.g. the victim, the suspect, etc.). However, there is a difference between forensic examination and digital investigation, the latter being far wider. In fact, following the scientific method applied to the digital forensics methodology [2], the investigation phase that precedes the production of evidences could be outlined as follows:

1. Data gathering and observation.
2. Hypotheses formation.
3. Hypotheses evaluation.
4. Conclusions and reporting.

Picture-to-Identity linking results can conveniently be used during (2) and (3), i.e., the formation of the hypotheses and their evaluation. Moreover, the complexity of computer systems in general requires awareness that individual pieces of digital evidence may have multiple interpretations, therefore contextualising and confining the information collected in the gathering phase, is of great importance in order to reach a correct conclusion. With all that said, a ranked list of candidate identities can be valuable for investigators and forensics practitioners exactly in circumstances where evidences lead to a pool of several people under suspicion. For example, if law enforcers are not able to identify and seize cameras belonging to each of the suspects, images taken from their social network accounts could be used as a set of candidates to test against the probe picture, using the ranking technique proposed in this paper. Another scenario is when the investigator knows, from other trails, certain characteristics related to the person of interest (e.g., nationality or ethnic group); accordingly, he/she focuses on a sub set of the ranked list, according to the presence/absence of such characteristics in the images. In all such cases, the proposed method would help to skim off the number of candidate identities related to the case, which, in conjunction with other facts, may speed up the investigation and increase its accuracy.

For the sake of completeness, we also evaluated the CMC and SRR curves in the task of associating each image with the

source account. In analogy with the terminology utilised so far in the paper, we refer to this task as *Picture-to-Account linking*. The corresponding plots are shown in Figs. 5-6. Note that, in this case, the number of targets is 30 (equal to the number of accounts), instead of 15 as in the previous experiment.

6 Conclusions

In this paper, we proposed a novel usage of SPN for digital image forensics, as a tool for finding social network accounts belonging to a certain person of interest, who has shot a given picture. This task, that we named Picture-to-Identity linking, has many potential applications, e.g., identification of perpetrators of On-line Child Abuse, of cyber-bullying, or of thefts of smart-phones. Yet, it is a challenging task, due to differences in image size, misalignment of the extracted SPNs, compression artefacts, and other issues.

We implemented Picture-to-Identity linking using the Wavelet-based filter proposed in [14] to extract the SPN, and used two techniques (namely, Normalised Cross Correlation and Peak to Correlation Energy ratio) to compare noise signatures. We evaluated the performance on a benchmark data set built using publicly accessible social network accounts. The reported results are promising; furthermore, we see room for various improvements. As an instance, the performance could be increased by combining the SPN information with other metadata (e.g., Exif data, if available), or with other camera identification techniques (e.g., de-mosaicking artefacts, dust traces).

It is worth to note the limited extent of the proposed evaluation, which is restricted to a small set of fifteen identities (and thirty social network accounts). Although we consider the size of our data set to be enough for a proof-of-concept analysis, Picture-to-Identity linking makes much more sense with a large-scale data base of social network accounts. The experimental evaluation provided can be seen as a simulation of the case when a set of "candidate" social network accounts has already been found by other means. One of the directions of future research will therefore be to design a large-scale test bed for Picture-to-Identity linking, and assess performance in a more general setting.

References

[1] Hong Cao and Alex C. Kot. Accurate detection of demosaicing regularity for digital image forensics. *IEEE Trans. on Inf. Forensics and Sec.*, 4(4):899–910, Dec. 2009.

[2] Eoghan Casey. *Handbook of Digital Forensics and Investigation*. Academic Press, 2009.

[3] Kai San Choi, Edmund Y. Lam, and Kenneth K. Y. Wong. Automatic source camera identification using the intrinsic lens radial distortion. *Optics Express*, 14(24):11551–11565, Nov. 2006.

[4] A. E. Dirik, H. T. Sencar, and N. Memon. Digital single lens reflex camera identification from traces of sensor dust. *IEEE Trans. on Information Forensics and Security*, 3(3):539–552, Sept. 2008.

[5] Jessica Fridrich. Digital image forensic using sensor noise. *IEEE Sig. Proc. Magazine*, 26(2):26–37, 2009.

[6] Miroslav Goljan, Jessica Fridrich, and Tom Filler. Large scale test of sensor fingerprint camera identification. In *Proc. SPIE, Electronic Imaging, Security and Forensics of Multimedia Contents XI*, pages 18–22, 2009.

[7] Douglas Gray, S. Brennan, and H. Tao. Evaluating appearance models for recognition, reacquisition, and tracking. In *10th IEEE Int. Workshop on Performance Evaluation of Tracking and Surveillance (PETS)*, 2007.

[8] Xiangui Kang, Yinxiang Li, Zhenhua Qu, and Jiwu Huang. Enhancing source camera identification performance with a camera reference phase sensor pattern noise. *IEEE Trans. on Information Forensics and Security*, 7(2):393–402, 2012.

[9] Chang-Tsun Li. Source camera identification using enhanced sensor pattern noise. *IEEE Trans. on Information Forensics and Security*, 5(2):280–287, June 2010.

[10] Chang-Tsun Li and Yue Li. Color-decoupled photo response non-uniformity for digital image forensics. *IEEE Trans. on Circuits and Systems for Video Technology*, 22(2):260–271, Feb. 2012.

[11] Chang-Tsun Li and Riccardo Satta. On the location-dependent quality of the sensor pattern noise and its implication in multimedia forensics. In *Proc. of the 4th Int. Conf. on Imaging for Crime Detection and Prevention 2011 (ICDP 2011)*, page 37, 2011.

[12] Chang-Tsun Li and Riccardo Satta. Empirical investigation into the correlation between vignetting effect and the quality of sensor pattern noise. *IET Computer Vision*, 6:560–566(6), Nov. 2012.

[13] Yangjing Long and Yizhen Huang. Image based source camera identification using demosaicking. In *2006 IEEE 8th Workshop on Multimedia Signal Processing*, pages 419–424, 2006.

[14] J. Lukas, J. Fridrich, and M. Goljan. Digital camera identification from sensor pattern noise. *IEEE Trans. on Information Forensics and Security*, 1(2):205–214, Nov. 2006.

[15] A.C. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. *IEEE Trans. on Signal Processing*, 53(10):3948–3959, Oct. 2005.

[16] Matthew James Sorrell. Digital camera source identification through jpeg quantisation. In Chang-Tsun Li, editor, *Multimedia forensics and security*. Information Science Reference, 2009.

[17] Lanh Tran Van, S. Emmanuel, and M.S. Kankanhalli. Identifying source cell phone using chromatic aberration. In *2007 IEEE Int. Conf. on Multimedia and Expo*, pages 883–886, 2007.