Smartphone Verification and User Profiles Linking Across Social Networks by Camera Fingerprinting

Flavio Bertini(✉), Rajesh Sharma, Andrea Iannì, and Danilo Montesi

Department of Computer Science and Engineering,
University of Bologna, Bologna, Italy
{flavio.bertini2,rajesh.sharma,andrea.ianni,danilo.montesi}@unibo.it

Abstract. In recent years, the spread of smartphones has attributed to changes in the user behaviour with respect to multimedia content sharing on online social networks (SNs). One noticeable behaviour is taking pictures using smartphone cameras and sharing them with friends through online social platforms. On the downside, this has contributed to the growth of the cyber crime through SNs. In this paper, we present a method to extract the characteristic fingerprint of the source camera from images being posted on SNs. We use this technique for two investigation activities (i) smartphone verification: correctly verifying if a given picture has been taken by a given smartphone and (ii) profile linking: matching user profiles belonging to different SNs. The method is robust enough to verify the smartphones in spite of the fact that the images get downgraded during the uploading/downloading process. Also, it is capable enough to compare different images belonging to different SNs without using the original images. We evaluate our process on real dataset using three different social networks and five different smartphones. The results, show smartphone verification and profile linking can provide 96.48 % and 99.49 % respectively, on an average of the three social networks, which shows the effectiveness of our approach.

Keywords: Pattern noise · Image fingerprint · Profile matching · Social network analysis · Online forensics

1 Introduction

In the last decade, many social platforms have invaded the web as well as mobile devices. These various networks model the specific needs of the users: social interactions, photo sharing, instant messaging to name a few, and users are often present across multiple social networks. Another important reason for the huge popularity of social platforms among users is the increase in usage of smartphones, which in turn has introduced changes in the user habits with respect to multimedia content on social networks [13].

An important problem across these social networks is that of fake profiles, which have seen a sharp increase in recent times. For example, *Facebook*'s most

J.I. James and F. Breitinger (Eds.): ICDF2C 2015, LNICST 157, pp. 176–186, 2015.
DOI: 10.1007/978-3-319-25512-5_12

recent annual report [8] has estimated that an average 8.35 % of its monthly active users are fake profiles.

In this paper, we deal with two problems (i) *smartphone verification*: the task to verify if a specific device is the source of given images and (ii) *user profiles linking*: the task to decide if a restricted set of user profiles (with different user ids or nicknames) belong to the same user. These two problems have their application in online forensics. Also, importantly, user profile linking is one of many kinds of missing data problem [14,15].

Recently, researchers exploited sensor imperfections to extract the fingerprint to identify a smartphone [2,6,7]. The concept behind a smartphone's fingerprint is similar to a human's fingerprint, which is used extensively in criminal investigations. The intuition behind the focus on smartphones are two. Firstly, smartphones are more personal than laptops or desktops, partially thanks to the hard bound phone contract. Secondly, and which is the base of our study, smartphones have various sensors, for example, camera, microphone-speaker [6], and accelerometer [7], which can be used to make a unique fingerprint of the device. Our proposed method is based on hardware imperfections of the built-in camera leveraging the fact that methods based on hardware imperfections provide better results than software imperfections [12].

We exploit the possibility of making a unique fingerprint of a smartphone based on the built-in camera imperfections, proposing a method robust enough that it does not get affected by the compression techniques used by various social networks. The smartphone camera fingerprint allows for linking different user profiles based on the pictures being posted on them, assuming the pictures have been taken with the same smartphone camera. In our experiments, we have compared the processed pictures from social networks with unprocessed ones and across social networks. The resulting method is strong enough to perform users linking from the sets of images belonging to different social networks and thus subject to different compression algorithms. In other words, it does not require original images for confirmation as original images might be difficult to obtain for various reasons such as for privacy and inaccessibility of the device. On an average of the three social networks, smartphone verification and profile linking can provide results of 96.48 % and 99.49 % respectively.

The rest of the paper is organized as follows. In Sect. 2 we briefly review the previous works related to smartphone fingerprinting techniques and forensic investigations on SNs. Section 3 describes our methodology. Section 4 presents the experiments and analyses of our results. Section 5 concludes the paper with future directions.

2 Related Works

In this section, we describe literature from three different domains, at the intersection of which our work lies. Firstly, we explain techniques to identify fingerprints of smartphone devices using various built-in sensors. Next, we describe various approaches proposed in the past for the source camera identification. In the last, we present methods to identify and match user profiles in SNs.

Fingerprinting the smartphones: Recently, researchers have proposed various techniques to fingerprint smartphones using built in sensors. For example, in [6] authors proposed a technique using speakers-microphones embedded in smartphones to uniquely fingerprint the individual devices through playback and recording of audio samples. The authors of [7] propose a method for identifying mobile phones based on the integrated accelerometers. In [2], authors exploit both (i) speakerphone-microphone and (ii) accelerometer calibration errors to de-anonymize the mobile devices.

Fingerprinting for source camera identification: Various techniques have been proposed for source camera identification. The manufacturing process of the camera introduces hardware defects. In [16] authors use the chromatic aberration to identify the source camera. In [12] it is shown that the Photo-Response Non-Uniformity (PRNU) is a unique feature of the sensor which is able to successfully distinguish between two cameras of the same brand and model. One of the main problems concerning the original Lukáš et al's algorithm presented in [12] is that it works correctly only with unscaled photos, because the footprint signal is of the same dimension of the image. To overcome this limitation, a method able to operate with different size images is proposed in [9]. To achieve our aim, that is, verifying the source camera and linking user profiles on SNs, we combine a PRNU-based method with a denoising algorithm to deal with the (unknown) compression methods of the SNs.

Identifying users in SNs: Despite SNs regulating their services very strictly, the large amount of data shared each day often includes information and content that go beyond what the law allows [18]. This has forced to increase the control and regulation of these platforms, seeing the evolution of new methods around social network forensics. In [1], authors proposed various solutions to extract information about user activities on various SNs from the smartphones. The method is made for Blackberry smartphones and cannot be used for all the devices, whereas our proposed method is device independent. There is great value in multimedia content that transits through SNs. In [10], the authors combine user ID and their tags to identify users across the social tagging system. In [11,17] researchers extract and use information about users' identities to match profiles belonging to the same user from different social networks, without compromising the privacy of the users, but the method fails if the malicious user falsifies his/her personal information, as it usually happens. Compared to all these approaches, our method does not only rely on the SN content, it verifies the user profiles and performs user profiles linking using smartphone's camera.

3 Methodology

First, we provide a small background in image processing as it is important in understanding the reasons behind the selection of our methodology. We then describe the procedure of verifying the image source. Finally, we explain the approach to test our method with different SNs and smartphones.

Images captured by cameras (smartphone cameras in this case) have two components, namely *signal* and *noise*. Technically the *signal* represents the information carrier, while the *noise* is an unavoidable effect on the signal due to many reasons.

The *noise* component can be categorise into a random and a deterministic component: the first one is the *shot noise* (or *photonic noise*), caused by factors such as brightness, temperature, humidity; the second one is the *pattern noise* which is systematic and regular. By systematic we mean it is present in every image, and regular signifies that it is present in the same location of every image captured by the same source (camera in this case).

3.1 Pattern Noise Extraction

We exploit a PRNU-based method [12] to extract the dominant part of the *pattern noise*, which is a regular component of the image and can be identified as average of residues of a large number of pictures. In particular, denoising algorithms [3] which are usually employed to clean up the image, can be used to remove the representative component of the image and thus leaving the noise component. If I represents the original image, RN the noise residuals and d the denoising function, then formally RN can be represented as $I - d(I)$. Then, the *pattern noise* PN_k, of the camera k can be approximated as the average residual noise of n images of the camera k [12]:

$$PN_k = \frac{1}{n} \sum_{j=1}^{n} RN_j \tag{1}$$

The denoising algorithm can affect the *pattern noise* computation, since it includes high-frequency details that might belong to signal component of the image. Although these errors can be reduced by increasing the number of samples, it is not always possible to acquire new samples (images). To address this, we have chosen the Block Matching 3D (BM3D) denoising algorithm [5] able to discern among high-frequency of noise and high-frequency of details and to deal with scaled photos.

As suggested in [5], we convert the colour images into the YCbCr color space. The Y identifies the luminance, while the Cb and Cr are the blue-difference and red-difference chroma components respectively. Then we take into account only the Y component that is the carrier of all high-frequency components (known as luminance noise) useful to determine the *pattern noise*.

3.2 Source Verification

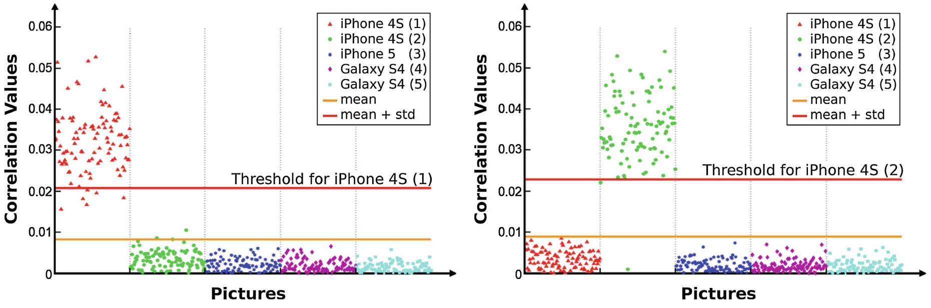
Let $\mathcal{N}_k$ represents the set of known images belonging to source k which is used for generating the PN_k (see Eq. 1 above). $\mathcal{U}_k$ defines the whole set of images taken by the source k. Also note $\mathcal{N}_k \subseteq \mathcal{U}_k$. Thus, we can define the set $\mathcal{S}$ as:

$$\mathcal{S} = \bigcup_k \mathcal{U}_k \setminus \mathcal{N}_k \tag{2}$$

The goal is to determine for each image $I \in \mathcal{S}$ whether it has been captured by the source k or not. To achieve this, we followed a two steps process. In the **first step**, we extract the residual noise RN from each image $I \in \mathcal{S}$, in order to apply the normalized correlation $corr(RN, PN_k)$ between each RN and PN_k as done in [12]:

$$\frac{(RN - \overline{RN})(PN_k - \overline{PN_k})}{\|(RN - \overline{RN})\|\|(PN_k - \overline{PN_k})\|} \tag{3}$$

In this way we compute the correlation between the unknown source of each image $I \in \mathcal{S}$ and each source k. We compute for each source k the mean μ_k of the correlation values an its standard deviation σ_k, then we define the threshold $\mathcal{T}_k$ as $\mu_k + \sigma_k$. In the **second step**, we decide that the camera k is the source of those images in $\mathcal{S}$ for which the correlation value is greater than the threshold $\mathcal{T}_k$. The reason behind this choice is that we know that some images in $\mathcal{S}$ originated from the camera k, and the correlation values have a characteristic distribution, as shown in Fig. 1.



(a) (b)

Fig. 1. Two examples of the distribution of correlation value of all the images in $\mathcal{S}$ using the fingerprints of two different devices. In (a) the threshold value is computed for the iPhone 4S (1) using $\mathcal{N}_1$, while in (b) for the iPhone 4S (2) using $\mathcal{N}_2$.

4 Evaluation

We describe the experimental settings and then the results of our experiments.

4.1 Experimental Setting

We choose five smartphones from two different brands, with two pairs of identical models (see Table 1). For each of these phones we have taken 200 high-resolution photographs under different conditions, in order to obtain independent samples and to reduce the random component of the noise (*shot noise*). We select three SNs: *Facebook*, *Google+* and *WhatsApp* for our analysis. Each of these SNs adopts different (unknown) compression algorithms, which lead to different characteristics in the image, summarized in Table 2. In all tests, we resize the images to compare pictures from different SNs.

Table 1. Smartphones' features.

ID	Brand	Model	Sensor	Resolution
1	Apple	iPhone 4s	CMOS	3264 × 2448
2	Apple	iPhone 4s	CMOS	3264 × 2448
3	Apple	iPhone 5	CMOS	3264 × 2448
4	Samsung	Galaxy S4	CMOS	4128 × 3096
5	Samsung	Galaxy S4	CMOS	4128 × 3096

Table 2. Characteristics of the SNs.

Service	Icon	Resolution	Quality
Facebook	f	960x720	medium
Google+	g+	2048x1536	high
WhatsApp	☎	800x600	low

4.2 Results

In this section, we present our results on the three tests, namely (i) original-by-original, (ii) social-by-social and (iii) cross-social. In each of these tests, to evaluate the classification process that allows to verify the source and link user profiles, we compute sensitivity (SEN) and specificity (SPE), which are well known statistical measures. In the context of this work, SEN indicates the ability of the method to correctly associate the images to the right source (i.e. smartphone or smartphone camera) and SPE as the ability to reject the other images.

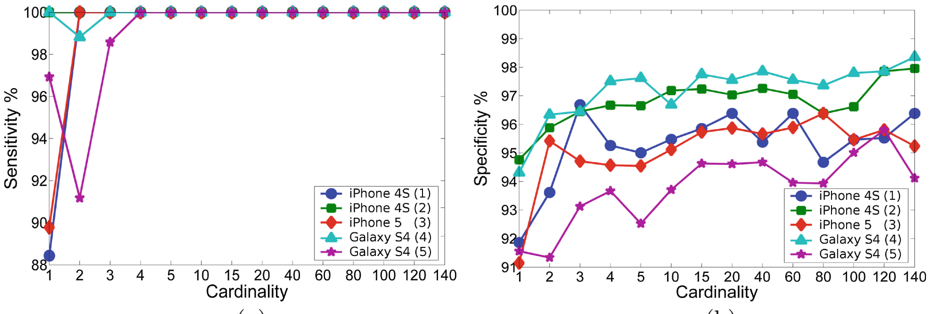
Let $\mathcal{S}_k$ represents the whole set of the images which belong to the source k. Out of all the images $\mathcal{S}_k$, let $\mathcal{S}_k^+$ signify the set of images that the algorithm has successfully assigned and those that it has not recognized is represented by $\mathcal{S}_k^-$, then we can define the **sensitivity** as:

$$SEN = \frac{|\mathcal{S}_k^+|}{|\mathcal{S}_k^+ \cup \mathcal{S}_k^-|} \tag{4}$$

Let $\widehat{\mathcal{S}}_k$ represents the whole set of the images which do not belong to the source k. Out of all the images $\widehat{\mathcal{S}}_k$, let $\widehat{\mathcal{S}}_k^-$ signify the set of images that the algorithm has successfully not assigned and those that it has wrongly recognized is represented by $\widehat{\mathcal{S}}_k^+$, then we can define the **specificity** as:

$$SPE = \frac{|\widehat{\mathcal{S}}_k^-|}{|\widehat{\mathcal{S}}_k^- \cup \widehat{\mathcal{S}}_k^+|} \tag{5}$$

Test 1: original-by-original: We first verify our approach on original images, that is images directly obtained from smartphones. The test is also helpful in determining the minimum cardinality of each set $\mathcal{N}_k$, with which the *pattern noise* can be correctly extracted. Starting with a single image, the cardinality is increased, according to the following sequence: 2, 3, 4, 5, 10, 15, 20, 40, 60, 80, 100, 120 and because of resource constraints, we limit our experiments to 140. For each cardinality, we first extract the *pattern noise* and compute the threshold $\mathcal{T}$ and then compute the sensitivity and specificity for the classification result of the images (Fig. 2). This process is repeated for each smartphone.



(a) (b)

Fig. 2. The graphs represent the sensitivity (a) and the specificity (b) results for each smartphone obtained by changing the cardinality of $\mathcal{N}_k$.

Based on the results we obtained, the cardinality of the subsets $\mathcal{N}_k$ is fixed to 100 images, for the following reasons: *(i)* starting from this value, specificity index has a good stability for each source; *(ii)* we preferred a wider value to curb the inherent difficulties of the denoising function [5] in discriminating the high frequencies. The cardinality of the set $\mathcal{S}$ is of 500 images as we fixed for each device a value of 100 images.

By setting the cardinality to 100 images, we calculate the sensitivity and specificity values for each device. The result shows that for each device, the method returns 100 % of sensitivity and 95 % of specificity (Fig. 3). In other words, in our experimental setup, the method is able to perform smartphone verification with 100 % correctness and is capable of rejecting at least the 95 % of images that does not belong to the right source.

Test 2: social-by-social: In the second test, the aim is to verify the robustness of the method when it is applied to images deteriorated by the uploading and downloading process of the SNs. This feature is extremely useful to verify which smartphone has taken and uploaded the images on SNs. In this test, all the images are previously uploaded and downloaded on the same SN. In practice, we use $\mathcal{N}_k^i$ to extract the *pattern noise* for each source k so as to classify the images in $\mathcal{S}^i$, where $i \in \{Facebook, Google+, Whatsapp\}$.

Among all the SNs, *Google+* returned highest sensitivity value that is of 100 % for all devices, and also it has the best specificity index with an average value of 97.56 %. This is due to the fact that *Google+* images are least compressed compared to the other two SNs (see Table 2). Although *Facebook* compresses the images more than *Google+*, the algorithm has return an average sensitivity values of 96.92 % and an average specificity value of 91.58 %. The third social network, *WhatsApp*, has given the worst results with an average sensitivity value of 92.52 % and an average specificity value of 90.84 %. This is probably due to the fact that *Facebook* and *Google+*, whose access is mainly done using computer with large screens, are bound to keep medium/high quality definition for the

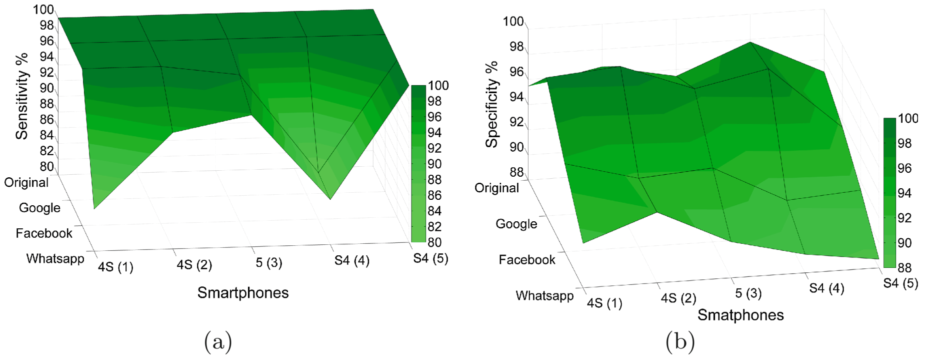


Fig. 3. Comparing the classification result values of the original images to those obtained by the downloaded images for (a) sensitivity and (b) specificity.

displayed images, while *WhatsApp*, being an application conceived for mobile devices, provides a much higher compression levels that reduces the information content of the image.

To understand the effectiveness of the algorithm, we compare the sensitivity and specificity of downloaded images with the original ones. Figure 3 shows the comparison of social-by-social with original-by-original for each device. We only show the range where is a change in values among the three SNs. On an average, our method is able to perform the smartphone verification using the images uploaded on the SNs with 96.48 % of sensitivity and 93.77 % of specificity.

Test 3: cross-social: In the final test which is the main contribution of our work, we want to demonstrate that it is possible to match a user profile on a SN using the images posted on various SNs. Moreover, it is possible to identify the source of certain images using the images posted on a user profile, the complementary of the previous test. The former case could be very useful if the smartphone is not available: the verification activity of the subject can be performed through another verified account on SN. While the latter case allows to perform a second important investigation activity, that is the ability to verify the source (smartphone) of the published images. This could be very useful to link a (fake) user profile with a smartphone. In this test, we use $\mathcal{N}_k^i$ to extract the *pattern noise* for each source k so as to classify the images in $\mathcal{S}^j$, where $i \neq j$ and i, $j \in \{$*Facebook*, *Google+*, *Whatsapp*$\}$.

We perform all the possible tests combination of the original images and the images from the SNs. The sensitivity and specificity results for each combination are shown in Fig. 4a, b, c and d. The icon in the center of the triangular histogram identifies the category from which the subset $\mathcal{N}_k$ has been selected, while the icons on the three sides represent the categories for classifying images, that is the set S.

The best results are obtained when the *pattern noise* and the relative threshold is computed starting from higher quality images as in the case of original

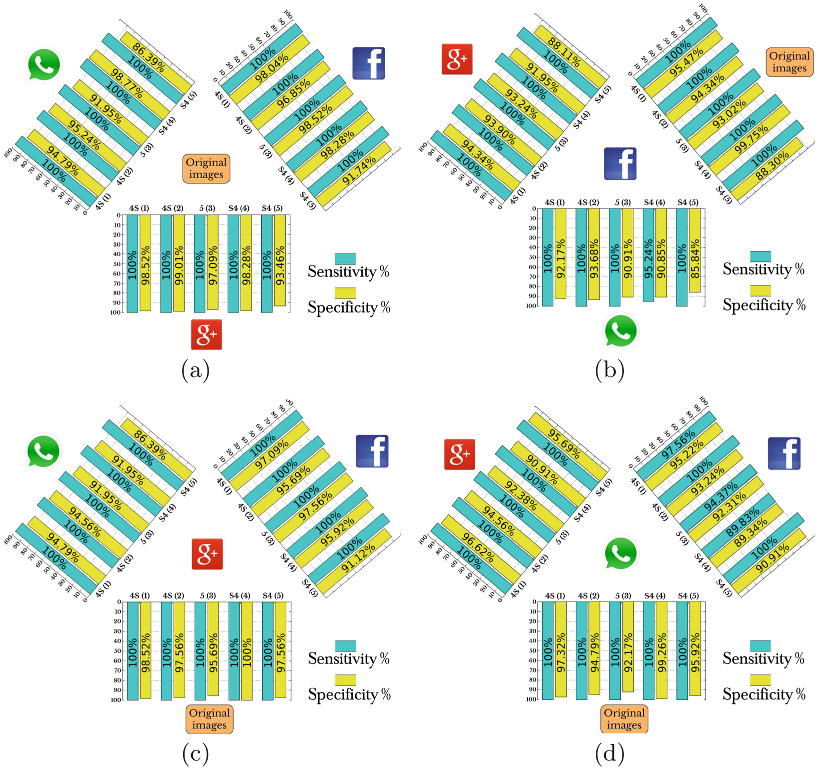


Fig. 4. Each triangular histogram shows the sensitivity and specificity results obtained. The threshold is computed using the subset $\mathcal{N}_k$ belonging to original (a), *Facebook* (b), *Google+* (c) and *WhatsApp* (d).

ones or those downloaded from *Google+*, shown in Fig. 4a and c respectively. The results are still good, even with *Facebook*, although *Facebook* reduces the image size during the uploading process: the sensitivity remains high while there is a decrease in the average specificity, see Fig. 4b. As expected, slightly worse results are obtained with *WhatsApp*. However, the method has successfully matched *WhatsApp* profiles with other SN user profiles with an average reliability of 98.78 %, as shown in Fig. 4d.

The sensitivity has a value of 100 % in all the tests, except the *Facebook* – *WhatsApp* combination. Although these two SNs reduce the image quality giving rise to a sensitivity degradation, the average value reaches the 99.49 %. In case of specificity, in all the categories, the average value is over 92 %. Thus, we can summarize that our method has a success rate over the 90 % for profile linking across all these three social networks.

5 Conclusions and Future Works

Social network forensic analysis, especially when coupled with smartphone devices [1], has become an important research problem. In this paper, we have presented a method by which it is possible to perform source camera verification and linking of user profiles using the images shared on social platforms. We perform our evaluation using five smartphones and three SNs with different compression characteristics of the image.

Especially given the fact that just as the uniqueness of the human fingerprints cannot be proved [4], the proposed method may fail due to the increasing number of devices and the increasing number of user profiles. To address this we plan to perform cluster based algorithm to decide if two user profiles belong to the same user. This will solve other problems, such as in classifying images of a single user profile that are taken from different sources (e.g. old or otherdevices of the user, front/rear smartphone's camera). Testing our methodology with a larger number of images, heterogeneous devices and several other SNs is another direction of our work. We also plan to test our approach on frames extracted from videos as video sharing is also a common behaviour on social platforms.

Acknowledgments. This work has been supported in part by the Italian Ministry of Education, Universities and Research IMPACT project (RBFR107725) and OPLON project (SCN_00176).

References

1. Al Mutawa, N., Baggili, I., Marrington, A.: Forensic analysis of social networking applications on mobile devices. Digit. Invest. **9**, S24–S33 (2012)
2. Bojinov, H., Michalevsky, Y., Nakibly, G., Boneh, D.: Mobile device identification via sensor fingerprinting. CoRR, abs/1408.1416 (2014)
3. Buades, A., Coll, B., Morel, J.-M.: A review of image denoising algorithms, with a new one. Multiscale Model. Simul. **4**(2), 490–530 (2005)
4. Cole, S.A.: Is fingerprint identification valid? Rhetorics of reliability in fingerprint proponents discourse. Law Policy **28**(1), 109–135 (2006)
5. Dabov, K., Foi, A., Katkovnik, V., Egiazarian, K.: Image denoising with block-matching and 3D filtering. In: Electronic Imaging 2006, p. 606414. International Society for Optics and Photonics (2006)
6. Das, A., Borisov, N., Caesar, M.: Do you hear what i hear? Fingerprinting smart devices through embedded acoustic components. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 441–452 (2014)
7. Dey, S., Roy, N., Xu, W., Choudhury, R.R., Nelakuditi, S.: Accelprint: imperfections of accelerometers make smartphones trackable. In: 21st Annual Network and Distributed System Security Symposium, NDSS, vol. 2013, pp. 23–26 (2014)
8. Facebook Inc., Form 10-K Annual Report. Technical Report 001–35551, Securities and Exchange Commission, December 2013
9. Goljan, M., Fridrich, J.: Camera identification from cropped and scaled images. In: Electronic Imaging (2008)

10. Iofciu, T., Fankhauser, P., Abel, F., Bischoff, K.: Identifying users across social tagging systems. In: ICWSM (2011)
11. Liang, X., Li, X., Zhang, K., Lu, R., Lin, X., Shen, X.: Fully anonymous profile matching in mobile social networks. IEEE J. Select. Areas Commun. **31**(9), 641–655 (2013)
12. Lukas, J., Fridrich, J., Goljan, M.: Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensics Secur. **1**(2), 205–214 (2006)
13. Salehan, M., Negahban, A.: Social networking on smartphones: when mobile phones become addictive. Computers in Human Behavior **29**(6), 2632–2639 (2013)
14. Sharma, R., Magnani, M., Montesi, D.; Missing data in multiplex networks: a preliminary study. In: International Workshop on Complex Networks and their Applications (2014)
15. Sharma, R., Magnani, M., Montesi, D.: Investigating the types and effects of missing data in multilayer networks. In: IEEE/ACM ASONAM (2015)
16. Van, L.T., Emmanuel, S., Kankanhalli, M.S.: Identifying source cell phone using chromatic aberration. In: IEEE ICME (2007)
17. Vosecky, J., Hong, D., Shen, V.Y.: User identification across multiple social networks. In: International Conference on Networked Digital Technologies (2009)
18. Ybarra, M.L., Mitchell, K.J.: How risky are social networking sites? a comparison of places online where youth sexual solicitation and harassment occurs. Pediatrics **121**(2), 350–357 (2008)