Image Manipulation on Facebook for Forensics Evidence

Marco Moltisanti[1](✉), Antonino Paratore[1], Sebastiano Battiato[1], and Luigi Saravo[2]

[1] Image Processing Laboratory – Dipartimento di Matematica e Informatica, Università degli Studi di Catania, Catania, Italy
{moltisanti,battiato,battiato@dmi.unict.it}@dmi.unict.it

[2] Arma dei Carabinieri – Reparto Investigazioni Scientifiche, Naples, Italy

Abstract. The growth of popularity of Social Network Services (SNSs) opened new perspectives in many research fields, including the emerging area of Multimedia Forensics. In particular, the huge amount of images uploaded to the social networks can represent a significant source of evidence for investigations, if properly processed. This work aims to exploit the algorithms and techniques behind the uploading process of a picture on Facebook, in order to find out if any of the involved steps (resizing, compression, renaming, etc.) leaves a trail on the picture itself, so to infer proper hypotheses about the authenticity and other forensic aspects of the pipeline.

1 Introduction

One of the most common problems in the image forensics field is the reconstruction of the history of an image or a video [3]. The data related to the characteristics of the camera that carried out the shooting, together with the reconstruction of the (possible) further processing, allow us to have some useful hints about the originality of the visual document under analysis. For example, if an image has been subjected to more than one JPEG compression, we can state that the considered image is not the exact bitstream generated by the camera at the time of shooting. In a digital investigation that includes JPEG images (the most widely used format on the network [4] and employed by most of cameras [1], [5]) as evidences, the classes of problems that we have to deal with, are essentially related to the authenticity of the visual document under analysis and to the retrieval of the device that generated the image under analysis. About the possibility to discover image manipulations in JPEG images, many approaches can be found in literature, as summarized in [6] and [7]. A first group of works (JPEG blocking artifacts analysis [8], [9], hash functions [10], JPEG headers analysis [5], thumbnails analysis [11], Exif analysis [12], etc.) proposes methods that seek the traces of the forgeries in the structure of the image or in its metadata. In [13] some methods based on PRNU (Photo Response Non-Uniformity) are exposed and tested. This kind of pattern characterizes, and allows to distinguish, every single camera sensor. Other approaches, as described in [14] and

V. Murino and E. Puppo (Eds.): ICIAP 2015, Part II, LNCS 9280, pp. 506–517, 2015.
DOI: 10.1007/978-3-319-23234-8_47

[15], [16] take care of analyzing the statistical distribution of the values assumed by the DCT coefficients. The explosion in the usage of Social Network Services (SNSs) enlarges the variability of such data and presents new scenarios and challenges.

The remainder of this paper is structured as follows: in Sec. 2 we present two possible scenarios where the information retrieved in this study can be applied. In Sec. 3 we explain the methodology used to build a coherent dataset and run the experiments. In Sec. 4 we analyze some aspects affected by the manipulation operated by the selected social network, and specifically the resizing algorithm, the variability of the Bits Per Pixels (BPP) and Compression Ratios (CR) on the images exposed to the uploading process. In Subsec. 4.3 we consider the quantization tables used to operate the compression and in Subsec. 4.4 the metadata manipulation is presented. Finally, in Sec. 5 we discuss our conclusions and talk about the possible future works on this subject.

2 Motivation and Scenarios

Investigators nowadays make extensive use of social networks activities in order to solve crimes[1][2]. A typical case involves the need to identify a subject: in such a scenario, the information provided by the naming conventions of Facebook[3], jointly with the possible availability of devices, can help the investigators in order to confirm the identity of a suspect person. More about Social Network Forensic can be read in [18]. Another interesting scenario consider the detection of possible forgeries, in order to prove the authenticity of a picture. Kee and Farid in [5] propose to model the parameters used in the creation of the JPEG thumbnail[4] in order to estimate possible forgeries, while Battiato *et al.* in [10] use a voting approach for the same purpose. For this task, the information inferred from this study can provide some priors to exclude or enforce such hypotheses.

Our analysis will focus on Facebook, because its pervasive diffusion[5] makes it the most obvious place to start for such a study.

3 Dataset

As previously stated, we refer in this phase to the Facebook environment, taking into account capabilities, data and related mobile applications available during the experimental phase.

[1] http://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/

[2] http://www.usatoday.com/story/news/nation/2015/03/20/facebook-cracks-murder-suspect/25069899/

[3] http://facebook.com

[4] http://www.w3.org/Graphics/JPEG/

[5] http://newsroom.fb.com/company-info/

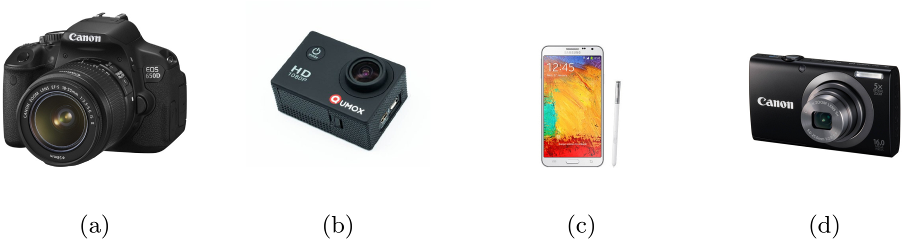


Fig. 1. The cameras used to build the dataset

In order to exploit how Facebook manages the images uploaded by the users, we decided to build a dataset, introducing three types of variability: the acquisition device, the input quality (in terms of resolution and compression rate) and the kind of scene depicted. Specifically we used the following imaging devices (see Fig. 1), which are respectively a reflex camera, a wearable camera, a camera-equipped phone and a compact camera:

- Canon EOS 650D with 18-55 mm interchangeable lens - Fig. 1a;
- QUMOX SJ-4000 - Fig. 1b;
- Samsung Galaxy Note 3 Neo - Fig. 1c;
- Canon Powershot A2300 - Fig. 1d.

The considered scenes are 3 (i.e. indoor, natural outdoor, artificial outdoor); for each scene we choose 10 frames, keeping the same point of view when changing the camera. Moreover, we took each frame 2 times, changing the camera resolution (see Fig. 1). The whole dataset is composed by 240 pictures.

Table 1. Resolution settings for the different devices (in pixels)

Camera	Low Resolution (LR)	High Resolution (HR)
Canon EOS 650D	720 × 480	5184 × 3456
QUMOX SJ4000	640 × 480	4032 × 3024
Samsung Galaxy Note 3 Neo	640 × 480	3264 × 2448
Canon Powershot A2300	640 × 480	4608 × 3456

Facebook actually provides two uploading options: the user can choose between low quality (LQ) and high quality (HQ). We uploaded each picture twice, using both options, and subsequently we downloaded them.

The whole dataset with both original pictures and their downloaded versions is available at http://iplab.dmi.unict.it/UNICT-SNIM/index.html. A subset is shown in Fig. 2.

4 Social Network Image Analysis

4.1 Facebook Resizing Algorithm

Our first evaluation focus on if and how Facebook rescales the uploaded images. We implemented a tool to ease the upload/download process of the images. The

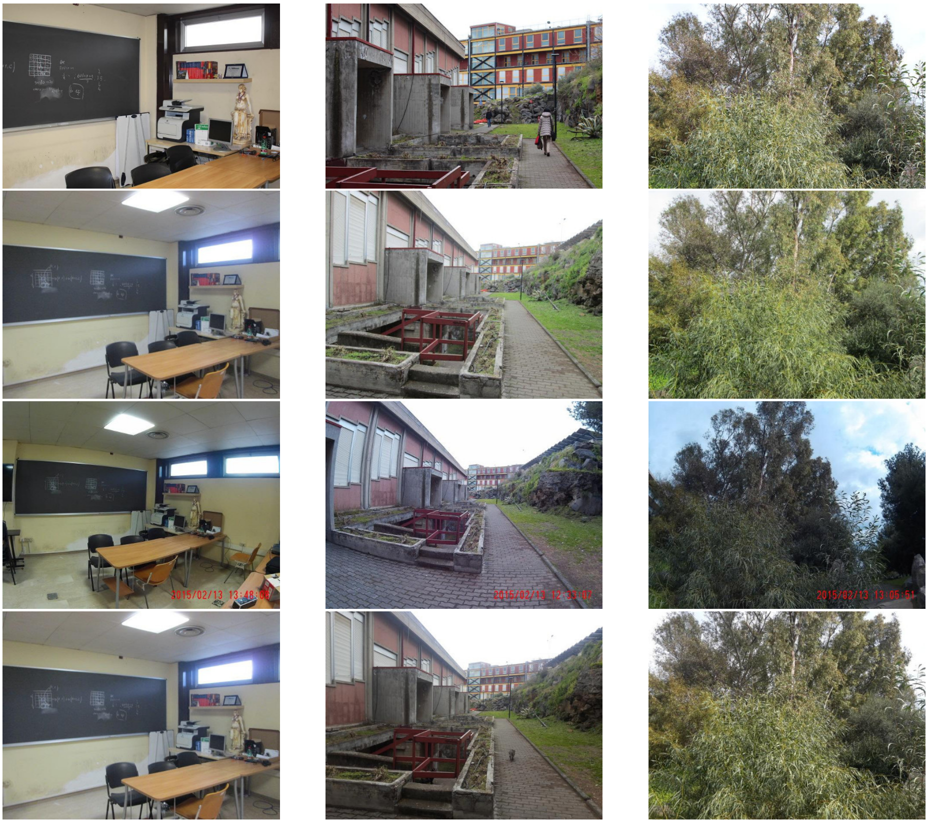


Fig. 2. Column 1: indoor, column 2: outdoor artificial, column 3: outdoor natural. Row 1: Canon EOS 650D, Row 2: QUMOX SJ4000, Row 3: Samsung Galaxy Note 3 Neo, Row 4: Canon Powershot A2300

different resolutions, related to the devices, are shown in Tab. 1. Performing a fine-grained tuning using synthetic images, we found out that the resizing algorithm is driven by the length in pixels of the longest side of the uploaded image coupled with the high quality option (on/off).

Figure 3 report the overall flow of the resizing pipeline. Let I be a picture of size $M \times N$. If $max\,(M, N) \leq 960$, I will not be resized; if $960 \leq max\,(M, N) \leq 2048$ and the user selected the HQ upload option, I will not be resized; if the user did not select the HQ option, then I will be scaled in such a way that the resulting image I' will have its longest side equal to $max\,(M', N') = 960$ pixels. If $max\,(M, N) > 2048$ Facebook scales I both in the case the HQ option is switched on or not. In the first case, the scaled image I' will have its longest side equal to 2048 pixels; in the second case, the longest side will be scaled down to 960 pixels.

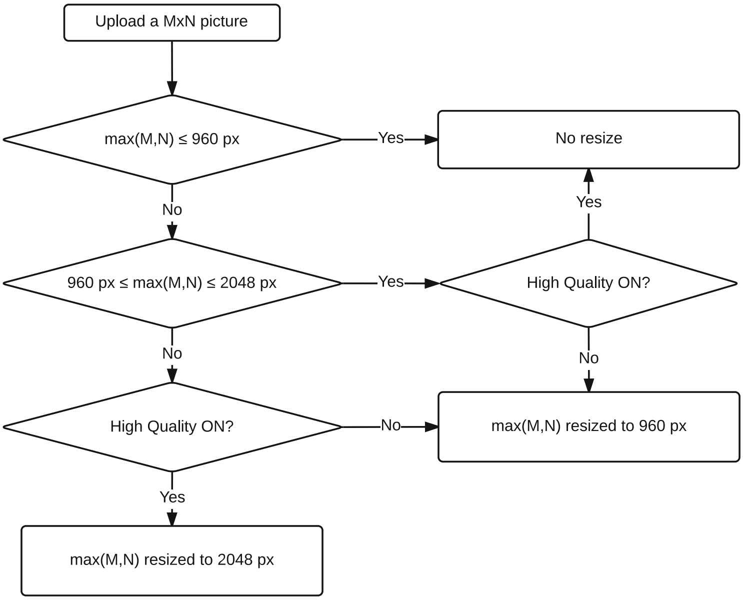


Fig. 3. Workflow of Facebook resizing algorithm for JPEG images

Naming of the Files. Facebook renames the image files after the upload. Nevertheless, it is still interesting to do a brief analysis on how this renaming is performed, in order to discover patterns in the name of the file and potential relationships among the different elements involved in the upload process: the user, the image itself, the options.

We found that the generated name is composed by three numeric parts: the first e and the third ones are random generated IDs, while the second part corresponds to the photo ID (see Fig. 4).

$$\underbrace{10996172}_{\text{Random}}\_\underbrace{745317175583308}_{\text{Photo ID}}\_\underbrace{271105793478350229}_{\text{Random}}\_(\text{n}|\text{o})].\text{jpg}$$

Fig. 4. The filename generated for an uploaded picture

The photo ID can be used to retrieve several information about the picture, using for instance the Facebook OpenGraph tool[6]. Just using a common browser and concatenating the photo ID to the OpenGraph URL, it is possible to discover:

- The direct links to the picture;
- The description of the picture;
- The URL of the server where the picture is hosted;
- The date and time of the creation;

[6] http://graph.facebook.com

- The date and time of last modification;
- The name and the ID of the user (both personal profile or page) who posted the photo;
- The name(s) and ID(s) of the user(s) tagged in the picture;
- Likes and comments (if any).

Moreover, OpenGraph shows the locations of all the copies at different resolutions of the picture, created by Facebook algorithms to be used as thumbnails to optimize the loading time.

It is also interesting to note that the resizing algorithm adds a suffix to the name of the file, depending on the original dimensions and on the upload quality option. Specifically, if the dimensions are beyond the thresholds set in the resizing algorithm and the high quality option is selected, the suffix "_o" will be added; otherwise the added suffix will be "_n".

4.2 Quantitative Measures

In this Section, we show how the processing done after the upload modify the Bits Per Pixel and the Compression Ratio for the images in the dataset. BPP are calculated as the ratio between the number of bits divided by the number of pixels (Eq. 1); CR, instead, is computed as the number of bits in the final image divided by the number of bits in the original image (Eq. 2). It is possible to compute the CR of a single image simply considering the uncompressed 24-bit RGB bitmap version.

$$BPP = \frac{\#\text{ bits in the final image}}{\#\text{ pixels}} \tag{1}$$

$$CR = \frac{\#\text{ bits in the final image}}{\#\text{ bit in the original image}} \tag{2}$$

Eq. 3 is a trivial proof that BPP and CR are proportional.

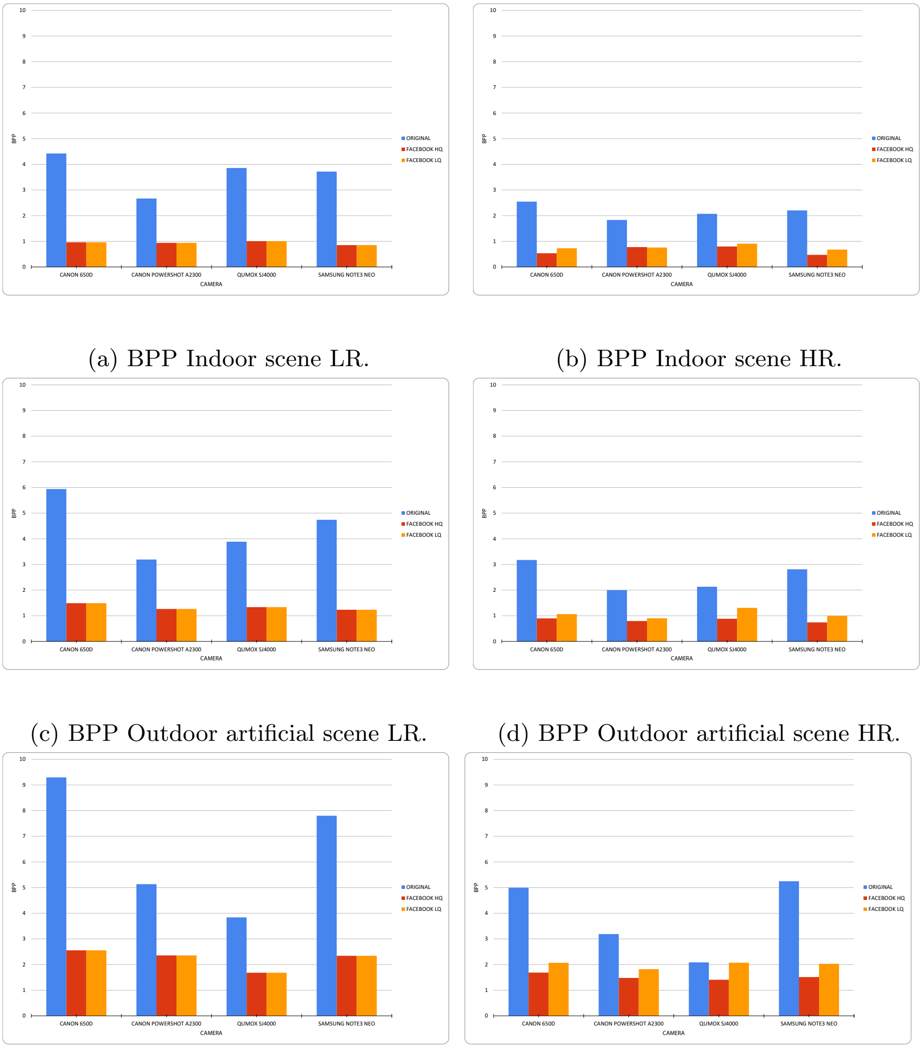
$$\begin{aligned} BPP \cdot \#\text{ pixels} = CR \cdot \#\text{ bits in the original image} = \\ = \#\text{ bits in the final image} \\ BPP = CR \cdot \frac{\#\text{ bits in the original image}}{\#\text{ pixels}} \end{aligned} \tag{3}$$

The charts in Fig. 5 report the average BPPs for the images, grouped by scene, which have been taken with the same camera, distinguished depending on the acquisition resolution. Since BPP and Compression Rate are proportional, we refer the reader to the supplementary material [7] for the charts related to CR.

In Fig. 6 and 7 we reported the relation of the number of pixels respectively with the BPP and the Quality Factor (QF) as estimated by JPEG Snoop[8].

[7] http://iplab.dmi.unict.it/UNICT-SNIM/index.html

[8] http://www.impulseadventure.com/photo/jpeg-snoop.html



(a) BPP Indoor scene LR.

(b) BPP Indoor scene HR.

(c) BPP Outdoor artificial scene LR.

(d) BPP Outdoor artificial scene HR.

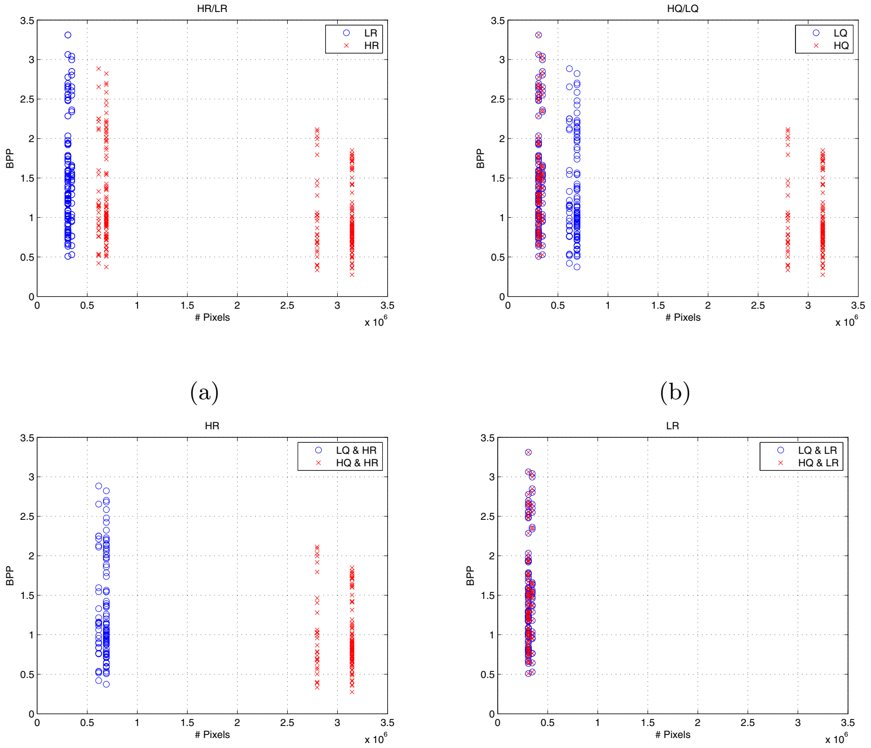
(e) BPP Outdoor natural scene LR.

(f) BPP Outdoor natural scene HR.

Fig. 5. BPP comparison with respect to scene and original resolution

Observing the graph in Fig. 6, it emerges a relation of inverse proportionality between the number of pixels and the maximum BPP; this would support the hypothesis of a maximum allowed size for the uploaded images.

A more interesting observation can be deducted from Fig. 7: trivially, we observe the same six vertical lines corresponding to the different sizes of the images, but all the points are vertically distributed in 17 discrete positions, corresponding to the quality factors reported in Tab. 2. Thus, we suppose there



(a)

(b)

(c)

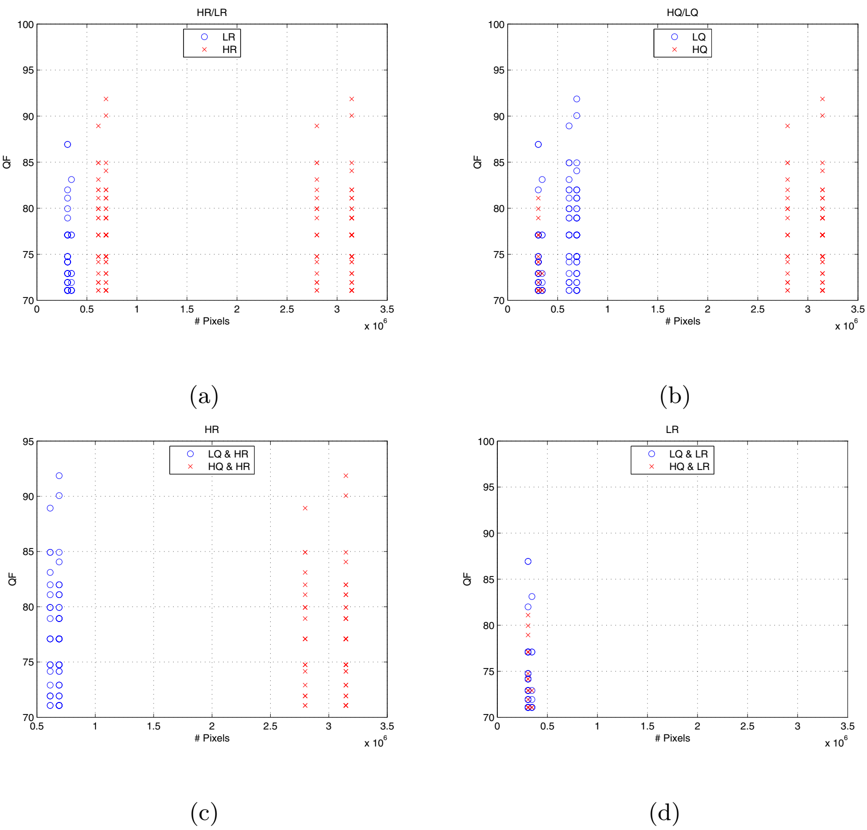
(d)

Fig. 6. Number of pixels in the images VS BPP. 6a: images grouped by input resolution (HR/LR); 6b: images group by upload quality (HQ/LQ); 6c: HR input images grouped by upload quality; 6d: LR input images grouped by upload quality.

should be 17 different Quantization Table used in the upload process of the pictures belonging to the proposed dataset. A further discussion about the quantization tables follows in Subsec. 4.3.

4.3 Quantization Tables

The images considered in our dataset are all in JPEG format, both the original versions and the downloaded ones. Thus, we want to find out how the JPEG compression affects the pictures, focusing on the Discrete Quantization tables used for that purpose. In fact, the Discrete Quantization Tables (DQT) can, in some way, certify that an image has been processed by some specific tool ([5]). We extracted the tables using JPEGSnoop. In Tab. 3 we report the DQTs for Luminance and Chrominance relative to the lowest and the highest quality factor.



(a)

(b)

(c)

(d)

Fig. 7. Number of pixels in the images VS Quality Factor. 7a: images grouped by input resolution (HR/LR); 7b: images group by upload quality (HQ/LQ); 7c: HR input images grouped by upload quality; 7d: LR input images grouped by upload quality

Moreover, we performed the same operation on some pictures belonging to the authors that were uploaded previously, to check if the tables changed over the years.

Together with this paper, we provide some supplementary material where we reported all the charts related to BPP and CR, and the complete description of the statics computed over each image in the dataset.

4.4 Metadata

Among others, Exif data[17] contain some additional information about the picture, such as camera settings, date, time and generic descriptions. Moreover, a thumbnail of the picture is included. These kind of data has been used for forensic purposes, because it can provide evidences of possible forgeries (e.g. the thumbnail is different from the actual photo). Often, if the camera is equipped

Table 2. Quality Factors of the JPEG Compression applied by Facebook (estimated by JPEG Snoop)

Quality Factor			
1	71.07	**10**	81.99
2	71.93	**11**	83.11
3	72.91	**12**	84.06
4	74.16	**13**	84.93
5	74.75	**14**	86.93
6	77.09	**15**	88.93
7	78.93	**16**	90.06
8	79.94	**17**	91.86
9	81.09		

Table 3. DQTs for minimum and maximum QF

DQT Luminance							
9	6	6	9	14	23	30	35
7	7	8	11	15	34	35	32
8	8	9	14	23	33	40	32
8	10	13	17	30	50	46	36
10	13	21	32	39	63	60	45
14	20	32	37	47	60	66	53
28	37	45	50	60	70	70	59
42	53	55	57	65	58	60	57

DQT Chrominance							
10	10	14	27	57	57	57	57
10	12	15	38	57	57	57	57
14	15	32	57	57	57	57	57
27	38	57	57	57	57	57	57
57	57	57	57	57	57	57	57
57	57	57	57	57	57	57	57
57	57	57	57	57	57	57	57
57	57	57	57	57	57	57	57

(a) DQT corresponding to QF = 71.07

DQT Luminance							
3	2	2	3	4	6	8	10
2	2	2	3	4	9	10	9
2	2	3	4	6	9	11	9
2	3	4	5	8	14	13	10
3	4	6	9	11	17	16	12
4	6	9	10	13	17	18	15
8	10	12	14	16	19	19	16
12	15	15	16	18	16	16	16

DQT Chrominance							
3	3	4	8	16	16	16	16
3	3	4	11	16	16	16	16
4	4	9	16	16	16	16	16
8	11	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16
16	16	16	16	16	16	16	16

(b) DQT corresponding to QF = 91.86

with a geo-tagging system, it is possible to find the GPS coordinates of the location where the photo has been captured.

Using JPEGSnoop, we extracted the Exif data from the downloaded images, and we found that Facebook completely removes them. Since no specification is available, our best guess is that, since removing the Exif data reduces the size in byte of the image, this procedure allows to save space on the storing servers, given the huge amount of pictures uploaded in the social network.

5 Conclusions

In this paper we introduced two different scenarios useful to infer forensic evidence starting from images publicly available on the most common social network platforms. We claim that, in almost all cases, knowing the involved processing acted during the uploading phase, is possible to infer evidence with respect to authentication and integrity of multimedia data.

Among others, we collected information about resolution and compression changes (quantization tables, metadata, compression ratio) applied to the uploaded image with respect to the input one.

Future works will be devoted to analyze the robustness of such changes with respect to the overall quality of the picture (recent versions of the Facebook mobile app allow to enhance the quality, in some way) and respect to the overall robustness of methods based on PRNU analysis.

Moreover, we plan to extend the involved study to other social networking platforms, such as Twitter, Instagram, Google+, considering also different kind of data (e.g. audio, video).

References

1. Battiato, S., Moltisanti, M.: The future of consumer cameras. In: Proceedings of the SPIE Eleconic Imaging, Image Processing: Algorithms and Systems XIII, PANORAMA special session, San Francisco, California, USA, February 8–12 (2015)
2. Jang, Y. J., Kwak., J.: Digital forensics investigation methodology applicable for social network services. Multimedia Tools and Applications, 1–12 (2014)
3. Oliveira, A., Ferrara, P., De Rosa, A., Piva, A., Barni, M., Goldenstein, S., Dias, Z., Rocha, A.: Multiple parenting identification in image phylogeny. In: IEEE International Conference on Image Processing (ICIP), pp. 5347–5351 (2014)
4. Usage of Image File Formats for Websites. http://w3techs.com/technologies/overview/image_format/all
5. Kee, E., Johnson, M.K., Farid, H.: Digital image authentication from JPEG headers. IEEE Transactions on Information Forensics and Security **6**(3), 1066–1075 (2011)
6. Piva, A.: An overview on image forensics. Proceedings of ISRN Signal Process., p. 496701 (2013)
7. Stamm, M.C., Wu, M., Liu, K.J.R.: Information forensics: An overview of the first decade. IEEE Access **1**, 167–200 (2013)
8. Bruna, A.R., Messina, G., Battiato, S.: Crop Detection through Blocking Artefacts Analysis. In: Maino, G., Foresti, G.L. (eds.) ICIAP 2011, Part I. LNCS, vol. 6978, pp. 650–659. Springer, Heidelberg (2011)
9. Luo, W., Qu, Z., Huang, J., Qiu G.: A novel method for detecting cropped and recompressed image block. In: Proceedings of IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP), vol. 2, pp. II217–II220 (2007)
10. Battiato, S., Farinella, G.M., Messina, E., Puglisi, G.: Robust image alignment for tampering detection. IEEE Transactions on Information Forensics and Security **7**(4), 1105–1117 (2012)
11. Kee, E., Farid, H.: Digital image authentication from thumbnails. In: Proceedings of SPIE, vol. 7541 (January 2010)
12. Gloe, T.: Forensic analysis of ordered data structures on the example of JPEG files. In: Proceedings of IEEE International Workshop on Information Forensics and Security (WIFS), pp. 139–144 (2012)
13. Chen, Y., Thing, V.L.L.: A study on the photo response nonuniformity noise pattern based image forensics in real-world applications. In: Proceedings of IEEE International Conference on Image Processing, Computer Vision, Pattern Recognit. (IPCV) (July 2012)
14. Battiato, S., Messina G.: Digital forgery estimation into DCT domain: A critical analysis. In: Proceedings of ACM Workshop on Multimedia Forensics (MiFor), pp. 37–42 (2009)
15. Redi, J.A., Taktak, W., Dugelay, J.L.: Digital image forensics: A booklet for beginners. Multimedia Tools and Applications **51**(1), 133–162 (2011)
16. Galvan, F., Puglisi, G., Bruna, A.R., Battiato, S.: First Quantization Matrix Estimation From Double Compressed JPEG Images. IEEE Transactions on Information Forensics and Security **9**(8), 1299–1310 (2014)

17. Camera & Imaging Products Association: Standardization Committee - Exchangeable image file format for digital still cameras: Exif Version 2.3. http://www.cipa.jp/std/documents/e/DC-008-2012_E_C.pdf
18. Pratama, S.F., Pratiwi, L., Abraham, A., Muda, A.K.: Computational Intelligence in Digital Forensics. In: Muda, A.K., Choo, Y.-H., Abraham, A., N. Srihari, S. (eds.) Computational Intelligence in Digital Forensics. SCI, vol. 555, pp. 1–16. Springer, Heidelberg (2014)