

Comparative Compression Robustness Evaluation of Digital Image Forensics

Oliver Remy, Sebastian Strumegger, Jutta Hämmerle-Uhl, and Andreas Uhl(✉)

Visual Computing and Security Lab (VISEL), Department of Artificial Intelligence and Human Interfaces, University of Salzburg, Salzburg, Austria
uhl@cs.sbg.ac.at

Abstract. The robustness of two important digital image forensic tasks (i.e. SIFT-based copy-move forgery detection and PRNU-based camera sensor identification) against four different lossy compression techniques is investigated (while typically, only JPEG compression is considered) to identify the best suited technique for this application scenario. Overall, we find that the accuracy of forensic tasks is reduced for increasing compression strength as expected, however, the relative performance of the compression schemes is different for the two tasks. While JPEG is superior for realistic application settings (where accuracy is in an acceptable range) in SIFT-based copy-move forgery detection, JPEG XR and BPG provide the best option for PRNU-based camera sensor identification, whereas JPEG is clearly impacting this forensic application most severely.

1 Introduction

In the past, images were considered as most authentic source of information – with increasing popularity and the availability of low-cost image editing software such as Adobe photoshop, corel paint shop, GIMP and recent techniques to produce "deep fakes", the truthfulness of an image can no longer be taken for granted. Among other forgery types, copy move forgery and object removal forgery are the most prominent ones. In a *copy move forgery*, a part of the image itself is copied and pasted into another part of the same image to conceal an important object or information, or to conceal that an object has been removed from the image in an *object removal forgery*. In most cases of image forgery, it is extremely difficult to distinguish between an original image and the forged one. Therefore, it is required to develop methods/techniques to assess the authenticity of an image – Digital Image Forensics (DIF [1]) has served this purpose to a large extent. Whenever an image is forged, there are some traces which are left behind in the forged image. These traces are useful for the forensic researcher to detect a forgery.

A wide range of DIF forgery detection techniques have been established in the recent years [2–5]. Besides recent deep learning based schemes [6,7], techniques relying on Scale Invariance Feature Transform (SIFT) keypoints have been shown to be effective. In particular, SIFT keypoints (and other local texture descriptors) have been proposed to reveal copy move forgeries [3,8–10] and image cloning [11], as well as to detect copyrighted material using CBIR techniques [12].

Another important DIF task is camera device identification and device linking. Besides its use in forgery detection [13], the photo response non-uniformity

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022, LNCS 13376, pp. 236–246, 2022.
https://doi.org/10.1007/978-3-031-10450-3_19

(PRNU [14]) of an imaging sensor has emerged as an important forensic tool for the realisation of these tasks. Slight variations among individual pixels during the conversion of photons to electrons in digital image sensors are considered as the source of the PRNU; thus, it is an intrinsic property which forms an inherent part of all digital imaging sensors and their output, respectively. All digital image sensors cast this weak, noise-like pattern into each and every image they capture. The most prominent way how to compute the PRNU is due to Fridrich in [15], the method describes how to estimate the PRNU image from set of images taken by the same camera, the PRNU estimator is derived using a maximum likelihood estimator (MLE), the MLE is modeled from the simplified sensor output model [15].

Typically, DIF techniques rely on subtle changes or properties in an image. Therefore, lossy compression is a "natural enemy" of such techniques as it removes high-frequency detail and thus can be considered an anti-forensic technique itself (e.g. robustness of copy-move detection under high compression is reduced [16,17], as it is the case for forensic image age approximation [18] and PRNU-based camera identification [19]). This is the reason why the detection of JPEG compression [20] is considered to be important for DIF, while corresponding anti-forensic techniques have already been developed to remove forensically significant indicators of compression from an image [21,22]. Also, the detection of recompression/double compression [23] is often intepreted as an indicator for image manipulation as the originally JPEG-compressed images might have undergone a second JPEG compression stage after image manipulation has taken place. Taken these observations together, it is obvious that techniques have been developed to increase the compression robustness for forensic techniques [24–26].

When talking about lossy compression, papers seen so far deal almost exclusively with lossy JPEG. In this paper, we look at the question of DIF compression robustness from a different perspective: We consider four different lossy compression schemes, i.e. JPEG, JPEG2000 (J2K), JPEG XR, and BPG (a H.265 derivative), and compare their impact on the DIF compression robustness. The aim is to answer the question which compression technique is favorable in case least impact of DIF is desired, and to also learn which technique is best suited to conceal forensic traces (in order to raise alarm in case this compression format is observed). For the experimental investigation we consider SIFT-based copy-move detection and PRNU-based camera identification as our target DIF techniques.

Section 2 reviews the applied SIFT-based copy-move detection and PRNU-based camera identification techniques, respectively. In Sect. 3, we briefly characterize the employed lossy compression tools. Section 4 describes the experimental settings and presents corresponding results on compression robustness. Section 5 concludes the paper and provides an outlook to future work in this direction.

2 Digital Image Forensics

2.1 SIFT-Based Copy-Move Detection

To detect a copy-move forgery, SIFT keypoints are computed together with their descriptors and then for each keypoint the two nearest neighbours from all remaining keypoints are identified using a K-d tree based on Euclidean distance d_1 and d_2 (where

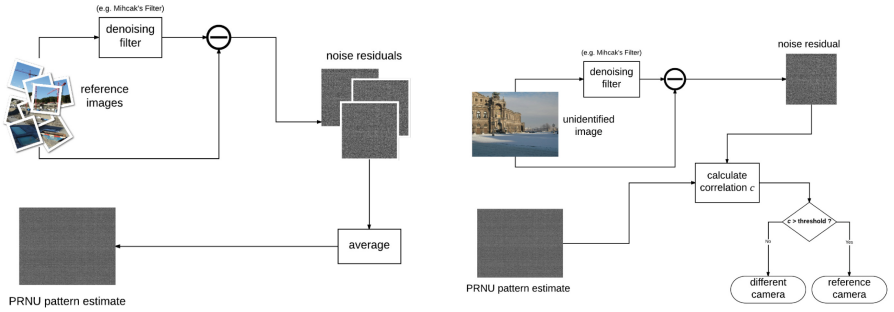
d_1 and d_2 are distances and d_1 corresponds to the closest neighbour) [27]. $T \in (0, 1)$ defines the fraction of distances d_1 and d_2 used to assess the relation between the the nearest neighbours. [28] and [29] suggested that there is a match only if $\frac{d_1}{d_2} < T$ holds. In these papers $T = 0.6$ but we looked also into results for $T = 0.53$. To classify if an image is forged or not, agglomerative hierarchical clustering is applied to the spatial locations ((x, y) coordinates) of the keypoints. This method creates a hierarchy of clusters which can be represented by means of a tree structure. If there are two or more clusters with at least n matched keypoints, these regions are considered cloned.

2.2 PRNU-Based Camera Identification

The PRNU (i.e. sensor fingerprint) can be obtained as follows:

$$\hat{K} = \sum_{i=1}^{N} R_i I_i \Big/ \sum_{i=1}^{N} I_i^2 \tag{1}$$

where the PRNU is denoted by $\hat{K}$ which is a noise-like signal carrying the PRNU. I_i is an image and R_i is the noise residual of an image which is obtained by (Eq. 2), note that i stands for the *i th* image out of N images which have been taken from a particular sensor (see Fig. 1a).



(a) Generation of PRNU (b) Camera Identification Process

Fig. 1. Schematic workflow of PRNU-based camera identification.

The residual image R_i is calculated by subtracting the original image from a denoised version of the image obtained by applying e.g. a wavelet denoising filter to an original image:

$$R_i = I_i - F(I_i) \tag{2}$$

where F denotes the denoising method. Eventually, a Wiener Filter (WF) [30] is applied additionally.

To detect whether the Residual of an image I (R_I) is taken by the sensor with PRNU estimator $\hat{K}$, we use normalized cross-correlation (NCC), which is illustrated in Fig. 1b:

$$\rho_{[R_I, I\hat{K}]} = NCC(R_I, I\hat{K}) \tag{3}$$

NCC as well as Peak Correlation Energy (PCE) have been proposed [15] as similarity metrics.

3 Lossy Image Compression Techniques

We consider three different ISO/IEC (lossy) image compression standards for increasing compression rates (i.e. ratio between original file size and file size after compression) using the respective default configurations unless stated otherwise:

1. JPEG (JPG): The well-known (ISO/IEC IS 10918-1) DCT-based image compression method [31]. By adjusting the divisors in the quantization phase, different compression ratios can be achieved. We adjust the quality parameter iteratively to achieve a file size closest to the desired compression rate.
2. JPEG 2000 (J2K): The wavelet-based image compression standard (ISO/IEC IS 15444-1) can operate also at higher compression ratios [32]. J2K is also a part of the DICOM standard where it replaced lossless JPEG compression. Results typically do not generate block-based artifacts as the original DCT-based JPG standard. J2K facilitates explicit rate control, i.e. target bitrates are met with high accuracy.
3. JPEG-XR (JXR): This compression standard based on Microsoft's HD Photo is known to produce higher quality than JPEG, but provides faster compression than JPEG 2000 [33]. In the default configuration the Photo Overlay/Overlap Transformation is only applied to high pass coefficients prior to the Photo Core Transformation (ISO/IEC IS 29199-2). We adjust quantization levels iteratively to achieve a target bitrate closest to the desired one.

Additionally, we use the "Better Portable Graphics" (BPG) algorithm which is based on a subset of the H.265 (HEVC, ISO/IEC 23008-2) video compression standard [34]. We adjust quantisation levels iteratively to achieve a target bitrate closest to the desired one.

While comparisons of these algorithms' compression performance wrt. image quality metrics are difficult to identify (except for specific image types, e.g. medical images [35]), application oriented comparisons have been done before, e.g. in biometrics (iris [36] and ear recognition [37], respectively) and in document image compression [38,39], and promising results have been obtained for JXR and in particular for BPG.

4 Experiments

4.1 Experimental Settings

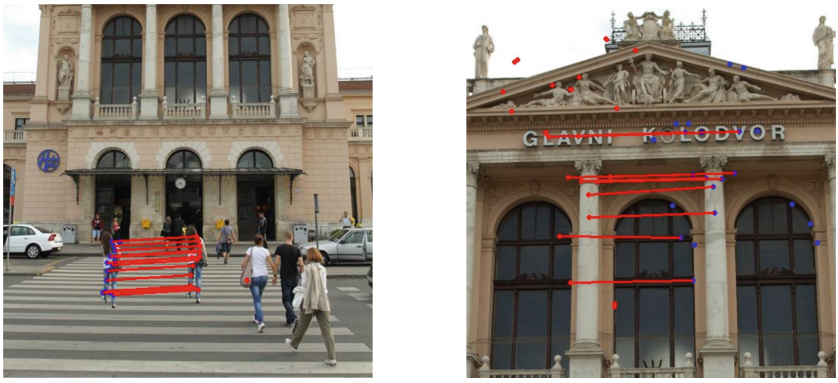
Concerning image compression, we use Imagemagick and NConvert for the three ISO standards and the BPG image library and utilities[1].

[1] https://bellard.org/bpg/.



Fig. 2. Compression example from the CoMoFoD public dataset.

Figure 2 displays the application of JPEG, JXR, and J2K to an example image of the CoMoFoD public dataset (see below) using compression ratio 60. The typical JPEG block artefacts and colour inconsistencies are clearly visible in the leftmost image. For the JXR case (middle image) we also notice some blocking artefacts while colouring is fine. The rightmost J2K case is a bit more blurry as compared to JXR while the colour display is equally well.



(a) True positive (b) False positive

Fig. 3. Examples from the CoMoFoD public dataset.

For copy-move detection, forged images are taken from the CoMoFoD public dataset for assessing forensic techniques [40], which contain simple translated copies of objects/regions. The 200 images of the small image category (512×512) have been used, however, we removed 58 of them as these indicated inconsistent results due to identical object parts within distinct objects. OpenCV[2] was used to compute SIFT keypoints and descriptor distances, while hierarchical clustering was implemented in Python. We consider compression ratios of up to 100 in steps of 10 - for some images,

[2] http://opencv.org/.

it was not possible to achieve the higher rates using JPEG; in this case, the affected images have been discarded for all compression schemes to maintain comparability. Figure 3 shows two examples of identified SIFT keypoint matches where Fig. 3b shows an example where the result incorrectly suggests the presence of a copy-move attack.

For PRNU-based camera identification tests we used a subset of the Dresden Image Database [41] containing images of one Afga 505 x, Canon Ixus 55, Nikon D70, and Sony H50 each, plus images from two Canon Ixus 70. Experiments have been done using software from the Matlab version of the Camera Fingerprint Library[3]. We consider compression ratios of 1.25, 1.66, 2.5, 5, 10.0, and 20.0.

4.2 Experimental Results

In Figs. 4 and 5 we visualise the effect of increasing compression strength on the accuracy the copy-move detection process (two different parameter settings as given in the figure are used).

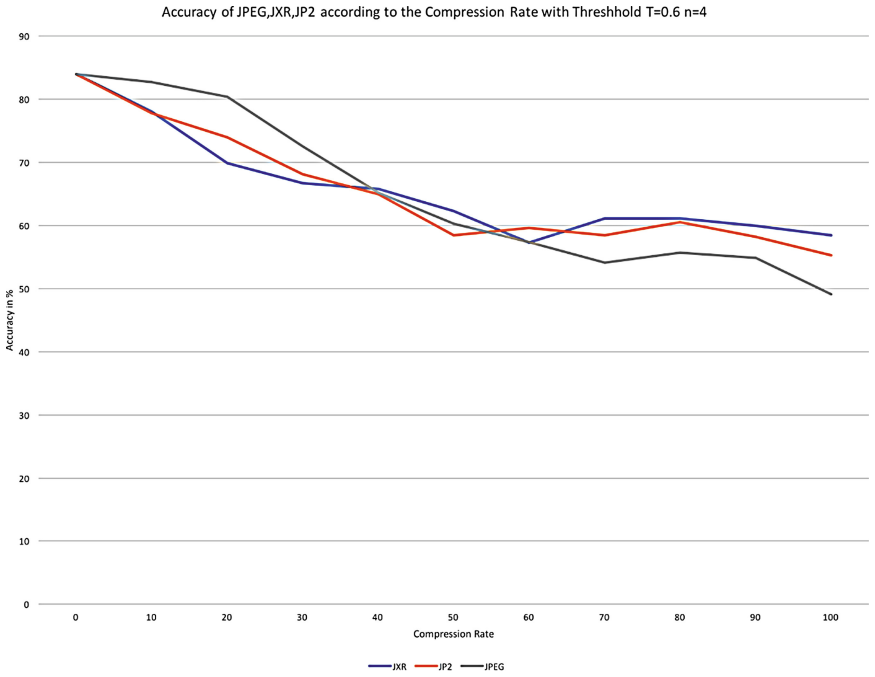


Fig. 4. Copy-move detection accuracy under increasing J2K compression ($T = 0.6$, $n = 4$).

For both settings, we observe clear trends: (i) For increasing compression strength, copy-move detection accuracy is decreasing. (ii) Up to compression ratio of 40, JPEG

[3] https://dde.binghamton.edu/download/camera_fingerprint/.

compression delivers accuracy superior to the other two compression schemes, for higher compression ratios above 70, JXR and J2K are clearly better. However, an accuracy of 60% for a binary decision is only slightly above guessing, so that this scenario is hardly realistic in practice.

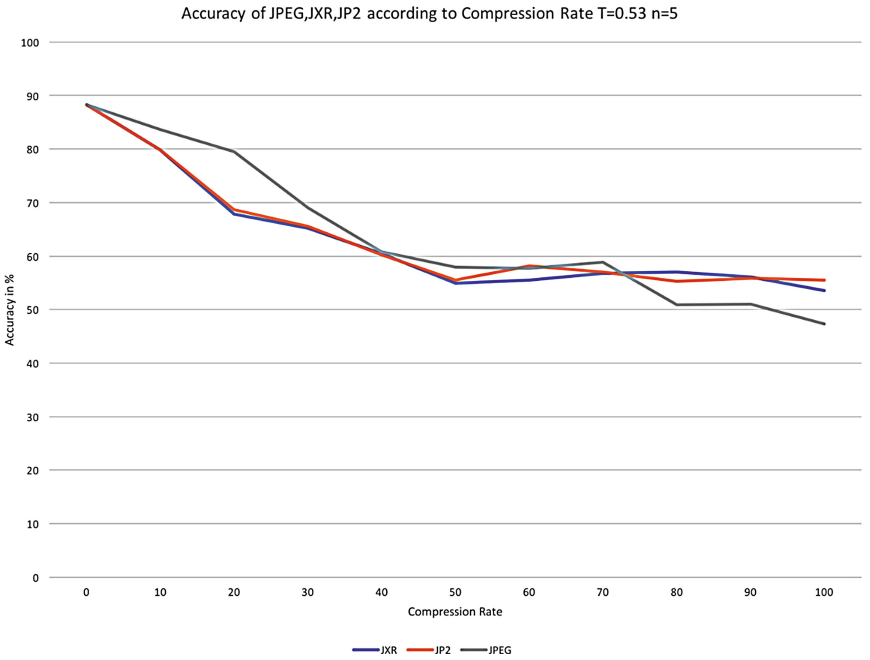
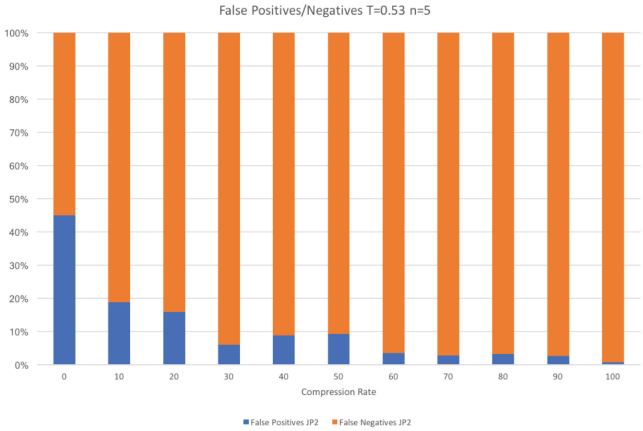


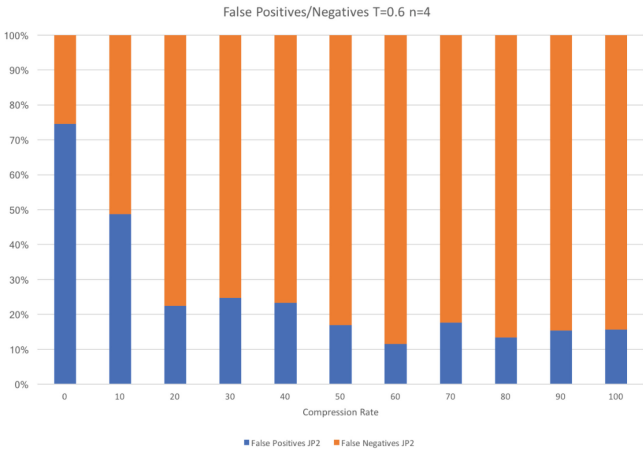
Fig. 5. Copy-move detection accuracy under increasing J2K compression ($T = 0.53$, $n = 5$).

Figure 6 illustrates an interesting additional effect of increasing compression ratio: While the amount of false positives and false negatives is rather balanced without compression being applied, we clearly notice that the share of false positive detections decreases for increasing compression ratio. A dominating share of false negatives is problematic for a forensic technique, as most actual copy-move forgeries are missed in this case.

In Fig. 7, we see the effect of increasing compression strength on PRNU-based camera identification, where we notice a clear tendency: The JPEG results detoriate significantly for increasing compression ratio, while the best suited compression techniques for this application case are JXR and BPG with J2K ranging in-between. Overall, this task suffers already significantly for moderate compression ratios as applied in our experiments.

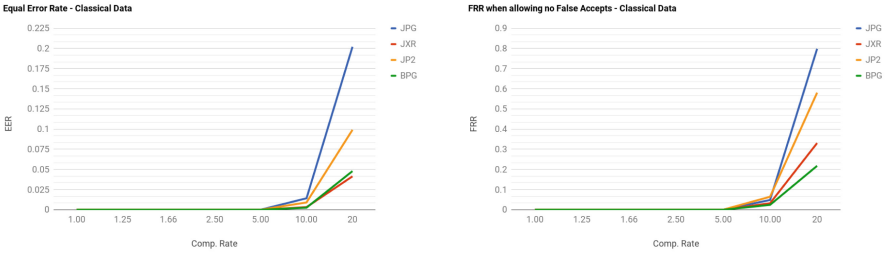


(a) $T = 0.53$, $n = 5$



(b) $T = 0.6$, $n = 4$

Fig. 6. Distribution of false negatives vs. false positives under increasing compression.



(a) EER (b) FRR @ FAR=0

Fig. 7. Camera identification results under increasing compression.

5 Conclusion

We have investigated the robustness of two important digital image forensic tasks against JPEG, JPEG XR, JPEG 2000, and BPG lossy compression. SIFT-based copy-move forgery detection and PRNU-based camera sensor identification are considered. While it is expected that the accuracy of forensic tasks is reduced for increasing compression strength, the relative performance of the compression schemes turns out to be different for the two tasks. While JPEG is superior for realistic application settings (where accuracy is in an acceptable range) in SIFT-based copy-move forgery detection, JPEG XR and BPG provide the best option for PRNU-based camera sensor identification, whereas JPEG is clearly impacting this forensic application most severely. When considering the properties of the two investigated forensic applications, this result could have been expected: SIFT is a very robust algorithm, and not by chance SIFT keypoints are also used in content-based retrieval applications. Additionally, artefacts generated in the same way in copied areas may additionally assist in the respective detection. When the image quality gets too poor, the other algorithms take the lead, however, the overall accuracy is already relatively low. On the other hand, PRNU and noise residuals are noise-like signals and severely impacted by the overall much lower compression performance of JPEG. For this reason all three other compression schemes turn out to be superior for this forensic application case.

Future work will include the consideration of JPEG XL as well as deep learning-based lossy compression schemes to observe their respective performance in a forensic context.

Acknowledgments. The authors gratefully acknowlege the contribution of the further Media Data Formats Lab students Max Göttl, Christoph Schwengler, Dennis Strähhuber, Benedikt Streitwieser, and Tim Ungerhofer. This work has been partially supported by the Salzburg State Government project “Artificial Intelligence in Industrial Vision Salzburg”.

References

1. Sencar, H.T., Memon, N.: Digital Image Forensics: There is More To a Picture than Meets the Eye. Springer Verlag, New York (2012). https://doi.org/10.1007/978-1-4614-0757-7
2. Ardizzone, E., Bruno, A., Mazzola, G.: Detecting multiple copies in tampered images. In: 2010 IEEE International Conference on Image Processing, pp. 2117–2120. IEEE (2010)
3. Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**(6), 1841–1854 (2012)
4. Zandi, M., Mahmoudi-Aznaveh, A., Mansouri, A.: Adaptive matching for copy-move forgery detection. In: 2014 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 119–124. IEEE (2014)
5. Mushtaq, S., Mir, A.H.: Image copy move forgery detection: a review. Int. J. Future Gener. Commun. Netw. **11**(2), 11–22 (2018)
6. Abdalla, Y., Iqbal, M.T., Shehata, M.: Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network. Information **10**, 286 (2019)

7. Wu, Y., Abd-Almageed, W., Natarajan, P.: BusterNet: detecting copy-move image forgery with source/target localization. In: Ferrari, V., Hebert, M., Sminchisescu, C., Weiss, Y. (eds.) ECCV 2018. LNCS, vol. 11210, pp. 170–186. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01231-1_11
8. Huang, H.-Y., Ciou, A.-J.: Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. EURASIP J. Image Video Process. **2019**(1), 1–16 (2019). https://doi.org/10.1186/s13640-019-0469-9
9. Pavlović, A., Glišović, N., Gavrovska, A., Reljin, I.: Copy-move forgery detection based on multifractals. Multimed. Tools Appl. **78**(15), 20655–20678 (2019). https://doi.org/10.1007/s11042-019-7277-1
10. Bilal, M., Habib, H.A., Mehmood, Z., Yousaf, R.M., Saba, T., Rehman, A.: A robust technique for copy-move forgery detection from small and extremely smooth tampered regions based on the DHE-SURF features and mDBSCAN clustering. Australian J. Forensic Sci. **53**, 1–24 (2020)
11. Saleem, M.: A key-point based robust algorithm for detecting cloning forgery. In: IEEE International Conference on Control System, Computing and Engineering (ICCSCE), vol. 4, pp. 2775–2779 (2014)
12. Do, T.T., Kijak, E., Furon, T., Amsaleg, L.: Deluding image recognition in SIFT-based CBIR systems. In: Proceedings of the 2nd ACM Workshop on Multimedia in Forensics, Security and Intelligence, pp. 7–12. ACM (2010)
13. Chierchia, G., Poggi, G., Sansone, C., Verdoliva, L.: PRNU-based forgery detection with regularity constraints and global optimization. In: 2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP), pp.236–241 (2013)
14. Lukas, J., Fridrich, J., Goljan, M.: Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensics Secur. **1**(2), 205–214 (2006)
15. Fridrich, J.: Digital image forensics. IEEE Signal Process. Mag. **26**(2), 26–37 (2009)
16. Huang, D.Y., Huang, C.N., Hu, W.C., Chou, C.H.: Robustness of copy-move forgery detection under high jpeg compression artifacts. Multimed. Tools Appl. **76**, 1509–1530 (2015)
17. Huang, D.Y., Huang, C.N., Hu, W.C., Chou, C.H.: Robustness of copy-move forgery detection under high jpeg compression artifacts. Multimedia Tools Appl. **76**(1), 1509–1530 (2017)
18. Joechl, R., Uhl, A.: Effects of image compression on image age approximation. In: 20th International Workshop on Digital-forensics and Watermarking (IWDW2021), Beijing, China (2021)
19. Goljan, M., Chen, M., Comesara, P., Fridrich, J.: Effect of compression on sensor-fingerprint based camera identification. Electron. Imaging. Media Watermark. Secur. Forensics **2016**, 1–10 (2016)
20. Kumawat, C., Pankajakshan, V.: A robust jpeg compression detector for image forensics. Signal Process. Image Commun. **89**, 116008 (2020)
21. Stamm, M.C., Liu, K.R.: Anti-forensics of digital image compression. IEEE Trans. Inf. Forensics Secur. **6**(3), 1050–1065 (2011)
22. Stamm, M.C., Tjoa, S.K., Lin, W.S., Liu, K.R.: Undetectable image tampering through jpeg compression anti-forensics. In: 2010 IEEE International Conference on Image Processing, pp. 2109–2112 (2010)
23. Lu, W., Zhang, Q., Luo, S., Zhou, Y., Huang, J., Shi, Y.Q.: Robust estimation of upscaling factor on double jpeg compressed images. IEEE Trans. Cybern. 1–13 (2021)
24. Diallo, B., Urruty, T., Bourdon, P., Fernandez-Maloigne, C.: Robust forgery detection for compressed images using CNN supervision. Forensic Sci. Int. Rep. **2**, 100112 (2020)
25. Diallo, B., Urruty, T., Bourdon, P., Fernandez-Maloigne, C.: Improving robustness of image tampering detection for compression. In: MMM 2019: MultiMedia Modeling, Thessaloniki, Greece, January 2019

26. Mandelli, S., Bonettini, N., Bestagini, P., Tubaro, S.: Training CNNs in presence of jpeg compression: Multimedia forensics vs computer vision. In: 2020 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6 (2020)
27. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G.: A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011)
28. Mahdian, B., Saic, S.: Detection of copy-move forgery using a method based on blur moment invariants. Forensic Sci. Int. **171**(2–3), 180–189 (2007)
29. Huang, H., Guo, W., Zhang, Y.: Detection of copy-move forgery in digital images using SIFT algorithm. In: Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. PACIIA 2008, vol. 2, pp. 272–276. IEEE (2008)
30. Mihcak, M.K., Kozintsev, I., Ramchandran, K.: Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising. In: Proceedings of 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing, 1999, vol. 6, pp. 3253–3256. IEEE (1999)
31. Pennebaker, W., Mitchell, J.: JPEG - Still Image Compression Standard. Van Nostrand Reinhold, New York (1993)
32. Taubman, D., Marcellin, M.: JPEG2000 – Image Compression Fundamentals. Standards and Practice. Kluwer Academic Publishers, The Nethrlands (2002)
33. Dufaux, F., Sullivan, G.J., Ebrahimi, T.: The JPEG XR image coding standard. IEEE Signal Process. Mag. **26**(6), 195–199 (2009)
34. Li, F., Krivenko, S., Lukin, V.: An approach to better portable graphics (BPG) compression with providing a desired quality. In: 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), pp. 13–17 (2020)
35. Liu, F., Hernandez-Cabronero, M., Sanchez, V., Marcellin, M.W., Bilgin, A.: The current role of image compression standards in medical imaging. Information **8**(4), 131 (2017)
36. Hofbauer, H., Rathgeb, C., Wagner, J., Uhl, A., Busch, C.: Investigation of better portable graphics compression for iris biometric recognition. In: Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG 2015), Darmstadt, Germany, p. 8 (2015)
37. Rathgeb, C., Busch, C., Wagner, J., Pflug, A.: Effects of image compression on ear biometrics. IET Biom. **5**(3), 252–261 (2016)
38. Darwiche, M., Pham, T.A., Delalandre, M.: Comparison of jpeg's competitors for document images. In: 2015 International Conference on Image Processing Theory, Tools and Applications (IPTA), pp. 487–493 (2015)
39. Wild, P., Štolc, S., Valentín, K., Daubner, F., Clabian, M.: Compression effects on security document images. In: 2016 European Intelligence and Security Informatics Conference (EISIC), pp. 76–79 (2016)
40. Ardizzone, E., Bruno, A., Mazzola, G.: Copy-move forgery detection by matching triangles of keypoints. IEEE Trans. Inf. Forensics Secur. **10**(10), 2084–2094 (2015)
41. Gloe, T., Böhme, R.: The Dresden image database for benchmarking digital image forensics. In: SAC 2010: Proceedings of the 2010 ACM Symposium on Applied Computing, pp. 1584–1590ACM (2010)