Diffusion models meet image counter-forensics
Suplementary material

Matías Tailanián[1,2], Marina Gardella[3], Alvaro Pardo[2,4], Pablo Musé[1]
[1]IIE, Facultad de Ingeniería,Universidad de la República
[2]Digital Sense
[3]Centre Borelli, École Normale Supérieure Paris-Saclay, Université Paris-Saclay
[4]Universidad Católica del Uruguay

1. Forensic methods

In this section, we provide a brief description of the forensic methods used to analyze the effectiveness of the counter-forensic approaches.

Choi et al. [2] aims to detect inconsistencies in the mosaic pattern with which the raw image was captured. To do so, they use the fact that sampled pixels were more likely to take extreme values. Also aiming at demosaicing inconsistencies, Shin et al. [12] use the fact that sampled pixels have a higher variance to detect forged regions. Bammey et al. [1] combined the translation invariance of convolutional neural networks with the periodicity of the mosaic pattern to train a self-supervised network into implicitly detecting demosaicing artefacts.

Splicebuster [4] uses the co-occurrences of noise residuals as local features revealing tampered image regions. Noiseprint [5] extends on Splicebuster and uses a Siamese network trained on authentic images to extract the noise residual of an image, which is then analyzed for inconsistencies. TruFor [7] also relies on a noise-sensitive fingerprint that is used with the RGB image to detect deviations from the expected regular pattern that characterizes each pristine image.

Zero [11] targets JPEG artifacts. This method counts the number of null DCT coefficients in all blocks and deduces the grid origin. By doing this locally, this method can detect regions having an inconsistent grid origin. Comprint [10] combines the use of a compression fingerprint with the noise fingerprint in [5]. Comprint is an end-to-end fully convolutional neural network including RGB and DCT streams, aiming at learning compression artifacts on RGB and DCT domains jointly.

ManTraNet [14] is a bipartite end-to-end network, trained to detect image-level manipulations with one part, while the second part is trained on synthetic forgery datasets to detect and localize forgeries in the image.

2. Forgery detection scores

In terms of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN), the IoU is the ratio between the number of pixels in the intersection of detected samples and of ground-truth-positive samples and the number of pixels in the union of these sets:

$$IoU = \frac{TP}{TP + FN + FP}, \tag{1}$$

while the MCC represents the correlation between the ground truth and detections:

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}. \tag{2}$$

3. Complete IQA scores

In this Section, we present the Image Quality Assessment for all CF methods, like in Table 2 of the paper, but also include the results over the DSO-1 dataset [6]. For this dataset, we obtained the best scores for NIQE, BRISQUE, and LPIPS.

4. Complete F1, MCC and IoU scores

The F1 scores obtained by all the tested methods on the Korus dataset are presented in Table 2. Table 3 and Table 4 present the complete MCC and IoU scores (including Bammey *et al.* [1]), respectively.

The F1 scores obtained by all the tested methods on the FAU dataset are presented in Table 5. Table 6 and Table 7 present the complete MCC and IoU scores (including Bammey *et al.* [1]), respectively.

The F1 scores obtained by all the tested methods on the COVERAGE dataset are presented in Table 8. Table 9 and Table 10 present the complete MCC and IoU scores (including Bammey *et al.* [1]), respectively.

		NIQE (▼)	BRISQUE (▼)	LPIPS (▼)	PSNR (▲)	SSIM (▲)
Korus	Original	5.7271	13.7602	0.0000	80.0000	1.0000
	CamTE	5.5442	34.5632	0.1684	**38.2833**	**0.9433**
	BM3D	5.1004	38.0418	0.0835	**43.1409**	**0.9802**
	Diff-CF	**3.8693**	**23.1161**	**0.0733**	32.9680	0.8769
	Diff-CFG	**4.1070**	**28.3290**	**0.0771**	34.3391	0.9126
FAU	Original	4.7392	20.5726	0.0000	80.0000	1.0000
	CamTE	5.8360	40.1577	0.2098	**37.8765**	**0.9460**
	BM3D	5.4875	42.7470	0.1045	**41.2625**	**0.9797**
	Diff-CF	**3.8896**	**19.8268**	**0.0985**	33.0308	0.8792
	Diff-CFG	**4.2440**	**29.9920**	**0.0952**	34.4725	0.9159
COVERAGE	Original	4.5529	19.0256	0.0000	80.0000	1.0000
	CamTE	5.4513	30.3558	0.0631	**35.7974**	**0.9648**
	BM3D	5.8792	35.9560	**0.0237**	**44.1417**	**0.9888**
	Diff-CF	**4.3343**	**17.1298**	0.0281	33.4959	0.9275
	Diff-CFG	**5.0359**	**27.8903**	**0.0276**	34.6969	0.9487
DSO-1	Original	3.9174	16.6183	0.0000	80.0000	1.0000
	CamTE	5.2180	40.2867	0.2022	**38.5459**	**0.9446**
	BM3D	5.1870	39.8485	0.1239	**41.9057**	**0.9750**
	Diff-CFG	**3.3907**	**9.2614**	**0.0950**	34.1204	0.8862
	Diff-CFG	**3.6686**	**19.3601**	**0.0899**	35.3473	0.9154

Table 1. Image quality assessment results of the evaluated counter-forensics techniques. The ▼ indicates that the lower the score the better while the ▲ indicates that the higher the score the better. The best two scores are shown in bold and underlined for each database. For the no-reference metrics NIQE and BRISQE, the proposed diffusion-based counter-forensics methods achieve the best performance. This table extends Table 2 of the paper, including the results for DSO-1.

The F1 scores obtained by all the tested methods on the DSO-1 dataset are presented in Table 11. Table 12 and Table 13 present the complete MCC and IoU scores (including Bammey *et al*. [1]), respectively.

5. Interactive plots

For better visualization, all plots of Section 5.3 of the paper, are included in separate `.html` files, in interactive versions, as part of the supplementary materials.

6. Visual results

Figures 1-6 present supplementary examples of the results obtained by the different forensics methods on the different versions of the very same image. The image used in each figure is specified in the caption. For all figures, we present the result of all considered forensic methods, even if they do not perform a good detection.

References

[1] Quentin Bammey, Rafael Grompone von Gioi, and Jean-Michel Morel. An adaptive neural network for unsupervised mosaic consistency analysis in image forensics. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020. 1, 2

[2] Chang-Hee Choi, Jung-Ho Choi, and Heung-Kyu Lee. Cfa pattern identification of digital cameras using intermediate value counting. In *Proceedings of the Thirteenth ACM Multimedia Workshop on Multimedia and Security*, MM&Sec '11, page 21–26, New York, NY, USA, 2011. Association for Computing Machinery. 1

[3] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou. An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on Information Forensics and Security*, 7(6):1841–1854, 2012. 4, 11, 12

[4] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva. Splicebuster: A new blind image splicing detector. In *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2015. 1

[5] Davide Cozzolino and Luisa Verdoliva. Noiseprint: A cnn-based camera model fingerprint. *IEEE Transactions on Information Forensics and Security*, 15:144–159, 2020. 1

[6] Tiago José de Carvalho, Christian Riess, Elli Angelopoulou, Hélio Pedrini, and Anderson de Rezende Rocha. Exposing digital image forgeries by illumination color classification. *IEEE Transactions on Information Forensics and Security*, 8(7):1182–1194, 2013. 1, 6

[7] Fabrizio Guillaro, Davide Cozzolino, Avneesh Sud, Nicholas Dufour, and Luisa Verdoliva. Trufor: Leveraging all-round clues for trustworthy image forgery detection and localization. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 20606–20615, June 2023. 1

[8] P. Korus and J. Huang. Evaluation of random field models in multi-modal unsupervised tampering localization. In *Proc. of IEEE Int. Workshop on Inf. Forensics and Security*, 2016. 3, 7, 8, 9, 10

[9] P. Korus and J. Huang. Multi-scale analysis strategies in prnu-based tampering localization. *IEEE Trans. on Information Forensics & Security*, 2017. 3, 7, 8, 9, 10

[10] Hannes Mareen, Dante Vanden Bussche, Fabrizio Guillaro, Davide Cozzolino, Glenn Van Wallendael, Peter Lambert, and Luisa Verdoliva. Comprint: Image forgery detection and localization using compression fingerprints. *arXiv preprint arXiv:2210.02227*, 2022. 1

[11] Tina Nikoukhah, Jérémy Anger, Thibaud Ehret, Miguel Colom, Jean-Michel Morel, and Rafael Grompone von Gioi. Jpeg grid detection based on the number of dct zeros and its application to automatic and localized forgery detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 110–118, 2019. 1

[12] Hyun Jun Shin, Jong Ju Jeon, and Il Kyu Eom. Color filter array pattern identification using variance of color difference image. *Journal of Electronic Imaging*, 26(4):043015, 2017. 1

[13] Bihan Wen, Ye Zhu, Ramanathan Subramanian, Tian-Tsong Ng, Xuanjing Shen, and Stefan Winkler. Coverage – a novel

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.0657	0.0825	0.1717	0.0817	0.1607	0.1389	0.1035	0.1682	0.3473	0.0043
CamTE	0.0420 (-0.0237)	0.0833 (0.0009)	0.0562 (-0.1155)	0.0710 (-0.0107)	0.1147 (-0.0460)	0.0987 (-0.0402)	0.1059 (0.0024)	0.1261 (-0.0422)	0.2246 (-0.1227)	0.0000 (-0.0043)
BM3D	0.0937 (0.0280)	0.0877 (0.0053)	0.0314 (-0.1403)	0.0634 (-0.0184)	0.1278 (-0.0329)	0.0939 (-0.0450)	0.0987 (-0.0048)	0.1274 (-0.0409)	0.2803 (-0.0670)	0.0000 (-0.0043)
Diff-CF	0.0324 (-0.0333)	0.0931 (0.0106)	0.0440 (-0.1278)	0.0398 (-0.0419)	0.0769 (-0.0838)	0.0669 (-0.0720)	0.0903 (-0.0131)	0.0720 (-0.0963)	0.1841 (-0.1631)	0.0046 (0.0003)
Diff-CFG	0.0775 (0.0118)	0.0912 (0.0087)	0.0077 (-0.1640)	0.0520 (-0.0298)	0.0980 (-0.0627)	0.0816 (-0.0573)	0.0910 (-0.0125)	0.0852 (-0.0831)	0.2398 (-0.1074)	0.0019 (-0.0024)

Table 2. F1 scores obtained for all the tested methods on the Korus dataset [8, 9].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.0790	-0.1548	0.1971	0.0534	0.1261	0.0988	0.0221	0.1405	0.3428	0.0050
CamTE	0.0468 (-0.0322)	-0.0608 (0.0940)	0.0597 (-0.1374)	0.0356 (-0.0179)	0.0646 (-0.0614)	0.0420 (-0.0569)	0.0305 (0.0084)	0.0817 (-0.0588)	0.1961 (-0.1467)	0.0000 (-0.0050)
BM3D	0.0997 (0.0207)	-0.0452 (0.1095)	0.0352 (-0.1619)	0.0278 (-0.0256)	0.0652 (-0.0609)	0.0420 (-0.0569)	0.0155 (-0.0066)	0.0860 (-0.0545)	0.2579 (-0.0850)	0.0000 (-0.0050)
Diff-CF	0.0418 (-0.0371)	-0.0030 (0.1518)	0.0147 (-0.1825)	0.0024 (-0.0510)	0.0255 (-0.1005)	0.0190 (-0.0798)	0.0027 (-0.0194)	0.0350 (-0.1055)	0.1454 (-0.1974)	0.0045 (-0.0005)
Diff-CFG	0.0852 (0.0063)	-0.0096 (0.1452)	0.0044 (-0.1927)	0.0125 (-0.0409)	0.0442 (-0.0818)	0.0267 (-0.0722)	0.0040 (-0.0181)	0.0456 (-0.0950)	0.2064 (-0.1364)	0.0005 (-0.0045)

Table 3. MCC scores obtained for all the tested methods (including Bammey *et al.*) on the Korus dataset [8, 9].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.0433	0.0446	0.1261	0.0461	0.0982	0.0792	0.0568	0.1012	0.2575	0.0028
CamTE	0.0278 (-0.0155)	0.0452 (0.0005)	0.0400 (-0.0860)	0.0389 (-0.0072)	0.0644 (-0.0338)	0.0545 (-0.0247)	0.0578 (0.0011)	0.0729 (-0.0284)	0.1489 (-0.1086)	0.0000 (-0.0028)
BM3D	0.0646 (0.0213)	0.0478 (0.0031)	0.0227 (-0.1033)	0.0346 (-0.0115)	0.0746 (-0.0237)	0.0514 (-0.0278)	0.0540 (-0.0028)	0.0744 (-0.0268)	0.1964 (-0.0611)	0.0000 (-0.0028)
Diff-CF	0.0204 (-0.0229)	0.0505 (0.0059)	0.0246 (-0.1014)	0.0215 (-0.0246)	0.0416 (-0.0566)	0.0360 (-0.0432)	0.0487 (-0.0081)	0.0401 (-0.0611)	0.1131 (-0.1445)	0.0027 (-0.0001)
Diff-CFG	0.0527 (0.0095)	0.0495 (0.0048)	0.0043 (-0.1217)	0.0281 (-0.0180)	0.0552 (-0.0430)	0.0446 (-0.0346)	0.0491 (-0.0076)	0.0488 (-0.0525)	0.1601 (-0.0975)	0.0011 (-0.0017)

Table 4. IoU scores obtained for all the tested methods (including Bammey *et al.*) on the Korus dataset [8, 9].

database for copy-move forgery detection. In *IEEE International Conference on Image processing (ICIP)*, pages 161–165, 2016. 5

[14] Yue Wu, Wael AbdAlmageed, and Premkumar Natarajan. Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2019. 1

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.3187	0.0827	0.3122	0.0566	0.0630	0.0888	0.1843	0.0471	0.4203	0.2958
CamTE	0.0159 (-0.3027)	0.0909 (0.0082)	0.1496 (-0.1626)	0.0376 (-0.0190)	0.0787 (0.0157)	0.0806 (-0.0082)	0.1639 (-0.0204)	0.0517 (0.0045)	0.1008 (-0.3196)	0.1089 (-0.1870)
BM3D	0.0741 (-0.2446)	0.0911 (0.0084)	0.0722 (-0.2399)	0.0237 (-0.0328)	0.0690 (0.0060)	0.0606 (-0.0282)	0.1298 (-0.0545)	0.0460 (-0.0012)	0.1287 (-0.2917)	0.1012 (-0.1946)
Diff-CF	0.0099 (-0.3088)	0.0973 (0.0146)	0.0781 (-0.2341)	0.0294 (-0.0271)	0.0643 (0.0013)	0.0383 (-0.0505)	0.1061 (-0.0781)	0.0238 (-0.0233)	0.0935 (-0.3269)	0.0027 (-0.2931)
Diff-CFG	0.0301 (-0.2886)	0.0953 (0.0126)	0.0318 (-0.2804)	0.0275 (-0.0291)	0.0630 (-0.0000)	0.0544 (-0.0344)	0.1109 (-0.0733)	0.0450 (-0.0021)	0.1051 (-0.3153)	0.0016 (-0.2942)

Table 5. F1 scores obtained for all the tested methods on FAU dataset [3].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.3228	-0.1696	0.3045	0.0393	0.0203	0.0358	0.1134	0.0074	0.4039	0.2757
CamTE	0.0141 (-0.3087)	-0.0738 (0.0958)	0.1426 (-0.1620)	0.0092 (-0.0302)	0.0154 (-0.0049)	0.0242 (-0.0116)	0.0826 (-0.0308)	0.0045 (-0.0029)	0.0553 (-0.3486)	-0.0010 (-0.2767)
BM3D	0.0757 (-0.2471)	-0.0692 (0.1004)	0.0679 (-0.2367)	-0.0017 (-0.0410)	-0.0268 (-0.0470)	-0.0014 (-0.0372)	0.0411 (-0.0723)	0.0011 (-0.0064)	0.0802 (-0.3237)	-0.0114 (-0.2871)
Diff-CF	0.0070 (-0.3157)	-0.0130 (0.1567)	0.0242 (-0.2803)	0.0001 (-0.0392)	0.0057 (-0.0146)	-0.0018 (-0.0376)	0.0128 (-0.1006)	-0.0050 (-0.0124)	0.0399 (-0.3640)	-0.0007 (-0.2765)
Diff-CFG	0.0241 (-0.2986)	-0.0243 (0.1453)	0.0137 (-0.2908)	-0.0059 (-0.0452)	0.0128 (-0.0075)	0.0002 (-0.0355)	0.0202 (-0.0933)	0.0127 (0.0053)	0.0470 (-0.3569)	-0.0043 (-0.2800)

Table 6. MCC scores obtained for all the tested methods (including Bammey *et al.*) on FAU dataset [3].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.2329	0.0469	0.2670	0.0305	0.0336	0.0482	0.1289	0.0251	0.3373	0.2021
CamTE	0.0085 (-0.2244)	0.0516 (0.0047)	0.1173 (-0.1497)	0.0206 (-0.0099)	0.0427 (0.0091)	0.0434 (-0.0049)	0.1046 (-0.0243)	0.0277 (0.0026)	0.0572 (-0.2801)	0.0633 (-0.1388)
BM3D	0.0517 (-0.1812)	0.0517 (0.0048)	0.0559 (-0.2111)	0.0126 (-0.0179)	0.0377 (0.0041)	0.0331 (-0.0152)	0.0803 (-0.0486)	0.0243 (-0.0008)	0.0799 (-0.2574)	0.0583 (-0.1438)
Diff-CF	0.0056 (-0.2273)	0.0548 (0.0079)	0.0458 (-0.2213)	0.0159 (-0.0146)	0.0355 (0.0019)	0.0199 (-0.0283)	0.0602 (-0.0687)	0.0123 (-0.0128)	0.0520 (-0.2853)	0.0015 (-0.2006)
Diff-CFG	0.0184 (-0.2145)	0.0536 (0.0067)	0.0220 (-0.2451)	0.0143 (-0.0162)	0.0339 (0.0003)	0.0287 (-0.0196)	0.0646 (-0.0643)	0.0246 (-0.0005)	0.0592 (-0.2781)	0.0008 (-0.2012)

Table 7. IoU scores obtained for all the tested methods (including Bammey *et al.*) on FAU dataset [3].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.2971	0.1585	0.0184	0.1508	0.2948	0.1512	0.1948	0.0759	0.4864	0.1890
CameraTE	0.1651 (-0.1320)	0.1593 (0.0008)	0.0128 (-0.0056)	0.1263 (-0.0245)	0.1287 (-0.1661)	0.1360 (-0.0152)	0.1846 (-0.0102)	0.0661 (-0.0098)	0.3220 (-0.1644)	0.1830 (-0.0060)
BM3D	0.2934 (-0.0037)	0.1602 (0.0018)	0.0065 (-0.0120)	0.1118 (-0.0390)	0.1485 (-0.1463)	0.1379 (-0.0133)	0.1870 (-0.0079)	0.0613 (-0.0145)	0.3879 (-0.0985)	0.1830 (-0.0060)
Diff-CF	0.1797 (-0.1173)	0.1652 (0.0067)	0.0103 (-0.0082)	0.1222 (-0.0286)	0.0961 (-0.1987)	0.1404 (-0.0109)	0.1867 (-0.0082)	0.0692 (-0.0067)	0.3377 (-0.1488)	0.0000 (-0.1890)
Diff-CFG	0.2253 (-0.0717)	0.1571 (-0.0014)	0.0019 (-0.0166)	0.1136 (-0.0373)	0.1248 (-0.1700)	0.1510 (-0.0002)	0.1859 (-0.0090)	0.0609 (-0.0149)	0.3374 (-0.1490)	0.0000 (-0.1890)

Table 8. F1 scores for all tested methods on the COVERAGE dataset [13].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.2747	-0.0376	0.0075	0.0230	0.2617	0.0062	0.0615	-0.0571	0.4442	0.0326
CameraTE	0.1480 (-0.1267)	-0.0329 (0.0047)	0.0056 (-0.0020)	-0.0015 (-0.0245)	0.0790 (-0.1827)	-0.0230 (-0.0292)	0.0489 (-0.0127)	-0.0722 (-0.0151)	0.2614 (-0.1828)	0.0238 (-0.0088)
BM3D	0.2666 (-0.0081)	-0.0415 (-0.0039)	0.0051 (-0.0024)	-0.0281 (-0.0511)	0.0371 (-0.2246)	-0.0145 (-0.0207)	0.0515 (-0.0100)	-0.0771 (-0.0200)	0.3267 (-0.1175)	0.0236 (-0.0091)
Diff-CF	0.1598 (-0.1149)	-0.0238 (0.0138)	0.0011 (-0.0064)	-0.0065 (-0.0295)	0.0483 (-0.2133)	-0.0115 (-0.0176)	0.0514 (-0.0101)	-0.0602 (-0.0031)	0.2849 (-0.1594)	0.0000 (-0.0326)
Diff-CFG	0.2003 (-0.0745)	-0.0405 (-0.0029)	-0.0004 (-0.0079)	-0.0124 (-0.0354)	0.0680 (-0.1937)	0.0024 (-0.0038)	0.0475 (-0.0140)	-0.0717 (-0.0146)	0.2738 (-0.1704)	0.0000 (-0.0326)

Table 9. MCC scores for all tested methods (including Bammey *et al.*) on the COVERAGE dataset [13].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.2199	0.0879	0.0109	0.0856	0.1856	0.0858	0.1106	0.0423	0.3752	0.1082
CamTE	0.1162 (-0.1038)	0.0883 (0.0003)	0.0079 (-0.0030)	0.0711 (-0.0145)	0.0719 (-0.1137)	0.0770 (-0.0089)	0.1043 (-0.0063)	0.0361 (-0.0062)	0.2212 (-0.1541)	0.1046 (-0.0036)
BM3D	0.2151 (-0.0049)	0.0891 (0.0012)	0.0036 (-0.0072)	0.0617 (-0.0240)	0.0841 (-0.1015)	0.0773 (-0.0085)	0.1055 (-0.0051)	0.0336 (-0.0087)	0.2863 (-0.0889)	0.1046 (-0.0036)
Diff-CF	0.1278 (-0.0922)	0.0921 (0.0041)	0.0059 (-0.0050)	0.0687 (-0.0169)	0.0537 (-0.1320)	0.0790 (-0.0068)	0.1055 (-0.0051)	0.0383 (-0.0040)	0.2427 (-0.1325)	0.0000 (-0.1082)
Diff-CFG	0.1607 (-0.0592)	0.0871 (-0.0009)	0.0010 (-0.0099)	0.0630 (-0.0226)	0.0693 (-0.1163)	0.0858 (0.0000)	0.1051 (-0.0055)	0.0334 (-0.0090)	0.2386 (-0.1367)	0.0000 (-0.1082)

Table 10. IoU scores for all tested methods (including Bammey *et al.*) on the COVERAGE dataset [13].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.0300	0.6876	0.0638	0.0341	0.0853	0.0802	0.4881	0.0600	0.0655	0.0028
CameraTE	0.0069 (-0.0231)	0.6604 (-0.0272)	0.0490 (-0.0148)	0.0522 (0.0181)	0.2487 (0.1634)	0.1317 (0.0515)	0.5070 (0.0189)	0.0868 (0.0269)	0.2536 (0.1881)	0.0009 (-0.0018)
BM3D	0.0114 (-0.0186)	0.6264 (-0.0612)	0.0156 (-0.0482)	0.0575 (0.0234)	0.4571 (0.3718)	0.1312 (0.0509)	0.5161 (0.0280)	0.0909 (0.0309)	0.3338 (0.2683)	0.0020 (-0.0007)
Diff-CF	0.0035 (-0.0265)	0.5874 (-0.1002)	0.3084 (0.2446)	0.0500 (0.0159)	0.1431 (0.0577)	0.0898 (0.0095)	0.5182 (0.0301)	0.0604 (0.0004)	0.3661 (0.3006)	0.0025 (-0.0003)
Diff-CFG	0.0081 (-0.0219)	0.5908 (-0.0969)	0.1298 (0.0660)	0.0652 (0.0312)	0.1785 (0.0931)	0.1177 (0.0375)	0.5180 (0.0299)	0.0681 (0.0081)	0.4155 (0.3500)	0.0043 (0.0015)

Table 11. F1 scores for all tested methods on the DSO-1 dataset [6].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	-0.4471	0.0796	-0.0118	-0.3016	-0.3010	-0.3361	-0.0187	-0.2838	-0.8280	-0.1081
CameraTE	-0.0035 (0.4435)	0.0577 (-0.0219)	0.0062 (0.0180)	-0.0682 (0.2334)	-0.1165 (0.1845)	-0.0386 (0.2975)	-0.0037 (0.0151)	-0.1091 (0.1746)	-0.3528 (0.4752)	0.0016 (0.1098)
BM3D	-0.0425 (0.4046)	0.0070 (-0.0726)	-0.0041 (0.0077)	-0.0251 (0.2765)	-0.0795 (0.2215)	-0.0204 (0.3157)	-0.0035 (0.0152)	-0.1109 (0.1729)	-0.3161 (0.5119)	-0.0049 (0.1033)
Diff-CF	-0.0018 (0.4452)	0.0014 (-0.0782)	0.0228 (0.0346)	-0.0331 (0.2685)	-0.0621 (0.2389)	-0.0498 (0.2864)	-0.0026 (0.0162)	-0.0990 (0.1847)	-0.2850 (0.5430)	-0.0019 (0.1063)
Diff-CFG	-0.0186 (0.4285)	0.0010 (-0.0785)	0.0109 (0.0227)	-0.0473 (0.2543)	-0.1584 (0.1426)	-0.0619 (0.2742)	0.0028 (0.0215)	-0.1182 (0.1656)	-0.3032 (0.5248)	-0.0003 (0.1078)

Table 12. MCC scores for all tested methods (including Bammey *et al.*) on the DSO-1 dataset [6].

	CatNet	Bammey *et al.*	Choi	Comprint	MantraNet	Noiseprint	Shin	Splicebuster	TruFor	Zero
Original	0.0155	0.5260	0.0396	0.0186	0.0468	0.0438	0.3238	0.0316	0.0358	0.0015
CameraTE	0.0035 (-0.0120)	0.4943 (-0.0317)	0.0310 (-0.0086)	0.0280 (0.0094)	0.1457 (0.0990)	0.0724 (0.0286)	0.3402 (0.0164)	0.0464 (0.0147)	0.1512 (0.1154)	0.0005 (-0.0011)
BM3D	0.0058 (-0.0097)	0.4570 (-0.0690)	0.0090 (-0.0307)	0.0308 (0.0123)	0.3045 (0.2577)	0.0721 (0.0283)	0.3484 (0.0245)	0.0491 (0.0175)	0.2145 (0.1787)	0.0010 (-0.0005)
Diff-CF	0.0018 (-0.0137)	0.4162 (-0.1098)	0.2025 (0.1629)	0.0265 (0.0079)	0.0788 (0.0320)	0.0479 (0.0041)	0.3502 (0.0263)	0.0317 (0.0000)	0.2354 (0.1996)	0.0013 (-0.0003)
Diff-CFG	0.0041 (-0.0114)	0.4198 (-0.1062)	0.0843 (0.0446)	0.0348 (0.0162)	0.1048 (0.0580)	0.0643 (0.0205)	0.3501 (0.0263)	0.0357 (0.0041)	0.2794 (0.2436)	0.0022 (0.0007)

Table 13. IoU scores for all tested methods (including Bammey *et al.*) on the DSO-1 dataset [6].

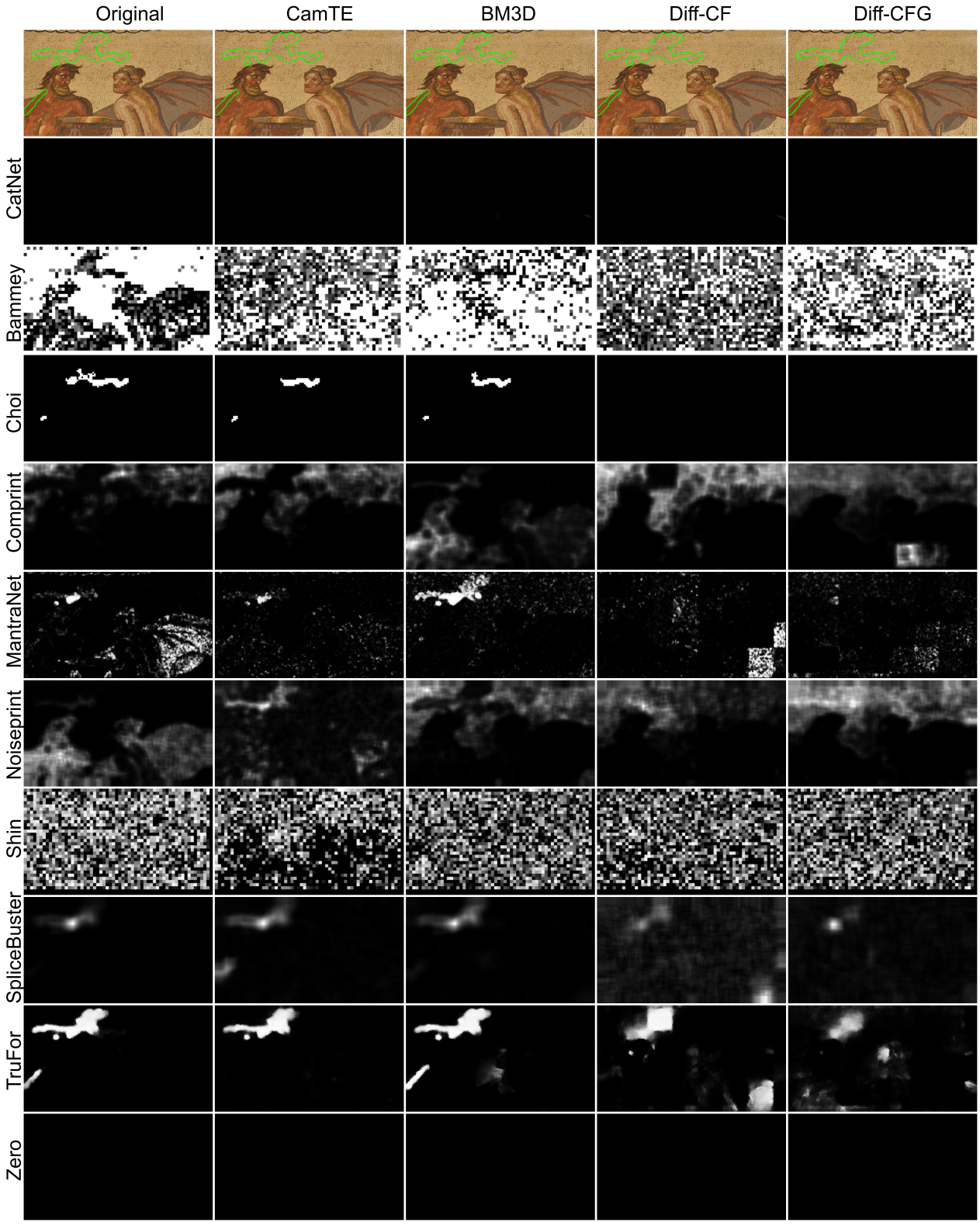

Figure 1. Results obtained by all considered forensics methods on the different versions of image `r7710a7fat` from the Korus dataset [8, 9]. This is the same image shown in Figure 1 in the paper, but with the results for all methods, even if they do not detect anything in the original image.

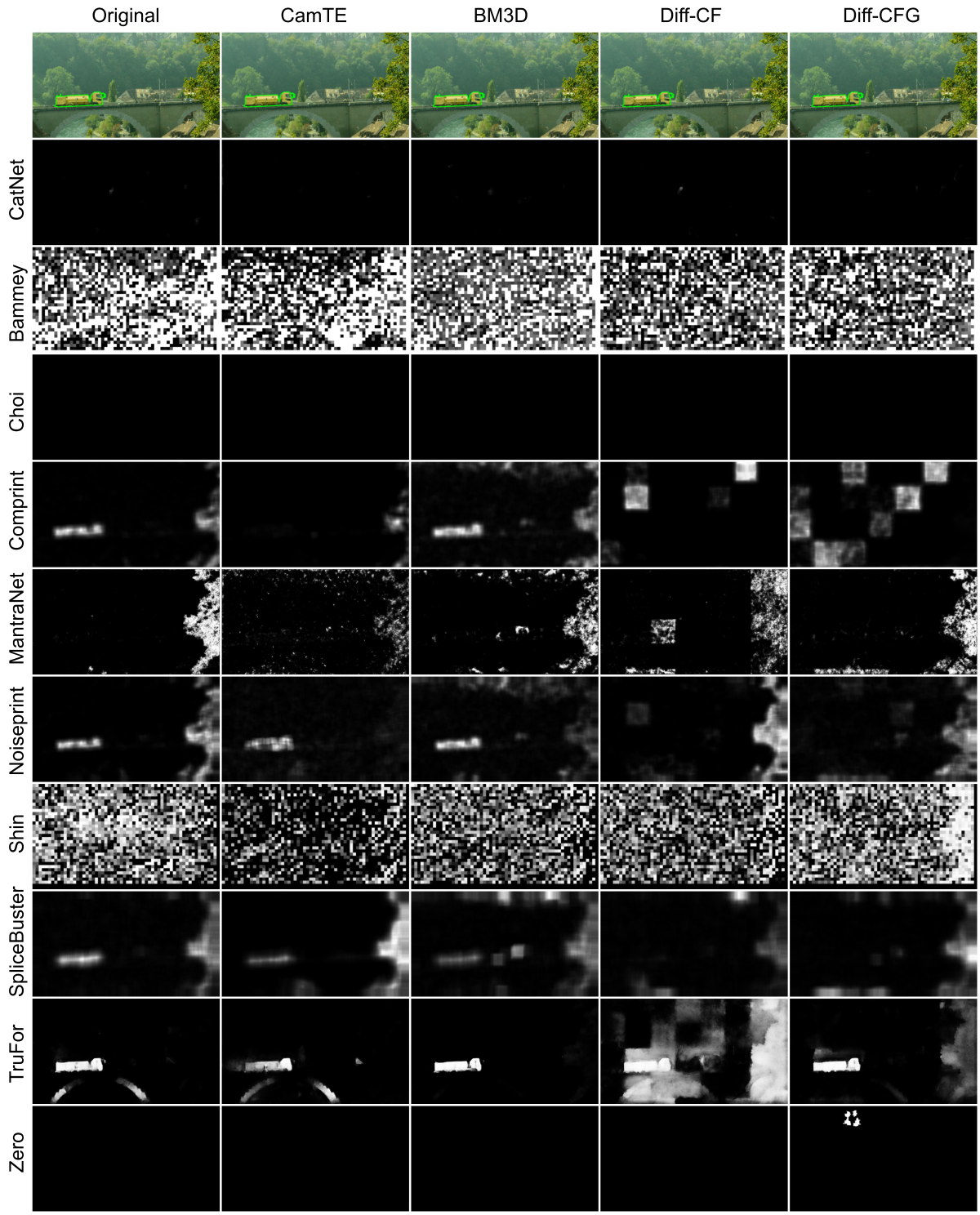

Figure 2. Results obtained by different forensics methods on the different versions of image `r02354285t` from the Korus dataset [8, 9]. In this image we observe that Noiseprintt, Splicebuster and TruFor give fairly correct detections in the original forged image. Splicebuster and Noiseprint present degraded detections once BM3D or CamTE are applied. However, the forgery is not even highlighted when *Diff-CF* or *Diff-CFG* are used as counter-forensics attacks. TruFor is more robust to such attacks. Still, their results degrade after *Diff-CF*

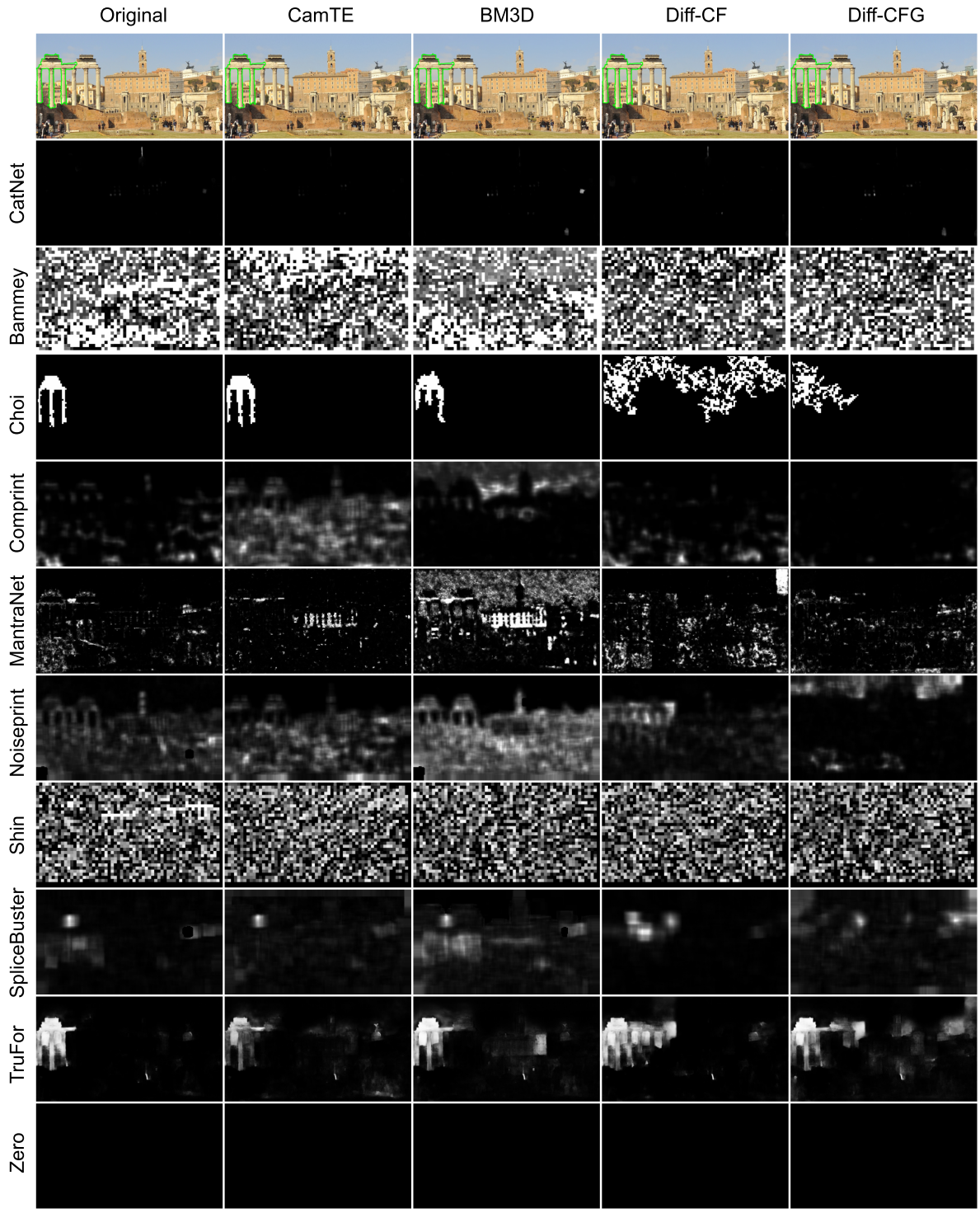

Figure 3. Results obtained by different forensics methods on the different versions of image `rbc87504ct` from the Korus dataset [8, 9]. In this image, we observe that only Choi and TruFor detect the forgery in the original image. Choi still detects the forgery once BM3D and CamTE are applied, but is unable to detect it once *Diff-CF* or *Diff-CFG*

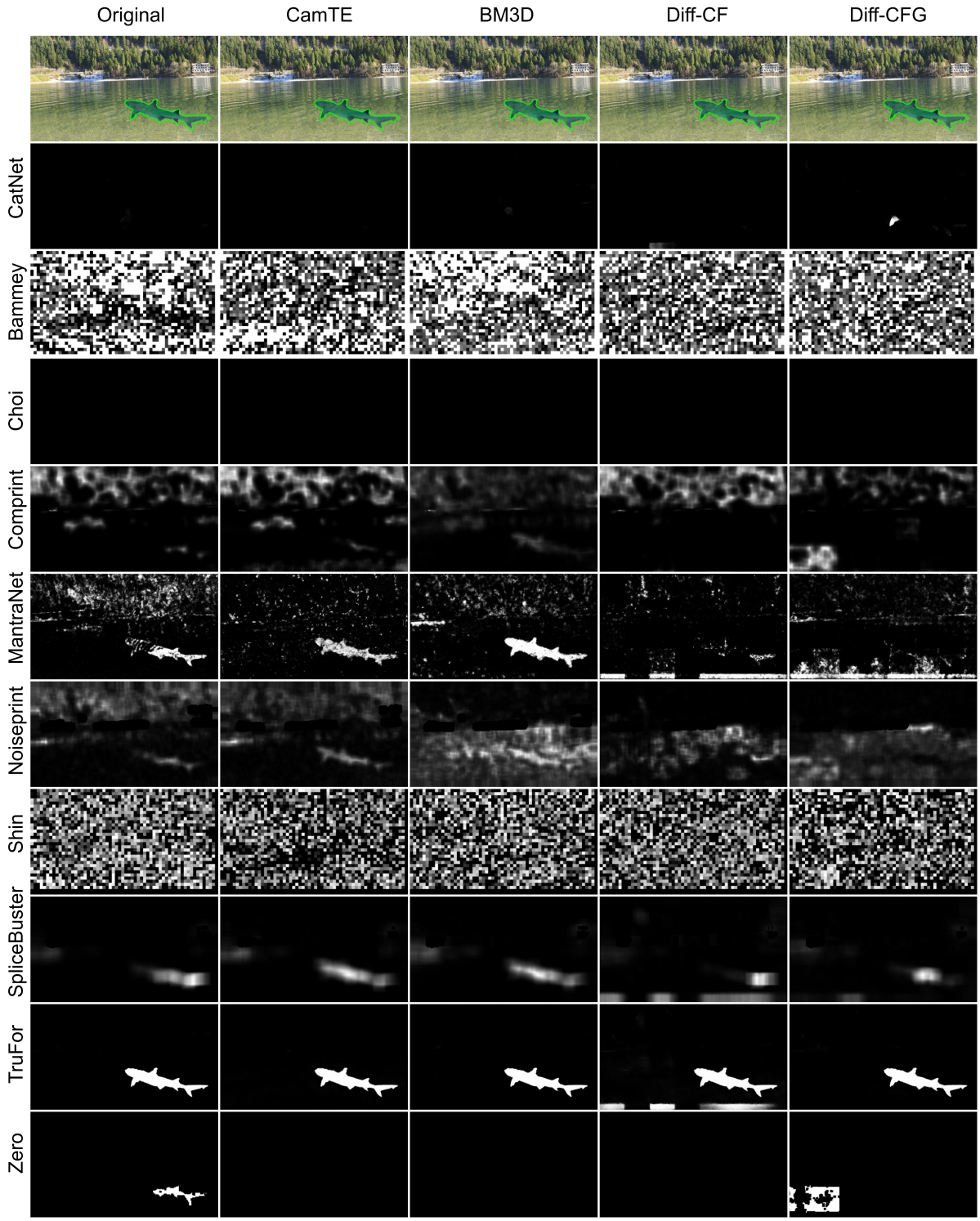

Figure 4. Results obtained by different forensics methods on the different versions of image `re6d1dc1et` from the Korus dataset [8, 9].

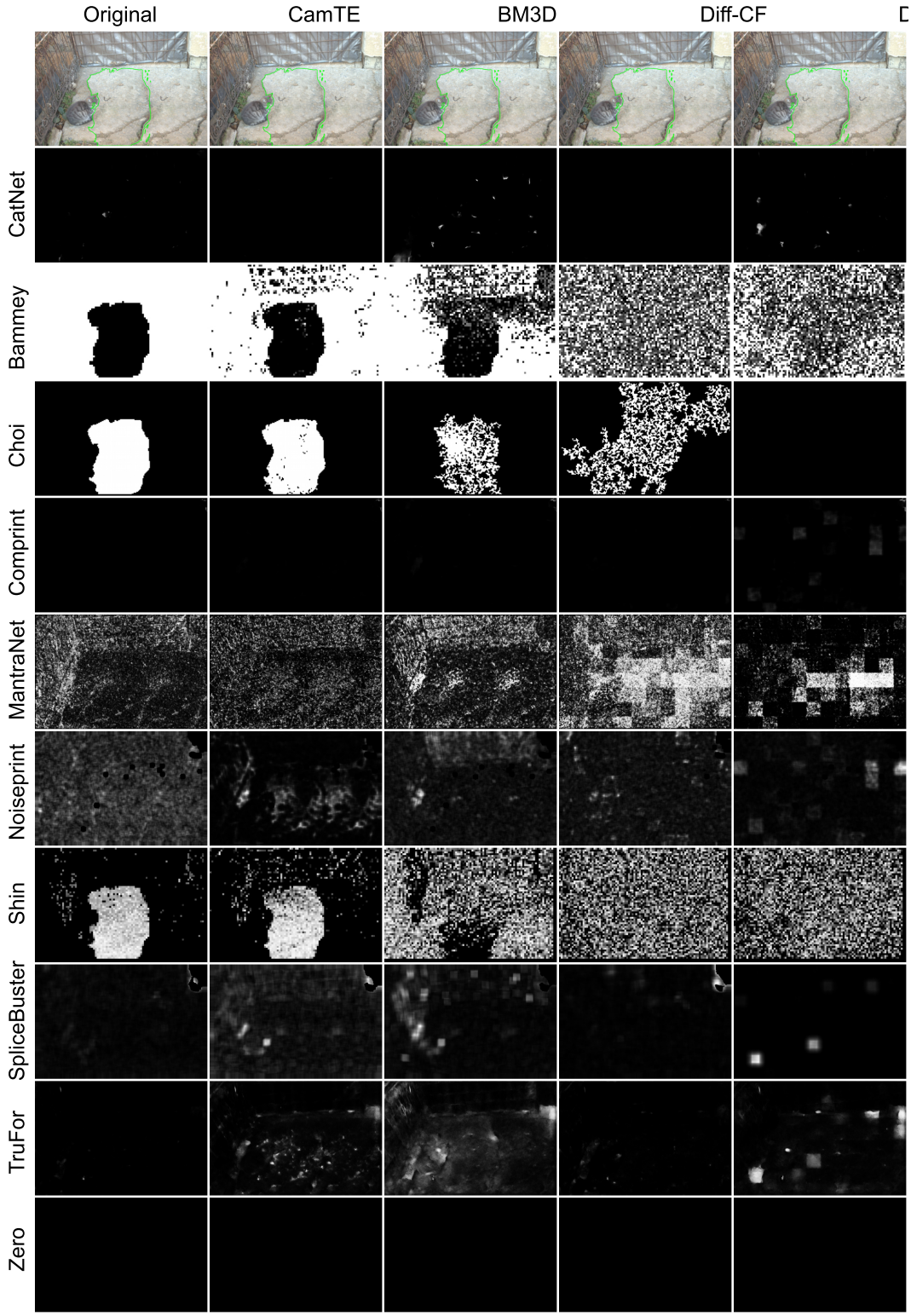

Figure 5. Results obtained by different forensics methods on the different versions of image `lone_cat_copy` from the FAU dataset [3].

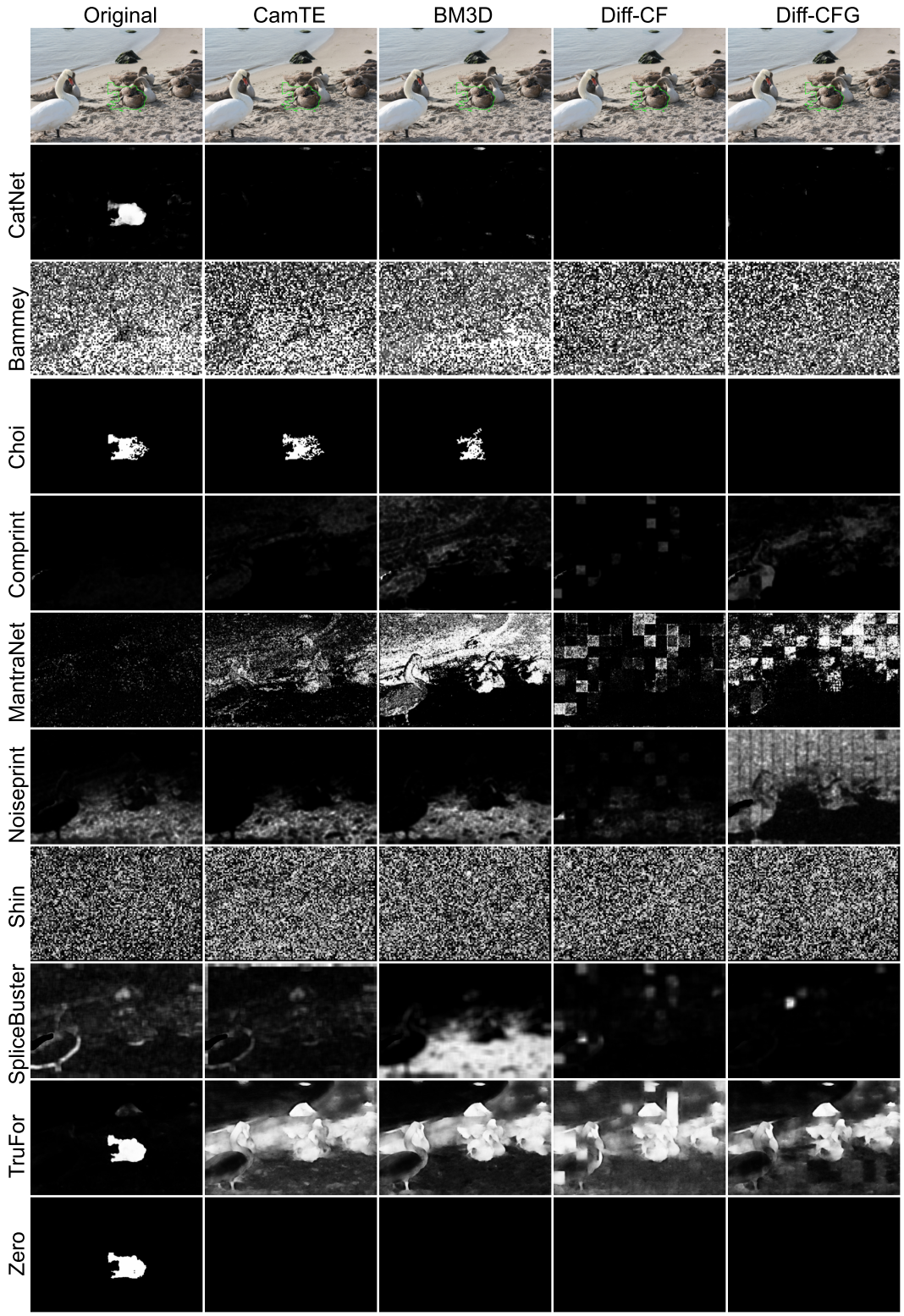

Figure 6. Results obtained by different forensics methods on the different versions of image `swan_copy` from the FAU dataset [3].