Robust Image Forgery Detection over Online Social Network Shared Images

Haiwei Wu, Jiantao Zhou, Jinyu Tian, and Jun Liu
State Key Laboratory of Internet of Things for Smart City
Department of Computer and Information Science, University of Macau
{yc07912, jtzhou, yb77405, yc07453}@um.edu.mo

1. Details of the testing datasets

The following four widely-used datasets are adopted for the performance evaluations.

DSO [2]: This dataset is formed by 100 skillfully-forged images, with the resolution of 2048×1536. To improve the photorealism, these forged images undergo a series of post-processing, *e.g.*, adjustments of color and illumination.

Columbia [5]: This dataset provides 160 splicing forgeries, where the source images are captured by four different cameras. These forged images are uncompressed and of high quality, with resolutions ranging from 757×568 to 1152×768.

NIST [1]: This dataset contains 564 high-resolution forgeries that are manipulated by commonly used tampering operations, *e.g.*, splicing, removal and copy-move, and post-processing with unknown editing software. The resolutions of the forgeries range from 500×500 to 5616×3744.

CASIA [4]: This dataset has 920 forgeries created by splicing with Adobe Photoshop CS3 version 10.0.1 on Windows XP. All images are resized to 384×256 and are in JPEG format.

To better evaluate the robustness of our proposed model against the transmission over OSNs, we utilize three most popular platforms, namely, Facebook, Weibo and Wechat, to further process the aforementioned testing datasets. Tab. 1 presents some basic impact of different OSNs on uploaded images, *e.g.*, Facebook retains the smallest compression while Wechat has the largest.

2. Implementation details

The proposed method is implemented using the PyTorch deep learning framework and adopting the Adam [6] with default parameters as the optimizer. The batch size is set to 32 and every epoch contains 312 batches. We train the network with an initial learning rate 1e-4, and halve it if the evaluation criteria fail to increase for 5 epochs until the convergence. All the images used in the training phase are cropped to 256×256, while there is no size limit for the testing phase.

OSNs	Max. Resolution	Avg. Size	Comp. Ratio
-	5616×3744	2489 KB	0.00%
Facebook	2048×1536	420 KB	83.13%
Weibo	1620×1080	195 KB	92.17%
Wechat	1440×1080	151 KB	93.93%

Table 1. Impact of different OSNs on dataset **NIST** [1].

3. Additional qualitative comparisons

More comparisons are given in Figs. 1-3.

References

[1] Nist nimble 2016 datasets. https://www.nist.gov/itl/iad/mig/nimble-challenge-2017-evaluation/. 1

[2] T. Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. Rezende Rocha. Exposing digital image forgeries by illumination color classification. *IEEE Trans. Inf. Forensics and Security*, 8(7):1182–1194, 2013. 1

[3] D. Cozzolino and L. Verdoliva. Noiseprint: a cnn-based camera model fingerprint. *IEEE Trans. Inf. Forensics and Security*, 15(1):114–159, 2020. 2, 3, 4

[4] J. Dong, W. Wang, and T. Tan. Casia image tampering detection evaluation database. In *IEEE China Summit Inter. Conf. Signal Info. Proc.*, pages 422–426. IEEE, 2013. 1

[5] Y. Hsu and S. Chang. Detecting image splicing using geometry invariants and camera characteristics consistency. In *IEEE Inter. Conf. Multim. Expo*, pages 549–552. IEEE, 2006. 1

[6] D. P. Kingma and J. Ba. Adam: a method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014. 1

[7] O. Mayer and M. C. Stamm. Forensic similarity for digital images. *IEEE Trans. Inf. Forensics and Security*, 15(1):1331–1346, 2020. 2, 3, 4

[8] Y. Wu, W. AbdAlmageed, and P. Natarajan. Mantra-net: manipulation tracing network for detection and localization of image forgeries with anomalous features. In *Proc. IEEE Conf. Comput. Vis. Pattern Recogn.*, pages 9543–9552, 2019. 2, 3, 4

[9] P. Zhuang, H. Li, S. Tan, B. Li, and J. Huang. Image tampering localization using a dense fully convolutional network. *IEEE Trans. Inf. Forensics and Security*, 16(1):2986–2999, 2021. 2, 3, 4

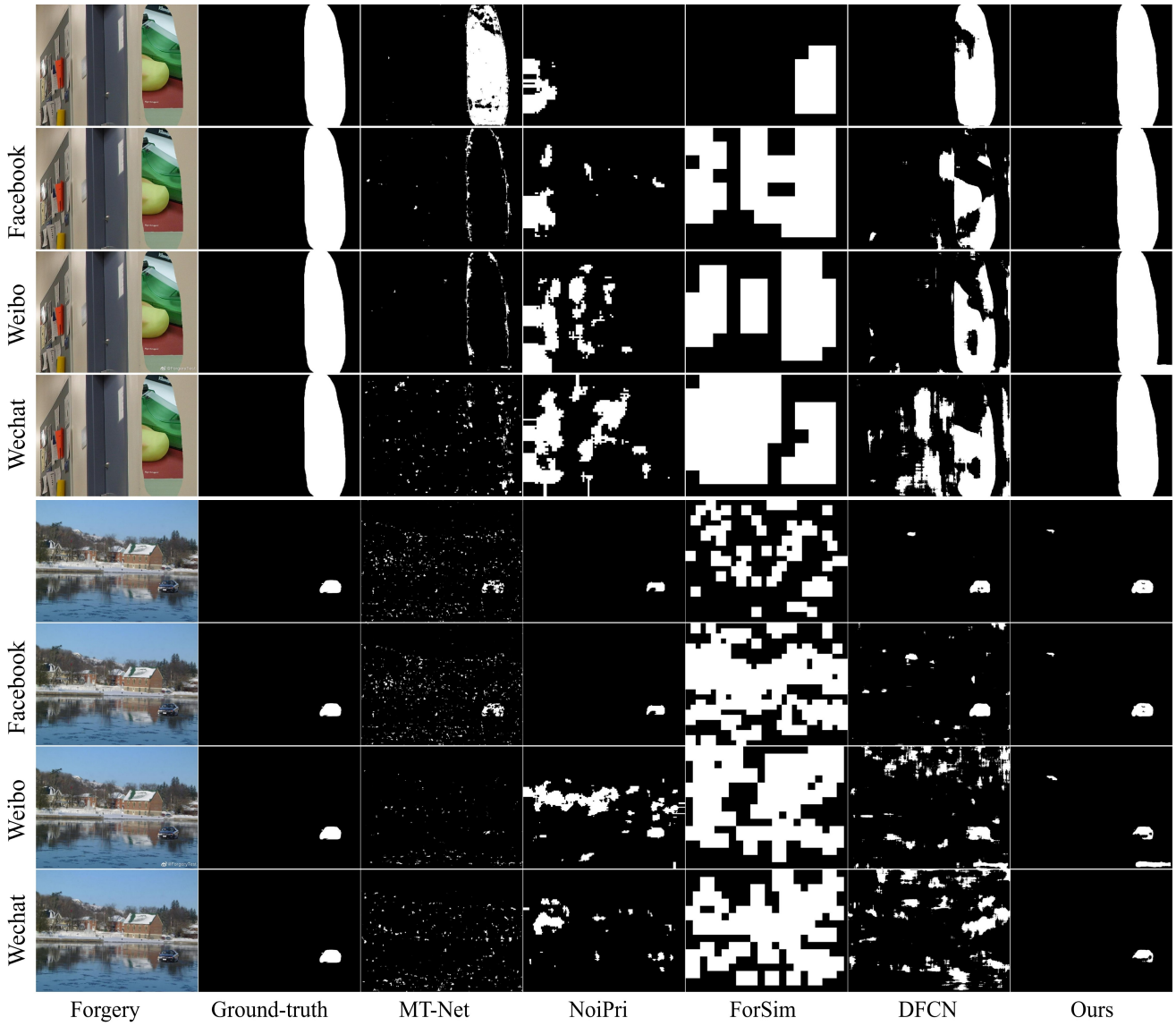

Figure 1. Qualitative comparisons for detecting the OSN-transmitted forgeries. For each row, the images from left to right are forgery (input), ground-truth, detection result (output) generated by **MT-Net** [8], **NoiPri** [3], **ForSim** [7], **DFCN** [9] and ours. The forgeries in each group from top to bottom are the cases without OSN transmission, and with Facebook, Weibo and Wechat transmissions, respectively.

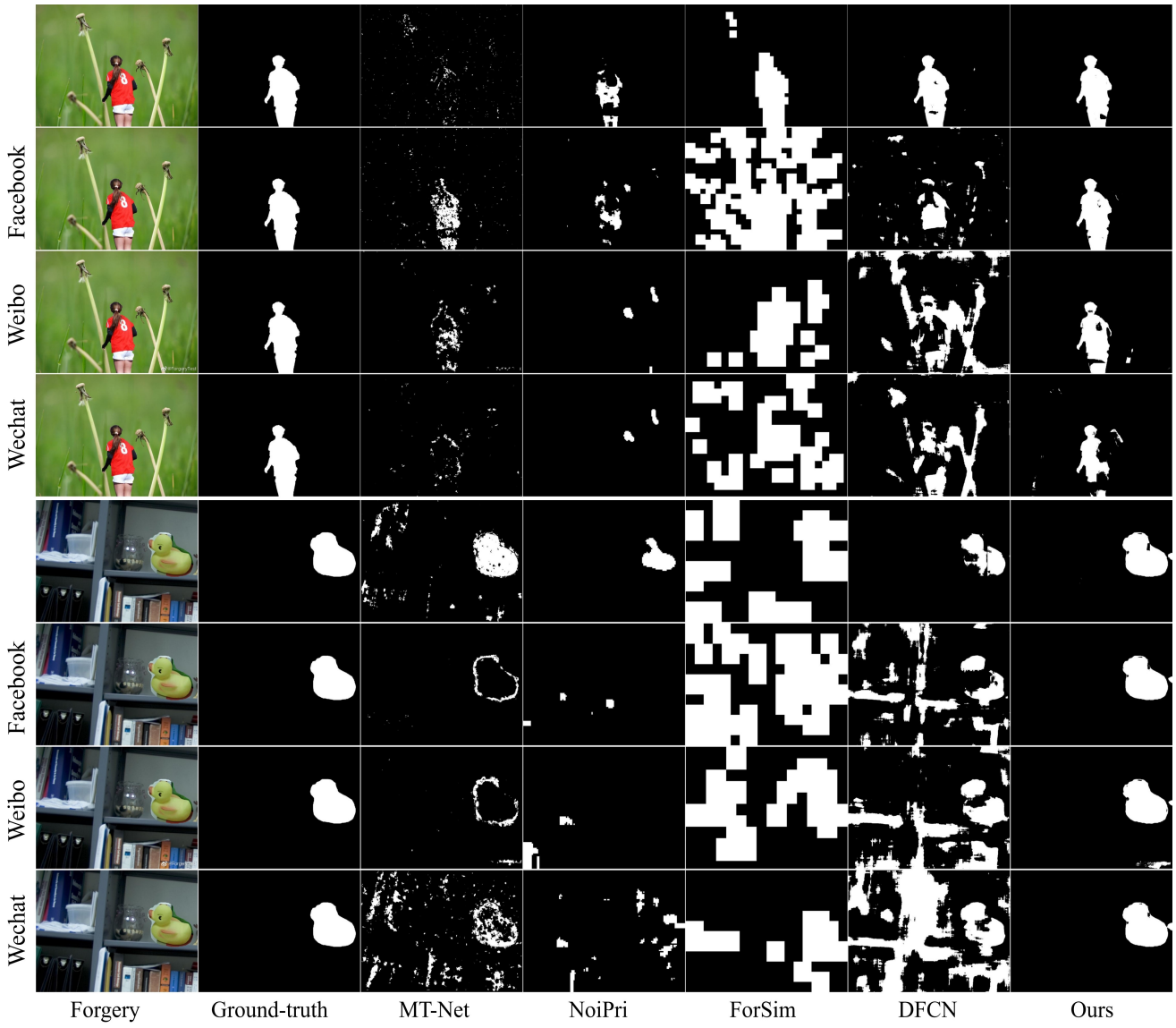

Figure 2. Qualitative comparisons for detecting the OSN-transmitted forgeries. For each row, the images from left to right are forgery (input), ground-truth, detection result (output) generated by **MT-Net** [8], **NoiPri** [3], **ForSim** [7], **DFCN** [9] and ours. The forgeries in each group from top to bottom are the cases without OSN transmission, and with Facebook, Weibo and Wechat transmissions, respectively.

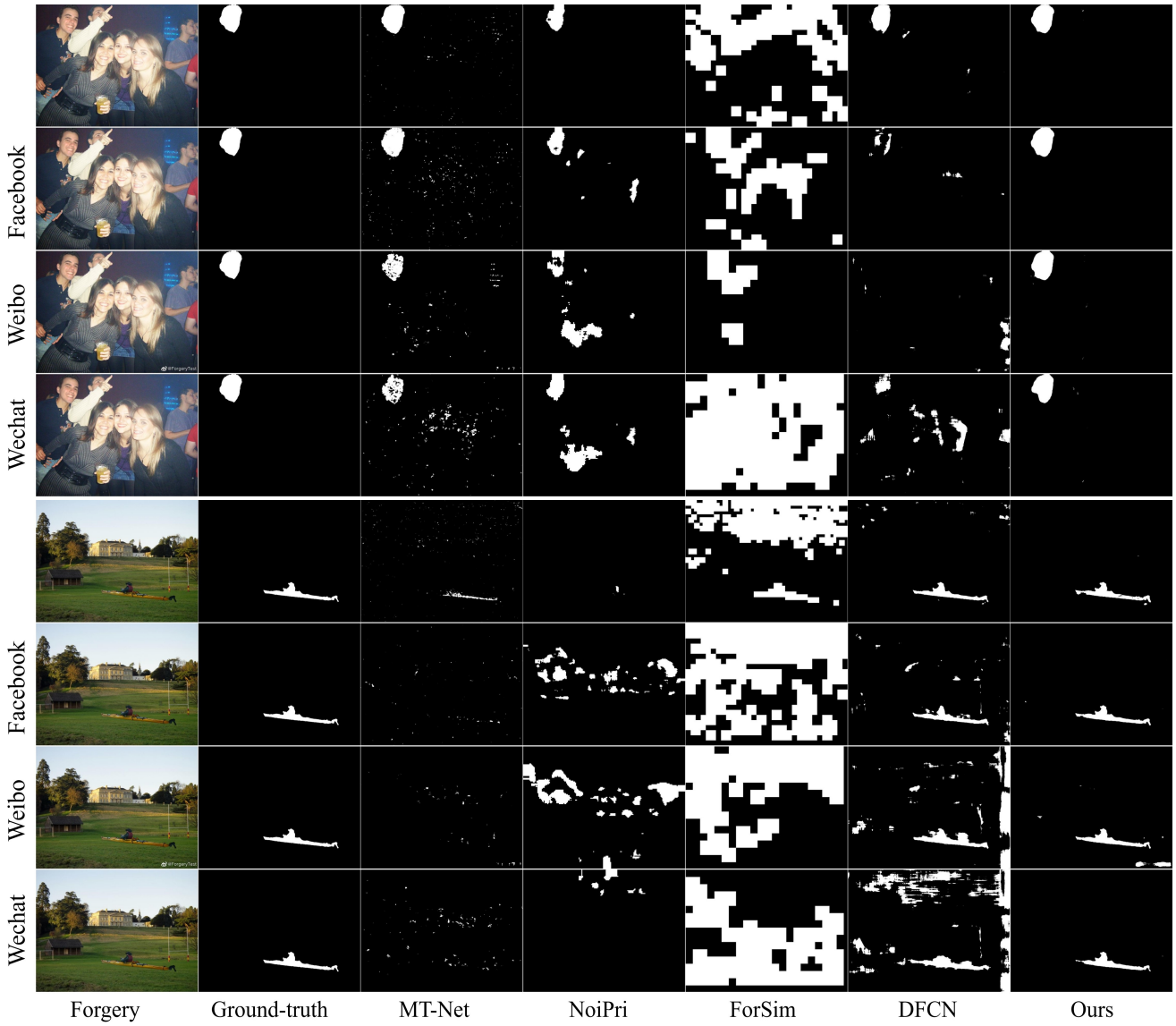

Figure 3. Qualitative comparisons for detecting the OSN-transmitted forgeries. For each row, the images from left to right are forgery (input), ground-truth, detection result (output) generated by **MT-Net** [8], **NoiPri** [3], **ForSim** [7], **DFCN** [9] and ours. The forgeries in each group from top to bottom are the cases without OSN transmission, and with Facebook, Weibo and Wechat transmissions, respectively.