Patterns

CellPress
OPEN ACCESS

Perspective

AI-enabled image fraud in scientific publications

Jinjin Gu,[1] Xinlei Wang,[1] Chenang Li,[2] Junhua Zhao,[2,3,*] Weijin Fu,[4,*] Gaoqi Liang,[2] and Jing Qiu[1]
[1]School of Electrical and Information Engineering, University of Sydney, Sydney, NSW, Australia
[2]School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, China
[3]Shenzhen Institute of Artificial Intelligence and Robotics for Society (AIRS), Shenzhen, China
[4]Department of Urology, The First Affiliated Hospital of Guangxi Medical University, Guangxi, China
*Correspondence: zhaojunhua@cuhk.edu.cn (J.Z.), fuwj66@aliyun.com (W.F.)
https://doi.org/10.1016/j.patter.2022.100511

THE BIGGER PICTURE This perspective reports on the vast risk of potential image fraud based on artificial intelligence (AI) generative technologies in academic publications that have been neglected. This article discusses the scenarios, capabilities, and effects of AI algorithms used in academic fraud. The issue described in this perspective is not only relevant to computer scientists. As members of the scientific community, each of us will be deeply involved in the peer-review process. Each of us may be deceived by the AI image-fraud methods described in this article. Although the algorithm developing itself belongs to the field of computer science, its impact, as mentioned in this perspective, is more related to a wider range of scientific fields, such as biology, medicine, and natural science. Arousing their attention to this threat is a necessary condition to resist this threat. Combined with state-of-the-art AI research, this perspective also discusses possible preventive measures to respond to this potential threat.

Concept: Basic principles of a new data science output observed and reported

SUMMARY

Destroying image integrity in scientific papers may result in serious consequences. Inappropriate duplication and fabrication of images are two common misconducts in this aspect. The rapid development of artificial-intelligence technology has brought to us promising image-generation models that can produce realistic fake images. Here, we show that such advanced generative models threaten the publishing system in academia as they may be used to generate fake scientific images that cannot be effectively identified. We demonstrate the disturbing potential of these generative models in synthesizing fake images, plagiarizing existing images, and deliberately modifying images. It is very difficult to identify images generated by these models by visual inspection, image-forensic tools, and detection tools due to the unique paradigm of the generative models for processing images. This perspective reveals vast risks and arouses the vigilance of the scientific community on fake scientific images generated by artificial intelligence (AI) models.

INTRODUCTION

Inappropriately duplicating and fabricating images in scientific papers would have serious consequences. Editors and reviewers may be deceived, scientific communities may be misled, and research resources may be wasted. To prevent this type of misconduct, people are motivated to search for efficient detection and forensic strategies. Recently, there is a high expectation that artificial intelligence (AI) may bring new techniques for automatic inspection of images fraud in academic publications. Despite controversies and difficulties, progress in this area is being made.[1]

However, the whirlwind of progress in AI has not only produced a steady stream of advanced image-retrieval and fraud-detection techniques but has also brought about promising image-editing and -generation tools.[2–7] These tools can generate images that are increasingly indistinguishable for automated checking systems and even human judgment. A successful representative of image-generation techniques is the generative adversarial network (GAN).[8] The GAN takes the adversariness of two deep neural networks (a generator and a discriminator) as the training paradigm and then automatically generates high-fidelity images out of nothing. Advanced generative models may be potentially applied to many fields. When they are widely used, "seeing is believing" may no longer hold true.[9]

It is not news that generative models are abused to a large extent and pose a threat to society. A typical example is Deepfake,[10] an algorithm that generates realistic fake images and videos in which a person in an existing image is replaced with someone else. News and videos produced by Deepfake can have tremendous implications. As more fields are involved, the threats brought about by these new technologies cannot be

This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

ignored. An important issue that we need to be alerted to is that intelligent generative models are used to forge images of scientific evidence and thus threaten academic integrity in publishing. Although it has not been formally reported, due to the effectiveness and easy accessibility of these advanced technologies, such forgeries, some of which are not detectable at all, may become disturbingly common.

In this perspective, we reveal how these advanced generative models might be abused for scientific image fraud with examples. We also demonstrate the identification accuracy of this fraud by both human experts and AI techniques. Our examples and identification results show troubling signs that this type of image fraud is efficient and covert and is expected to pose a threat to academic publishing. At last, we explore possible responses to this threat. We anticipate that our article will attract the scientific community's attention and bring about discussions on this emerging issue so that better responses can be developed and implemented.

SCIENTIFIC IMAGE FRAUD USING GENERATED MODELS

Although the criteria of detecting misconduct in the scientific community are not uniform, the following three situations are acknowledged as severe cases: (1) fabrication of non-existent images, (2) falsification or manipulation of existing images, and (3) plagiarism. Among the cases that have been revealed above, inappropriate duplication and editing are the most common measures to commit these misconducts.[11] The duplication of images includes using multiple identical images to represent different experimental results, reusing or plagiarizing images in previous publications as new experimental evidence, or creating images by synthesizing existing ones using rotating, scaling, cropping, and splicing. The editing of images involves using image-processing software to modify or tamper with images to meet authors' expectations. However, both duplication and modification would leave traces, such as repetition coincidences that are impossible to get to appear naturally or traces of modification revealed by image-forensic tools such as inverse or false-color view.

In contrast to the above "traditional" methods, generative models generate images from scratch or regenerate existing images. The following scenarios are used to show how generative models are misused. Experienced researchers may collect many scientific images in a specific field first. The most general paradigm of generative models is to capture the underlying patterns in these scientific images and fit the distribution of the target data. Sampling using trained generative models can produce fake images that follow patterns similar to the real images. Images generated by these models are visually realistic and even scientifically self consistent (see Figure 1A). These images are meaningless in science, but one may use them as evidence to report experiments that have never been conducted. In any field where a large amount of image data can be obtained, such generated images may become a source of fake scientific images.

Different from the above cases in which the models need to be trained using a large image dataset, another novel generative paradigm allows the model to be trained with a single image. The trained model can be used for image resampling or manipulation. SinGAN is an example of this paradigm.[13] It learns patch distribution hierarchically at different scales of an image and then regenerates high-quality, diverse images with the main style or with the content unchanged. The regenerated images preserve the statistical characteristics but have different local details compared with the original ones (see Figure 1B). This technique can be used to plagiarize published images or reuse existing images, such as reporting non-existent control-group experiments.

Apart from the fact that generated fake images may be used deliberately, modifications may also be used to produce images that meet authors' expectations in experiments. The generative models manipulate images by directly generating images featuring similar appearances but modified content.[13,14] For example, one may remove some cells from the image through an inpainting generative model or add new cells through an image harmonization model (see Figure 1C). In some cases, generative models are more remarkable for their ability to create images of different things that may not exist at all. The generative model may disentangle features of images during the training phase. Based on this, the model may mix these features and synthesize images that do not conform to the natural distribution of data, e.g., proteins that appear in a cell's image where they should not have appeared.

RISKS OF AI-ENABLED IMAGE FRAUD

The dangers of the fraud methods described above can be brought up in several ways, of which their difficult-to-detect nature is the most important one. Firstly, it is difficult for editors and reviewers to find such frauds through visual inspection during the peer-review process. A user study indicates that scientific images generated by generative models are likely to deceive the judgment of human experts (see Figure 2). The distribution of collected human ratings shows interesting patterns. It can be seen that humans tend to be more confident in the judgment of natural images, which is reflected in the fact that most of the ratings are either "definitely real" or "definitely fake." For scientific images, their relatively simple image structure makes them easier to learn by generative models. The difference between the real and generated images is more subtle and imperceptible, so the average rating is biased toward "real," and the ratings are also less confident. Secondly, the image-generation process is controlled by random noise, and different noise vectors create different images. The unnatural repetition between generated fake images no longer exists, which renders duplication inspection based on retrieving and comparing image details invalid. Third, as image generation is an end-to-end integrated process, there are no intrinsic irregularities of modification that existing image-forensic tools can detect. Detection of such generated images relies on features or fingerprints left by the generative model. This introduces very large uncertainties and difficulties for detection.

In response to the threats posed by fake scientific images, research on the quality and integrity in scientific literature has attracted significant attention.[15,16] The current forensic methods for scientific image fraud rely on unnatural repetitions found through visual inspection[11] or intrinsic irregularities visualized through forensic tools. On the research front, AI is also expected to bring about tools for efficient automatic image-fraud detection to address the difficulty of detecting such fraud.[17–20] Recent

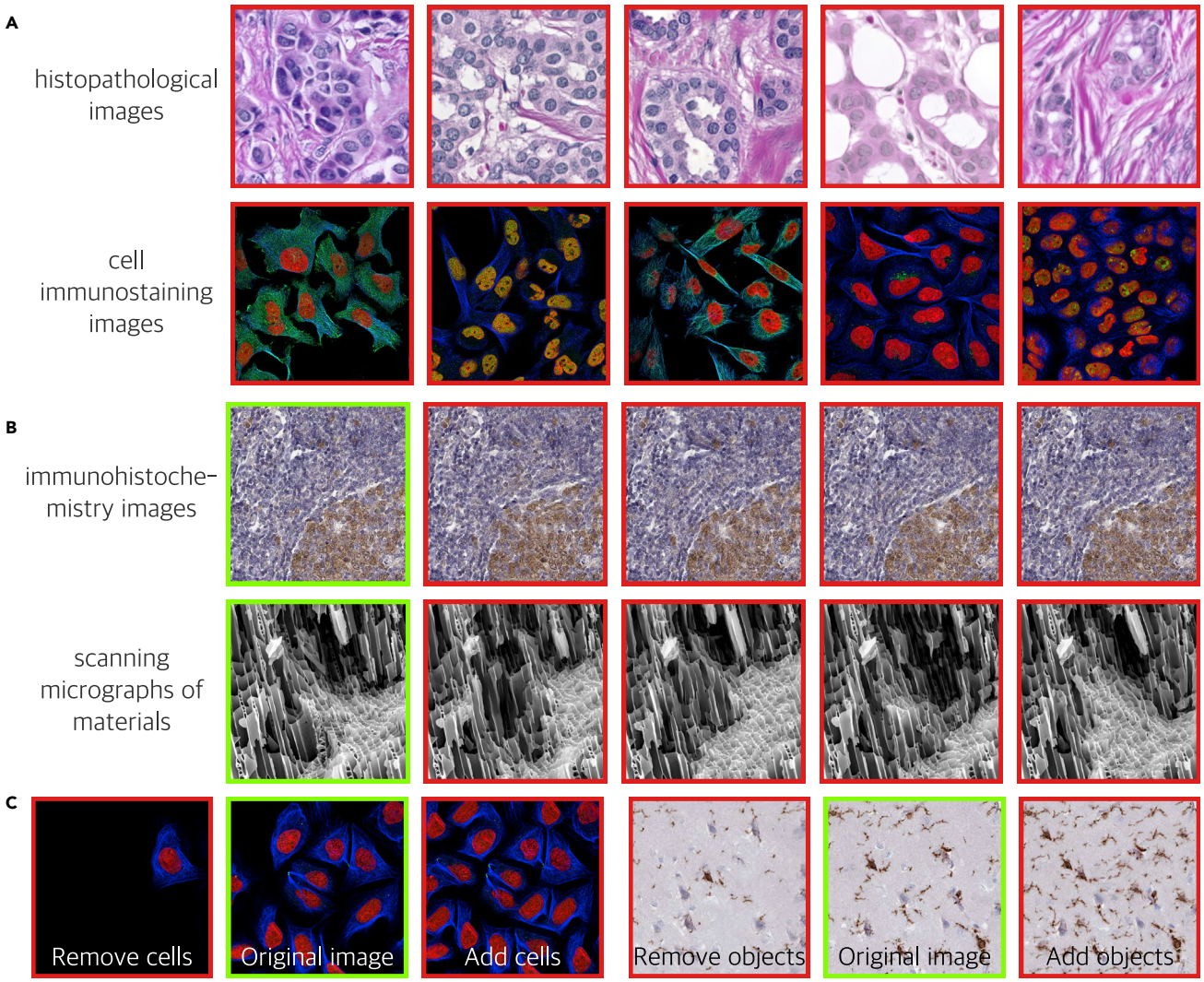

Figure 1. Scientific image fraud by intelligent models

We show several fake images generated by generative models. The images with the red border are all computer generated, while the images with the green border are real ones.

(A) Sampling fake images from a well-trained generative model. Fake images above are created by an advanced generation technology called StyleGAN.[12] All these images are fake and meaningless in science.

(B) Regenerating images using a generative model trained on a single image. For each group, the last four images are regenerated from the first real image. These images can escape the duplication detection methods based on the comparison of details because they have totally different local details.

(C) Manipulating images using generative models. The generative models manipulate images by directly generating images that are similar in features but with modified content. For each group, the images in the middle are the original images, and the images on both sides are deliberately manipulated fake images.

studies suggest that images created by generative models may retain detectable systematic flaws that may distinguish them from authentic images.[21–25] AI forensic tools can be built to tell generated images from real ones. We test two state-of-the-art AI forensic tools by using them to analyze the fake scientific images described above. We include the image classifier provided by Wang et al.,[21] which was trained on ProGAN[6]-generated images with careful pre- and post-processing and data augmentation, and the GAN image detector proposed by Gragnaniello et al.,[26] which was developed based on a limited sub-sampling network architecture and a contrastive-learning paradigm. The results are shown in Figures 3A and 3B. Wang et al.[21] only achieved a similar accuracy performance to human visual inspection, and Gragnaniello et al.[26] achieved generally better performance against Wang et al.[21] But neither method can make good enough detections, and relying on such accuracy is not enough to mitigate the threat of image forgery based on generative models. Imperfect automated forensic tools are also highly vulnerable. A malicious user may simply select a fake image that passes the detection threshold, as a single fake image is the only thing he/she needs to achieve his/her goal. The limitation of existing methods points to the fact that the detection and forensics of scientific image fraud is still open to questions.

Another equally dangerous thing is that, unlike manually modifying or forging images with software, the cost of using these advanced models is close to negligible. For one thing, researchers

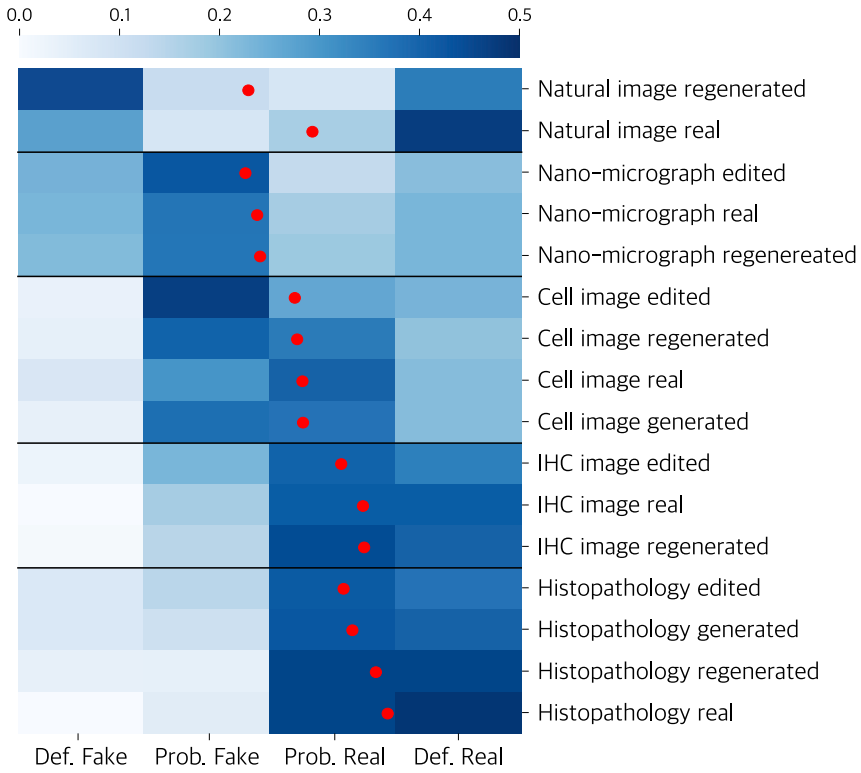

Figure 2. Images forged by generative models are hard to distinguish

We conducted a human-opinion study. This figure shows the normalized histogram of votes per image type. The image used for evaluation consists of five categories: (1) natural images, (2) scanning micrographs of nano materials (nano-micrograph), (3) cell immunostaining images, (4) immunohistochemistry (IHC) images, and (5) histopathological images. In total, 800 images are involved, and each image is rated by at least ten medical experts. The voting scale was between 1 to 4 corresponding to the following: 1 – definitely fake, 2 – probably fake, 3 – probably real, and 4 – definitely real. Mean scores are shown as red dots.

are very open to the open source and sharing of these advanced generative-model technologies. The result is that all these technologies for intelligent generative models may be shared with anyone defenselessly; for example, all of the techniques involved in this article are easily available on the Internet. This greatly lowers the barrier to entry for anyone trying this type of technology, which, in turn, further gives rise to the possibility for the abuse of these technologies. For another thing, many intelligent generative models can automatically process and generate images without human intervention. Making fake scientific images no longer requires complicated human labor but can be mass produced. This has the potential to make it easier for some "paper factories"[27] to systemically produce falsified research papers.

THE FIGHT AGAINST AI-ENABLED IMAGE FRAUD

There is an urgent need for effective measures to respond to this potential threat. Most critically, people need first to be subjectively prepared for the new risks brought by these new technologies. Although no cases of using such intelligent image technologies have been reported, a more worrying possibility is that this kind of misconduct has quietly occurred somewhere. The problem is that it has not yet been found. Nevertheless, a window of opportunity remains open to reduce the risks to a certain extent by improving the management system or process before such a high-tech fraud pervades in scientific publications.

In terms of all preventive measures that may be taken for the moment, asking authors to provide more detailed high-resolution raw image data is the most convenient one. Although impressive progress has been made, generative models are still straggled in generating large-size high-fidelity images. The high computational resources and algorithm complexity required to generate large-size fake images will increase the threshold of such frauds. In addition, we should continue to develop forensic tools for advanced image-generation and -processing models. Tools specialized for scientific images should also be given great importance, as we see that the detection accuracy is significantly better for natural images than for scientific images. An important reason for this is that the existing tools are developed based on natural images. Although the current situation is not optimistic, the advantage of these forensic tools lies in the ability to perform large-scale automatic screening. At last, when developing new image-generation technology, we must again consider the possible social impact of such technologies and attempt to eliminate the risk of such technologies being abused as much as possible. For example, when releasing the source code of generative models that may be used for improper purposes, we may annotate generated images through encryption or steganography.

CONCLUSION

Our discussion demonstrates that AI-enabled image fraud may pose serious challenges to the field of academic publishing. The difficult-to-detect nature, inexpensiveness, availability, and ease-of-use of advanced image generative models become major sources of threats when they are abused for scientific image fraud. We also explore responses to this type of fraud. However, the confrontation between new technologies and countermeasures that prevent them from being abused will become an enduring cat-and-mouse game. Perhaps when these advanced technologies are abused, our cost of obtaining the truth has been irretrievably increased.

Appendix A: Data acquisition

In this perspective, we discussed three methods for image fraud in the main text, namely image generation, image regeneration or resampling, and image editing. The images used for evaluation may be classified into five categories: (1) natural images, such as natural sceneries, architectures, flora, and fauna; (2) scanning micrographs of nano materials collected from Internet; (3) cell immunostaining confocal microscope images from the Human Protein Atlas dataset;[28] (4) immunohistochemistry (IHC) images collected from clinical and the

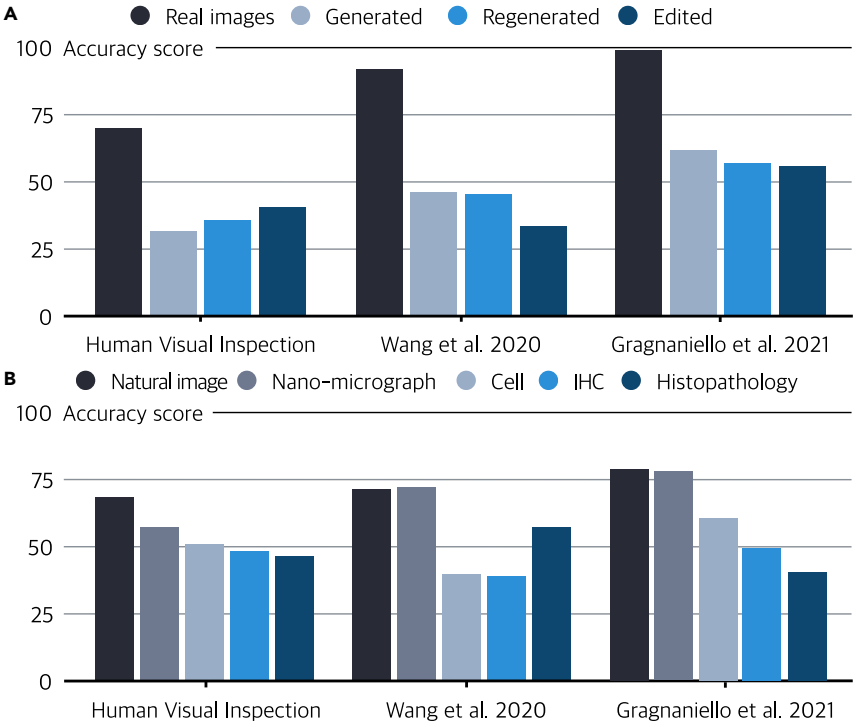

Figure 3. The accuracy of detecting generated images for each test subject

(A) Image-fraud-detection accuracy for different fraud methods.

(B) Image-fraud-detection accuracy for different image types.

Human Protein Atlas datasets;[28] and (5) histopathological images from the breast cancer histopathological dataset (BreCaHAD).[29]

Two generative models based on StyleGAN[12] were trained by using the cell immunostaining image dataset and the BreCaHAD histopathological image dataset. The generated images are 512 × 512 pixels. For the training of the StyleGAN generator, we follow the official suggestions. Eight NVIDIA V100 computing cards were used in the training, and the process lasted for 14 days. We used SinGAN[13] for the image-regeneration experiments. For each image category, we selected 10 images and regenerated 5 times for each trained model. The regenerated images are 512 × 512 pixels. We follow the official suggestions of applying SinGAN. We also used the NVIDIA V100 computing card for experiments. It takes about 5 h to calculate one image. For the edited images, we also employed SinGAN. SinGAN achieves image manipulation or image harmonization by regenerating images based on a modified input image. We demonstrated adding or removing cells or objects in the images by using cell immunostaining and IHC images.

Appendix B: User study

A total of 800 images were involved in the user study. For each image category and each image-fraud method, we prepared at least 50 images. We also prepared 50 real images for each category as a comparison. Ten volunteers with rich experience in the fields of medicine and biology participated in the study. Each volunteer was asked to fill out a set of questionnaires, and each questionnaire was limited to 16 questions. In order to prevent volunteers from feeling exhausted, the questionnaire was conducted at different times during a week. In each questionnaire, volunteers saw a set of the above images. Volunteers were informed that these images may appear in some scientific papers, popular science articles, and reports. They were also informed that these images may contain a number of unknown false, edited, or forged content. Each image may appear multiple times, and the number of times each image appeared has nothing to do with its authenticity. We asked volunteers to evaluate the authenticity of each picture based on their professional knowledge and intuition. The voting scale was between 1 and 4: 1 – definitely fake, 2 – probably fake, 3 – probably real, and 4 – definitely real. Volunteers were invited to choose the most suitable option.

ACKNOWLEDGMENTS

We thank all experts who participated in the user study. This work was supported in part by the Shenzhen Institute of Artificial Intelligence and Robotics for Society (AIRS) and the National Natural Science Foundation of China (72171206, 71931003, and 72061147004).

AUTHOR CONTRIBUTIONS

J.G. and J.Z. designed the study. C.L. facilitated data collection. J.G. and C.L. collected and analyzed the data. J.G. and X.W. wrote the manuscript with input from all authors. W.F. provided professional knowledge about the fields involved in this article, such as life and medical sciences. J.Z. coordinated the project.

DECLARATION OF INTERESTS

The authors declare no competing interests.

REFERENCES

1. Van Noorden, R. (2020). Pioneering duplication detector trawls thousands of coronavirus preprints. Nature. https://doi.org/10.1038/d41586-020-02161-3.

2. Wang, X., Yu, K., Wu, S., Gu, J., Liu, Y., Dong, C., and Qiao, Y.; Change Loy (2018). Esrgan: enhanced super-resolution generative adversarial networks. In Proceedings of the European conference on computer vision (ECCV) workshops, p. 0.

3. Gu, J., Shen, Y., and Zhou, B. (2020). Image processing using multi-code gan prior. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 3012–3021.

4. Chan, K.C., Wang, X., Xu, X., Gu, J., Loy, C., and Glean, C. (2021). Generative latent bank for large-factor image super-resolution. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 14245–14254.

5. Wang, X., Li, Y., Zhang, H., and Shan, Y. (2021). Towards real-world blind face restoration with generative facial prior. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 9168–9178.

6. Karras, T., Aila, T., Laine, S., and Lehtinen, J. (2018). Progressive growing of gans for improved quality, stability, and variation. In International Conference on Learning Representations.

7. Shen, Y., and Zhou, B. (2021). Closed-form factorization of latent semantics in gans. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 1532–1540.

8. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y. (2014). Generative adversarial nets. Adv. Neural Inf. Process. Syst. *27*.

9. Beridze, I., and Butcher, J. (2019). When seeing is no longer believing. Nat. Machine Intelligence *1*, 332–334. https://doi.org/10.1038/s42256-019-0085-5.

10. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., and Ortega-Garcia, J. (2020). Deepfakes and beyond: a survey of face manipulation and fake detection. Inf. Fusion *64*, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014.

11. Bik, E.M., Casadevall, A., and Fang, F.C. (2016). The prevalence of inappropriate image duplication in biomedical research publications. MBio *7*, e00809–e00816. https://doi.org/10.1128/mbio.00809-16.

12. Karras, T., Laine, S., and Aila, T. (2019). A style-based generator architecture for generative adversarial networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4401–4410.

13. Shaham, T.R., Dekel, T., and Michaeli, T. (2019). Singan: learning a generative model from a single natural image. In Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 4570–4580.

14. Shen, Y., Gu, J., Tang, X., and Zhou, B. (2020). Interpreting the latent space of gans for semantic face editing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 9243–9252.

15. Fang, F.C., Steen, R.G., and Casadevall, A. (2012). Misconduct accounts for the majority of retracted scientific publications. Proc. Natl. Acad. Sci. *109*, 17028–17033. https://doi.org/10.1073/pnas.1212247109.

16. Begley, C.G., and Ellis, L.M. (2012). Raise standards for preclinical cancer research. Nature *483*, 531–533. https://doi.org/10.1038/483531a.

17. Verdoliva, L. (2020). Media forensics and deepfakes: an overview. IEEE J. Selected Top. Signal Process. *14*, 910–932. https://doi.org/10.1109/jstsp.2020.3002101.

18. Mirsky, Y., and Lee, W. (2022). The creation and detection of deepfakes: a survey. ACM Comput. Surv. (Csur) *54*, 1–41. https://doi.org/10.1145/3425780.

19. Cozzolino, D., Gragnaniello, D., Poggi, G., and Verdoliva, L. (2021). Towards universal gan image detection. In 2021 International Conference on Visual Communications and Image Processing (VCIP) (IEEE), pp. 1–5.

20. Zhang, X., Karaman, S., and Chang, S.F. (2019). Detecting and simulating artifacts in gan fake images. In 2019 IEEE International Workshop on Information Forensics and Security (WIFS) (IEEE), pp. 1–6.

21. Wang, S.Y., Wang, O., Zhang, R., Owens, A., and Efros, A.A. (2020). Cnn-generated images are surprisingly easy to spot for now. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 8695–8704.

22. Marra, F., Saltori, C., Boato, G., and Verdoliva, L. (2019a). Incremental learning for the detection and classification of gan-generated images. In 2019 IEEE International Workshop on Information Forensics and Security (WIFS) (IEEE), pp. 1–6.

23. Yu, N., Davis, L.S., and Fritz, M. (2019). Attributing fake images to gans: learning and analyzing gan fingerprints. In Proceedings of the IEEE/CVF international conference on computer vision, pp. 7556–7566.

24. Marra, F., Gragnaniello, D., Verdoliva, L., and Poggi, G. (2019b). Do gans leave artificial fingerprints? In 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR) (IEEE), pp. 506–511.

25. Frank, J., Eisenhofer, T., Schönherr, L., Fischer, A., Kolossa, D., and Holz, T. (2020). Leveraging frequency analysis for deep fake image recognition. In International Conference on Machine Learning (PMLR), pp. 3247–3258.

26. Gragnaniello, D., Cozzolino, D., Marra, F., Poggi, G., and Verdoliva, L. (2021). Are gan generated images easy to detect? a critical analysis of the state-of-the-art. In 2021 IEEE International Conference on Multimedia and Expo (ICME) (IEEE), pp. 1–6.

27. Else, H., and Van Noorden, R. (2021). The fight against fake-paper factories that churn out sham science. Nature *591*, 516–519. https://doi.org/10.1038/d41586-021-00733-5.

28. Uhlen, M., Oksvold, P., Fagerberg, L., Lundberg, E., Jonasson, K., Forsberg, M., Zwahlen, M., Kampf, C., Wester, K., Hober, S., et al. (2010). Towards a knowledge-based human protein atlas. Nat. Biotechnol. *28*, 1248–1250. https://doi.org/10.1038/nbt1210-1248.

29. Aksac, A., Demetrick, D.J., Ozyer, T., and Alhajj, R.B. (2019). A dataset for breast cancer histopathological annotation and diagnosis. BMC Res. Notes *12*, 1–3.

About the authors

Jinjin Gu is currently pursuing a PhD degree in engineering and information technology (IT) with the University of Sydney. He received his BEng degree in computer science and engineering from the Chinese University of Hong Kong, Shenzhen, in 2020. His research interests include computer vision, image processing, interpretability of deep-learning algorithms, and machine-learning applications in industry.

Xinlei Wang is currently pursuing a PhD degree in engineering and IT with the University of Sydney. She received her BBA degree in finance in 2018 and her MS degree in data science in 2020 from the Chinese University of Hong Kong, Shenzhen. Currently, she is studying in electrical and information engineering at the University of Sydney, Australia. Her research interests focus on the electricity market mechanism and the Chinese emission trading market.

Chenang Li is currently a senior student in the Chinese University of Hong Kong, Shenzhen.

Dr. Junhua Zhao is an associate professor at CUHK(SZ), the Director of Energy Markets and Finance Lab, Shenzhen Finance Institute, and a scientist at Shenzhen Institute of Artificial Intelligence and Robotics for Society (AIRS). He joined CUHKSZ in 2015. Before joining CUHKSZ, he was a senior lecturer and also acted as the principal research scientist of Center for Intelligent Electricity Networks, the University of Newcastle, Australia. He has 11 years of experience in the power industry in Australia. His research area includes smart grid, electricity market, energy economics, data mining, and AI.

Dr. Weijin Fu is chief physician at the Department of Urology at The First Affliated Hospital of GuangXi Medical University. He graduated from FuDan university and acquired his medical doctor degree in July of 2009. His research area includes the basic and clinical research of genitourinary tumors in urology.

Dr. Gaoqi Liang received her BS degree in automation from North China Electric Power University, China, in 2012. She received her PhD degree in electrical engineering from the University of Newcastle, Australia, in 2017. Currently, she is a research assistant professor at the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, China. Her research interests include smart grid and electricity market and their cyber-physical security as well as machine learning and its cybersecurity in smart grid, etc.

Dr. Jing Qiu is currently a senior lecturer in electrical engineering at the University of Sydney, Australia. He obtained his BEng degree in control engineering from Shandong University, China; his MSc degree in environmental policy and management, majoring in carbon financing in the power sector, from The University of Manchester, UK; and his PhD in electrical engineering from The University of Newcastle, Australia, in 2008, 2010, and 2014, respectively. His areas of interest include power-system operation and planning, energy economics, electricity markets, and risk management.