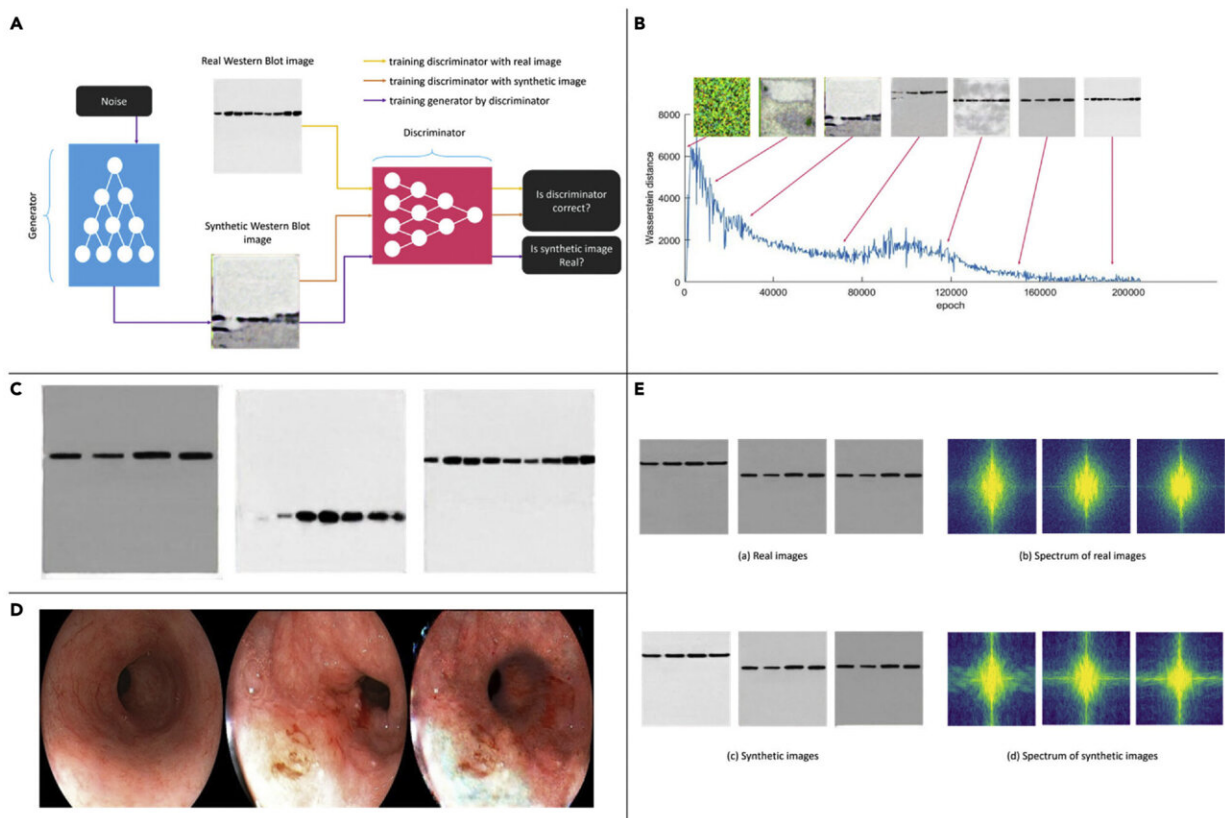# Computer scientists suggest research integrity could be at risk due to AI generated imagery

May 25 2022, by Bob Yirka

Workflow and example usage. (A) The GAN pipeline. (B) The Wasserstein distance reduces when training epochs increase and the generated images at different training epochs. (C) Examples of generated western blot images. (D) Examples of generated esophageal cancer images. (E) The synthetic images from GAN have more high-frequency parts than the real images. Credit: *Patterns* (2022). DOI: 10.1016/j.patter.2022.100509

A small team of researchers at Xiamen University has expressed alarm at the ease with which bad actors can now generate fake AI imagery for use in research projects. They have published an opinion piece outlining their concerns in the journal *Patterns*.

When researchers publish their work in established journals, they often include photographs to show the results of their work. But now the integrity of such photographs is under assault by certain entities who wish to circumvent standard research protocols. Instead of generating photographs of their actual work, they can instead generate them using artificial-intelligence applications. Generating fake [photographs](#) in this way, the researchers suggest, could allow miscreants to publish research papers without doing any real research.

To demonstrate the ease with which fake research [imagery](#) could be generated, the researchers generated some of their own using a [generative adversarial network](#) (GAN), in which two systems, one a generator, the other a discriminator, attempt to outcompete one another in creating a desired image. Prior research has shown that the approach can be used to create images of strikingly realistic human faces. In their work, the researchers generated two types of images. The first kind were of a western blot—an imaging approach used for detecting proteins in a [blood sample](#). The second was of esophageal cancer images. The researchers then presented the images they had created to biomedical specialists—two out of three were unable to distinguish them from the real thing.

The researchers note that it is likely possible to create algorithms that can spot such fakes, but doing so would be stop-gap at best. New technology will likely emerge that could overcome detection software, rendering it useless. The researchers also note that GAN software is

readily available and easy to use, and has therefore likely already been used in fraudulent research papers. They suggest that the solution lies with the organizations that publish research papers. To maintain integrity, publishers must prevent artificially generated images from showing up in work published in their journals.

More information: Liansheng Wang et al, Deepfakes: A new threat to image fabrication in scientific publications? *Patterns* (2022). [DOI: 10.1016/j.patter.2022.100509](#)