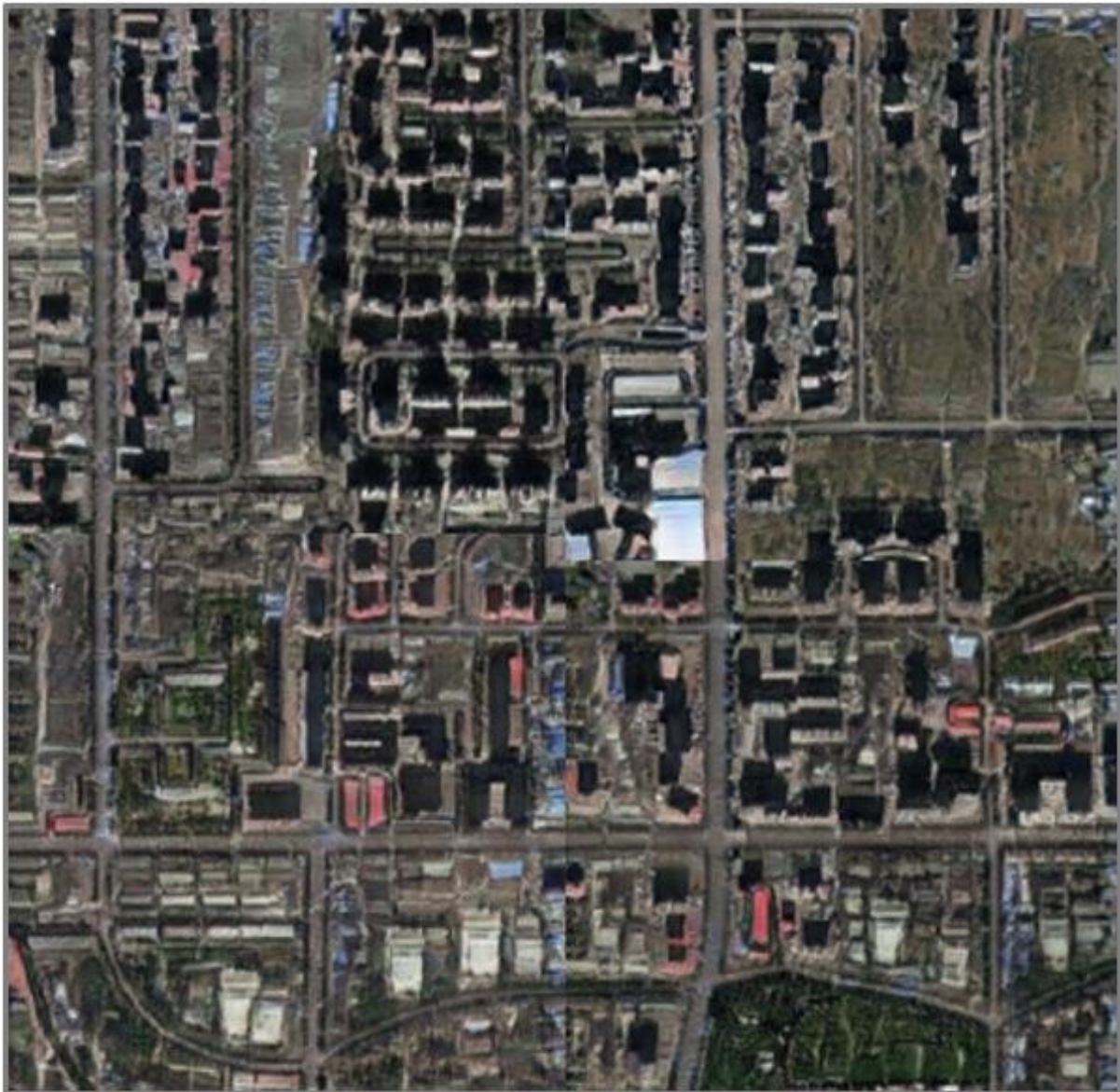# A growing problem of 'deepfake geography': How AI falsifies satellite images

April 21 2021

What may appear to be an image of Tacoma is, in fact, a simulated one, created by transferring visual patterns of Beijing onto a map of a real Tacoma neighborhood. Credit: Zhao et al., Cartography and Geographic Information Science

A fire in Central Park seems to appear as a smoke plume and a line of flames in a satellite image. Colorful lights on Diwali night in India, seen from space, seem to show widespread fireworks activity.

Both images exemplify what a new University of Washington-led study calls "location spoofing." The photos—created by different people, for different purposes—are fake but look like genuine images of real places. And with the more sophisticated AI technologies available today, researchers warn that such "deepfake geography" could become a growing problem.

So, using satellite photos of three cities and drawing upon methods used to manipulate video and audio files, a team of researchers set out to identify new ways of detecting fake satellite photos, warn of the dangers of falsified geospatial data and call for a system of geographic fact-checking.

"This isn't just Photoshopping things. It's making data look uncannily realistic," said Bo Zhao, assistant professor of geography at the UW and lead author of the study, which published April 21 in the journal *Cartography and Geographic Information Science*. "The techniques are already there. We're just trying to expose the possibility of using the same techniques, and of the need to develop a coping strategy for it."

As Zhao and his co-authors point out, fake locations and other inaccuracies have been part of mapmaking since ancient times. That's

due in part to the very nature of translating real-life locations to map form, as no map can capture a place exactly as it is. But some inaccuracies in maps are spoofs created by the mapmakers. The term "paper towns" describes discreetly placed fake cities, mountains, rivers or other features on a map to prevent copyright infringement. On the more lighthearted end of the spectrum, an official Michigan Department of Transportation highway map in the 1970s included the fictional cities of "Beatosu and "Goblu," a play on "Beat OSU" and "Go Blue," because the then-head of the department wanted to give a shoutout to his alma mater while protecting the copyright of the map.

These are maps and satellite images, real and fake, of one Tacoma neighborhood. The top left shows an image from mapping software, and the top right is an actual satellite image of the neighborhood. The bottom two panels are simulated satellite images of the neighborhood, generated from geospatial data of Seattle (lower left) and Beijing (lower right). Credit: Zhao et al., 2021, Cartography and Geographic Information Science

But with the prevalence of geographic information systems, Google Earth and other satellite imaging systems, location spoofing involves far greater sophistication, researchers say, and carries with it more risks. In 2019, the director of the National Geospatial Intelligence Agency, the organization charged with supplying maps and analyzing satellite images for the U.S. Department of Defense, implied that AI-manipulated satellite images can be a severe national security threat.

To study how satellite images can be faked, Zhao and his team turned to an AI framework that has been used in manipulating other types of digital files. When applied to the field of mapping, the algorithm essentially learns the characteristics of satellite images from an urban area, then generates a deepfake image by feeding the characteristics of the learned satellite image characteristics onto a different base map—similar to how popular image filters can map the features of a human face onto a cat.

Next, the researchers combined maps and satellite images from three cities—Tacoma, Seattle and Beijing—to compare features and create new images of one city, drawn from the characteristics of the other two. They designated Tacoma their "base map" city and then explored how geographic features and urban structures of Seattle (similar in topography and land use) and Beijing (different in both) could be incorporated to produce deepfake images of Tacoma.

In the example below, a Tacoma neighborhood is shown in mapping software (top left) and in a satellite image (top right). The subsequent deep fake satellite images of the same neighborhood reflect the visual patterns of Seattle and Beijing. Low-rise buildings and greenery mark the "Seattle-ized" version of Tacoma on the bottom left, while Beijing's taller buildings, which AI matched to the building structures in the Tacoma image, cast shadows—hence the dark appearance of the structures in the image on the bottom right. Yet in both, the road

networks and building locations are similar.

The untrained eye may have difficulty detecting the differences between real and fake, the researchers point out. A casual viewer might attribute the colors and shadows simply to poor image quality. To try to identify a "fake," researchers homed in on more technical aspects of image processing, such as color histograms and frequency and spatial domains.
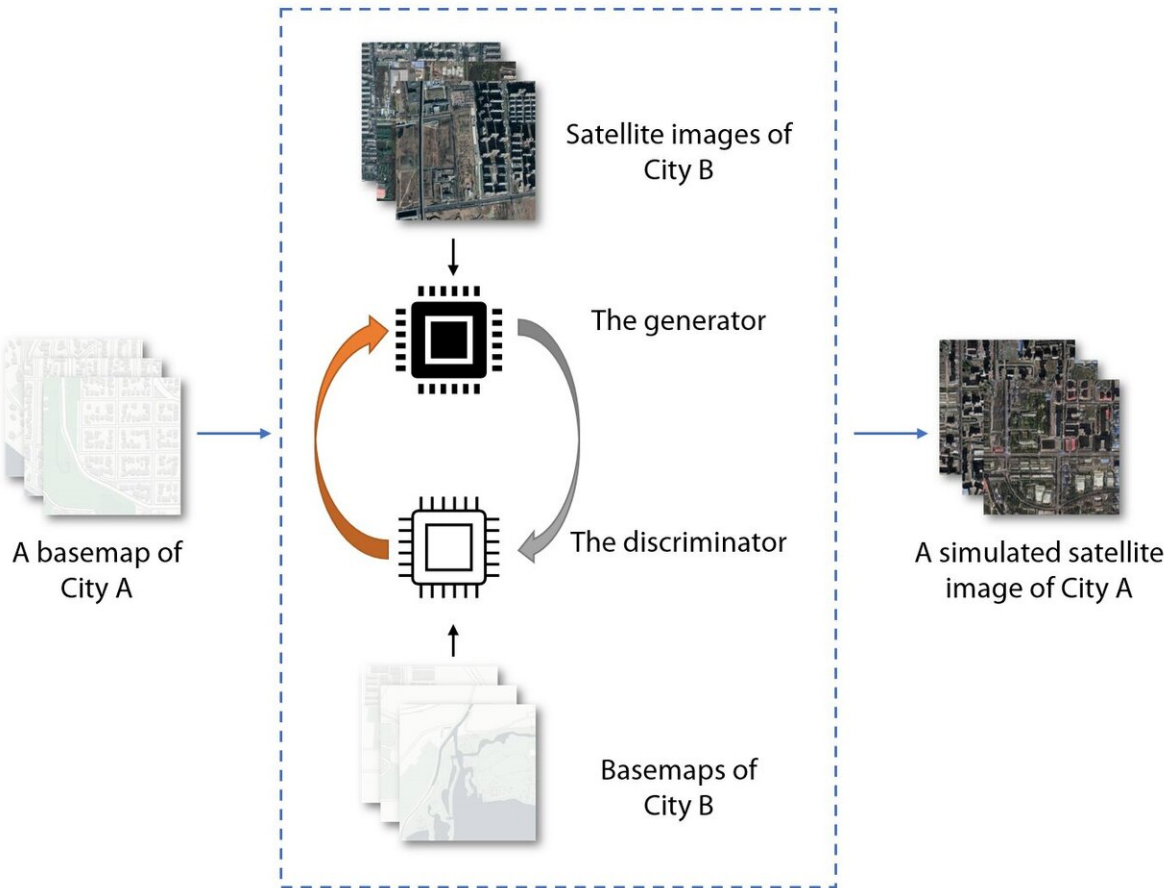
This simplified illustration shows how a simulated satellite image (right) can be generated by putting a base map (City A) into a deepfake satellite image model. This model is created by distinguishing a group of base map and satellite image pairs from a second city (City B). Credit: Zhao et al., 2021, Cartography and Geographic Information Science

Some simulated satellite imagery can serve a purpose, Zhao said, especially when representing geographic areas over periods of time to, say, understand urban sprawl or climate change. There may be a location for which there are no images for a certain period of time in the past, or in forecasting the future, so creating new images based on existing ones—and clearly identifying them as simulations—could fill in the gaps and help provide perspective.

The study's goal was not to show that geospatial data can be falsified, Zhao said. Rather, the authors hope to learn how to detect fake images so that geographers can begin to develop the data literacy tools, similar to today's fact-checking services, for public benefit.

"As technology continues to evolve, this study aims to encourage more holistic understanding of geographic data and information, so that we can demystify the question of absolute reliability of satellite images or other geospatial data," Zhao said. "We also want to develop more future-oriented thinking in order to take countermeasures such as fact-checking when necessary," he said.

Co-authors on the study were Yifan Sun, a graduate student in the UW Department of Geography; Shaozeng Zhang and Chunxue Xu of Oregon State University; and Chengbin Deng of Binghamton University.

Provided by University of Washington