

Deep Fake Geography?

Towards GIScience in the Post-truth Era

Bo Zhao, Associate Professor

zhaobo@uw.edu

Department of Geography

University of Washington Seattle

Increasing Media Attention to Deepfake Geography



American Association of Geographers @theAAG · May 7
Can We Stop "Deepfake Geography"? A team of @UW geographers led by Bo Zhao is using an AI to detect fake satellite imagery



Can We Spot Deepfaked Satellite Imagery?
To highlight the problem of "deepfake geography," Washington researchers built an AI tool to detect fake satellite imagery.
freethink.com



Canadian Geographers @CanGeographers · Apr 22
Growing Problem Of 'Deep Fake Geography': How AI Falsifies Satellite Images



Growing Problem Of 'Deep Fake Geography'
A fire in Central Park seems to appear as a satellite image. Colorful lights on the ground appear as flames in a satellite image. Colorful lights on the ground appear as flames in a satellite image.
eurasiareview.com



The American Geographical Society @AmericanGeo · Jun 2
Seattle or Beijing? Learn more about how people are using AI to create deepfake maps:



Deepfake Maps Could Really Mess With Your Sense of the World
Researchers applied AI techniques to make portions of Seattle look more like Beijing. Such imagery could mislead governments or spread misinformation.
wired.com

Zhao, B., Zhang, S., Xu, C., Sun, Y., & Deng, C. (2021). **Deep fake geography? When geospatial data encounter Artificial Intelligence.** *Cartography and Geographic Information Science*, 48(4), 338-352.

Deepfake Geography as a Pressing National Security Concern



“They’re already doing it right now, using GANs—which are generative adversarial networks—to manipulate scenes and pixels to create things for nefarious reasons.”



— Todd Myers, CIO at the National Geospatial-Intelligence Agency.

SCIENCE & TECH The Newest AI-Enabled Weapon: ‘Deep-Faking’ Photos of the Earth

Step 1: Use AI to make undetectable changes to outdoor photos. Step 2: release them into the open-source world and enjoy the chaos.



BY PATRICK TUCKER
TECHNOLOGY EDITOR

MARCH 31, 2019



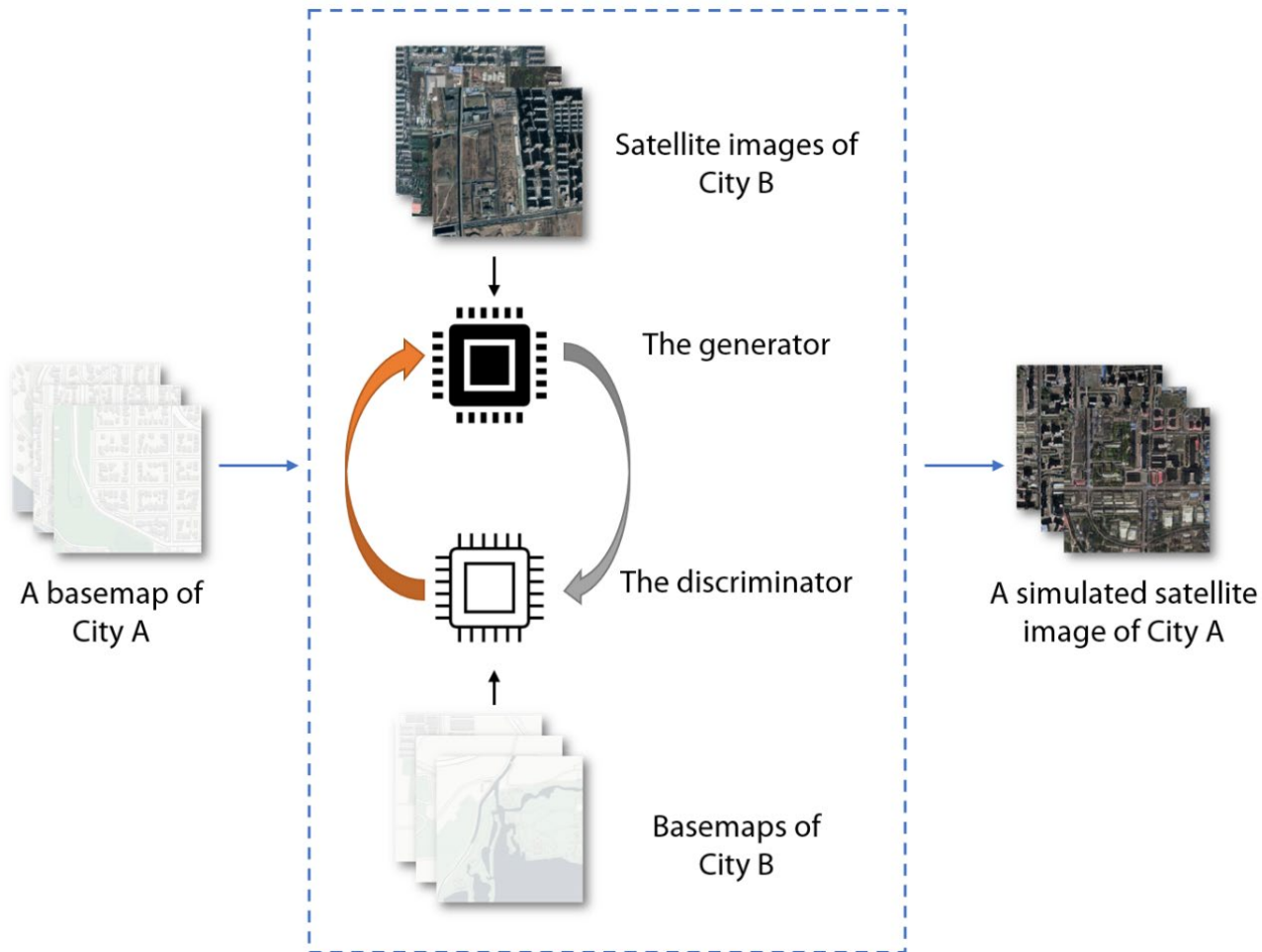
Worries about deep fakes — machine-manipulated videos of celebrities and world leaders purportedly saying or doing things that they really didn’t — are quaint compared to a new threat: doctored images of the Earth itself.

China is the acknowledged leader in using an emerging technique called generative adversarial networks to trick computers into seeing objects in landscapes or in satellite images that aren’t there, says Todd Myers, automation lead for the CIO-Technology Directorate at the National Geospatial-Intelligence Agency.

“The Chinese are well ahead of us. This is not classified info,” Myers said Thursday at the second annual *Genius Machines* summit, hosted by Defense One and Nextgov. “The Chinese have already designed; they’re already doing it right now, using GANs—which are generative adversarial networks—to manipulate scenes and pixels to create things for nefarious reasons.”

<https://www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/>

Satellite Imagery Synthetization



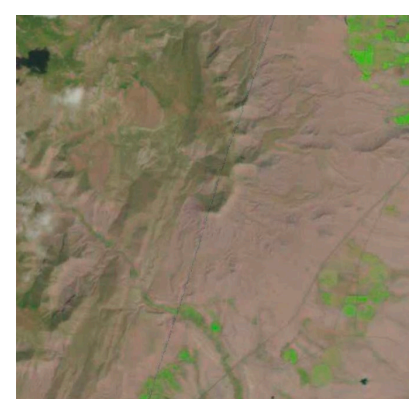
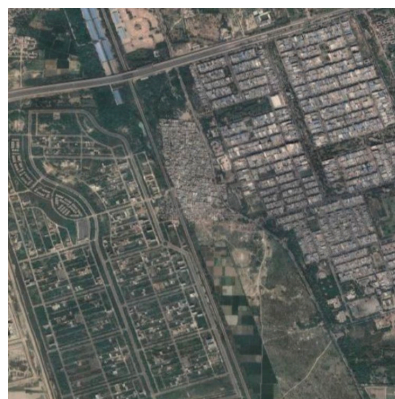
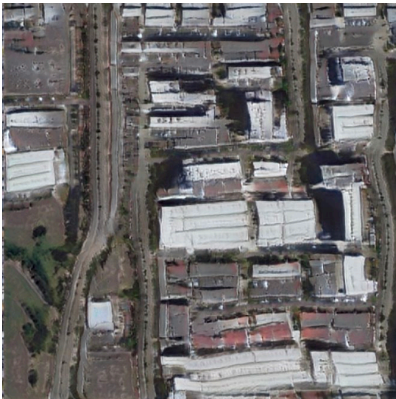
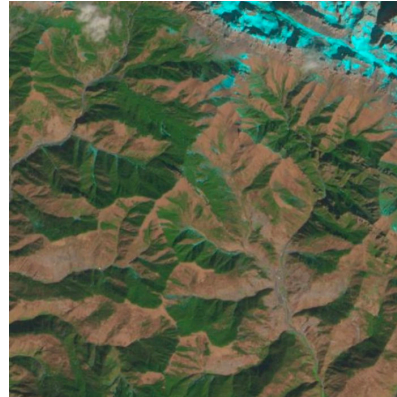
This simplified illustration shows how a synthetic satellite image (right) can be simulated by satellite image pairs from a second city (City B).

Synthetic Satellite Images



Figure 4. Fake satellite images of a neighborhood in Tacoma with landscape features of other cities. (a) The original CartoDB basemap tile; (b) the corresponding satellite image tile. The fake satellite image in the visual patterns of (c) Seattle and (d) Beijing.

Satellite Imagery Synthetization (Cont'd)



Google Earth Level-18 (0.5m)

Google Earth Level-16 (2.4m)

Sentinel-2 (10m)

Landsat-8 (30m)

Deepfake Detection

- Scholars found that GAN-generated fake images were different from authentic ones in multiple visual features such as color, texture and details, and in frequency domain features such as a certain type of periodic replications (Galbally & Marcel, 2014; Wang et al., 2020; X. Zhang et al., 2019).
- 26 selected features of three categories.

Table 1. Features of authentic and fake satellite images.

Code	Feature description
Spatial	
CFI	Image Colorfulness Index: A larger value indicates a more colorful image
BIQ	Brenne Image Quality Index: A larger value indicates a clearer image
TIQ	Tenengrad Image Quality Index: A larger value indicates a clearer image
LIQ	Laplacian Image Quality Index: A larger value indicates a clearer image
ASM	Angular Second Moment of GLCM: A larger value indicates a more uniform and regularly changing texture pattern
CON	Contrast of GLCM: The greater the CON, the deeper the grooves of the texture, and the clearer the visual effect
ENT	Entropy of GLCM: The more complex and uneven the texture in the image, the greater the ENT value
IDM	Inverse Different Moment of GLCM: The larger the IDM, the smaller the change between areas of the image texture, or the local pattern is more uniform
Frequency	
FASM	ASM at Frequency Domain: Similar to ASM
FCON	CON at Frequency Domain: Similar to CON
FENT	ENT at Frequency Domain: Similar to ENT
FIDM	IDM at Frequency Domain: Similar to IDM
Histogram	
MEAN	Mean of GLH, The larger the value the brighter the image
STD	Standard Deviation of GLH, the larger the value less concentrated the GLH
SKEW	Skewness of GLH, the larger the value more skewed the GLH
KURT	Kurtosis of GLH, the larger the value the steeper the GLH
GET	Entropy of GLH, the larger the value, the less even the GLH
CM1_R/G/B	First Order Color Moment of Red (Green/Blue): mean of color histogram
CM2_R/G/B	Second Order Color Moment of Red (Green/Blue): variance of color histogram
CM3_R/G/B	Third Order Color Moment of Red (Green/Blue): skewness of color histogram

GLCM means gray level concurrence matrix; GLH refers to gray level histogram.

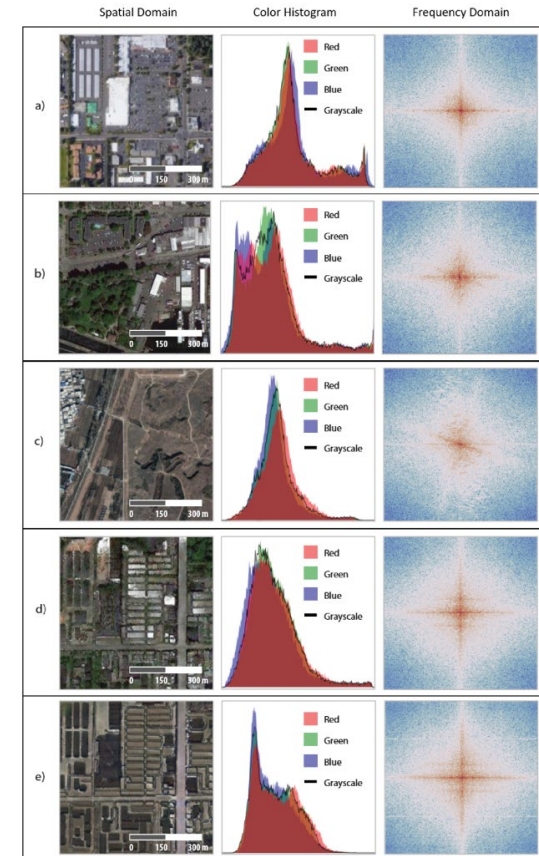


Figure 6. The comparison between authentic and fake satellite image records with respect to their spatial domains, color histograms, and frequency domains. Three authentic satellite image records showing (a) an area in Tacoma, (b) an area in Seattle, and (c) another area in Beijing, respectively. Two fake satellite image records of Tacoma in (d) a transferred visual pattern of Seattle and in (e) another transferred visual pattern of Beijing, respectively.

Deepfake Detection

Does the workflow work well?

Table 3. Performance of different fake satellite images detection models.

Model	F1 score	Precision	Recall
Spatial	0.9399	0.9316	0.9483
Histogram	0.8795	0.8196	0.9484
Frequency	0.8324	0.7283	0.9697
Spatial + Histogram	0.9484	0.9472	0.9516
Spatial + Frequency	0.9387	0.9308	0.9468
Histogram + Frequency	0.8879	0.8347	0.9481
Spatial + Histogram + Frequency	0.9530	0.9482	0.9579

The proposed approach can effectively detect CycleGAN-generated fake satellite images.

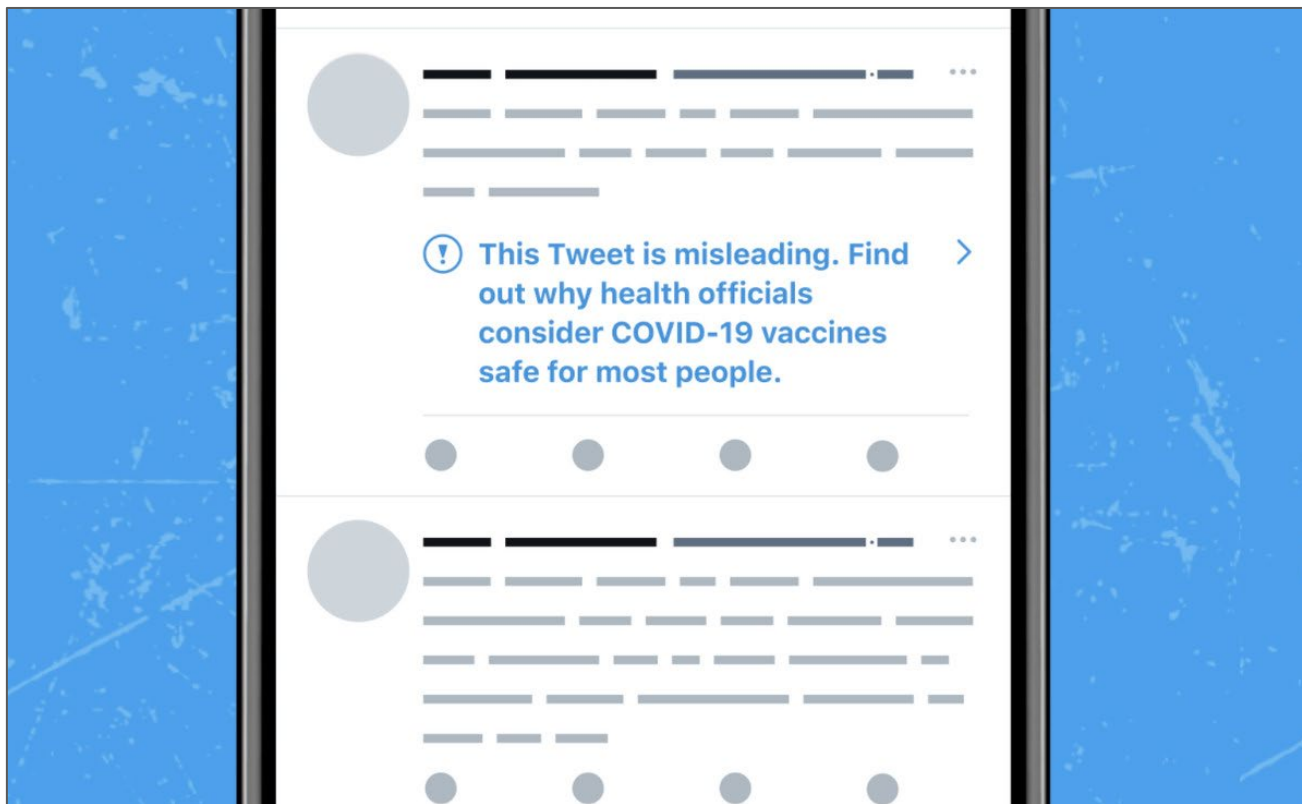
Table 2. The independent *t*-test between features of authentic and fake satellite images.

Feature	Mean Fake	Mean Authentic	Diff.
<i>Spatial</i>			
CFI	12.1343	20.6602	-8.5259***
BIQ	496.2755	462.3757	33.8998**
TIQ	19284.5431	19472.7016	-188.1585
LIQ	4897.4112	4937.9481	-40.5369
ASM	0.0089	0.0258	-0.0169***
CON	373.3451	364.6969	8.6482
ENT	7.7601	7.5506	0.2096**
IDM	0.1767	0.2764	-0.0997***
<i>Histogram</i>			
MEAN	79.0960	91.1394	-12.0434***
STD	28.8618	28.5261	0.3357
SKEW	0.9246	0.7465	0.1781***
KURT	5.9737	3.5810	2.3927***
GET	6.2897	6.1589	0.1308**
CM1_R	80.3252	89.2334	-8.9084***
CM2_R	30.4465	31.710	-1.2675***
CM3_R	25.1773	13.3325	11.8447***
CM1_G	80.7005	92.9016	-12.2011***
CM2_G	28.9633	28.5668	0.3965**
CM3_G	26.4078	15.7421	10.6658***
CM1_B	75.4713	88.3756	-12.9042***
CM2_B	29.1654	29.6676	-0.5022
CM3_B	28.6201	23.1306	5.4895***
<i>Frequency</i>			
FASM	0.0007	0.0047	-0.0041***
FCON	245.7877	251.9979	-6.2102***
FENT	8.2935	8.2288	0.0648***
FIDM	0.0956	0.0903	0.0054***

Mean Fake (Authentic) refers to the mean value of different features of all fake (authentic) samples, Diff. indicates difference between the mean value of features for all authentic samples and all fake samples; *, $p < 0.05$; **, $p < 0.01$; ***, $p < 0.001$.

Next Steps

1. A NFT (Non-fungible-Token) based digital licensing system
2. Deepfake detection API for satellite images on social media platform



Next Steps

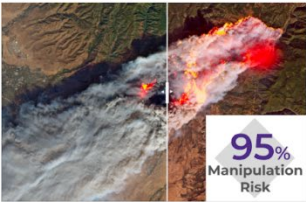
3. A Public-facing Platform for Fact-checking Satellite Imagery

RSFactChecker.org A public-facing platform to fact-check satellite imagery

HOME | REPORT | EDUCATION

2018 Camp Fire, California

A satellite images is processed and posted by Pixyz, Krikree on Medium. It's used as evidence to indicate the seriousness of California Camp Fire 2018. >>> Original Article



95% Manipulation Risk

Powered by Sentinel-2 Model - Performance is indicated on RSFactChecker.org database

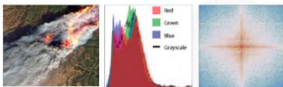
Local feature mismatch **detected**
Global color enhancement **detected**
Overlay modification **un-detected**
Texture inconsistency **un-detected**

Collective Trustworthiness Scores

Extremely trustworthy	5%
Trustworthy	12%
Not sure	35%
Untrustworthy	30%
Extremely untrustworthy	18%

Post Your Opinion

Imagery Characteristics



Spatial **Histogram** **Frequency**

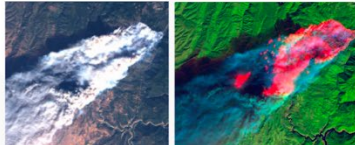
CP: 1.14 (15-25)
BIC: -99 (142-460)
IDM: 0.18 (0.24-0.36)

Skew: 0.02 (0.65-0.85)
CM: 81.83 (79-90)
CET: 6.29 (6.1-6.3)

FOON: 245.8 (230-270)
FOH: 6.17 (5.9-6.3)
FIDM: 0.1 (0.08-0.12)

Claimed Data Source: Landsat 8
Identified Data Source: Landsat 8
Claimed Place: Butte County, California
Identified Place: (38.158, -121.8) - (38.228, -121.549)

Cross Validation



MODIS **Short-wave infrared Landsat 8**

The open source cross validation dataset is collected from official databases

Extremely Trustworthy

Jane Doe GIS Analyst
★★★★★

great visualization strong evidence

Reviewed in Seattle on October 21, 2020

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae.

96 people found this helpful

Search public opinions

Sort By: Top reviews
Filter: All reviewers Not sure only

Extremely Untrustworthy

John Doe Remote Sensing Expert
★☆☆☆☆

manipulation adverse impact

Reviewed in New York on August 12, 2019

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae.


147 people found this helpful

Nancy Doe
★★★★★

strong evidence manipulation

Reviewed in San Francisco on January 5, 2020

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis in aliquet justo. Nulla varius vitae.



58 people found this helpful

Helpful Report abuse

GIScience in the Post-truth Era



AMERICAN ASSOCIATION
of GEOGRAPHERS
ANNUAL MEETING

GIScience in the Post-Truth Era

Organizers: Bo Zhao (UW); Ling Bian (SUNY at Buffalo)

- Rethinking of ground truth, spatial data quality, and uncertainty under the context of post-truth.
- Fake location detection, proof of location and/or other countermeasures using innovative GIS methods, including, but not limited to, spatial statistics, spatial network analysis, time geography, spatial-temporal analysis, natural language processing, GeoAI, and etc.
- The spatial dissemination of fake geographic information, and in the context of post-truth.
- Critique of fake locational information (e.g., check-in, geo-tag, location-based review, etc.) and its impacts on geo-privacy, policing, surveillance, and digital governance.
- Case studies of geospatial information falsification (e.g., location spoofing, check-in hacking, satellite image forgery, etc.) and its relevance in public health, national security, and everyday life.

Zhang, S., Zhao, B., Tian, Y., & Chen, S. (2021). Stand with# StandingRock: Envisioning an epistemological shift in understanding geospatial big data in the “post-truth” era. *Annals of the American Association of Geographers*, 111(4), 1025-1045.

Thank you, any questions and comments?

I would like to express my gratitude to my co-authors of this paper. They are Yifan Sun (University of Washington), Chunxue Xu (ESRI), Shaozeng Zhang (Oregon State University), Mia Bennett (University of Washington), and Chengbin Deng (University of Oklahoma).



Zhao, B., S. Zhang, C. Xu, Y. Sun, and C. Deng. (2021) Deep fake geography? When geospatial data encounter artificial intelligence. *Cartography and Geographic Information Science*. 48(4), 338-352.