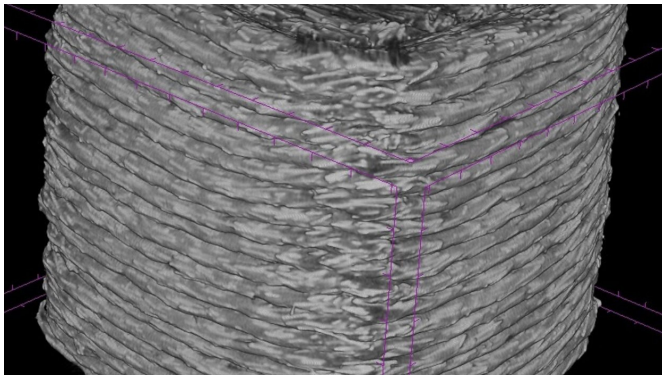
Reverse engineering of 3-D-printed parts by machine learning reveals security vulnerabilities

2 July 2020



A three-dimensional view of a reconstructed CT scan model of a 3D printed composite part showing overall dimensions and geometry. Credit: NYU Tandon School of Engineering

Over the past 30 years, the use of glass and carbon-fiber reinforced composites in aerospace and other high-performance applications has soared along with the broad industrial adoption of composite materials.

Key to the strength and versatility of these hybrid, layered materials in high-performance applications is the orientation of fibers in each layer. Recent innovations in additive manufacturing (3-D printing) have made it possible to finetune this factor, thanks to the ability to include within the CAD file discrete printer-head orientation instructions for each layer of the component being printed, thereby optimizing strength, flexibility, and durability for specific uses of the part. These 3-D-printing toolpaths (a series of coordinated locations a tool will follow) in CAD file instructions are therefore a valuable trade secret for the manufacturers.

However, a team of researchers from NYU Tandon School of Engineering led by Nikhil Gupta, a professor in the Department of Mechanical and Aerospace Engineering showed that these toolpaths are also easy to reproduce—and therefore steal—with machine learning (ML) tools applied to the microstructures of the part obtained by a CT scan.

Their research, "Reverse engineering of additive manufactured composite part by toolpath reconstruction using imaging and machine learning," published in *Composites Science and Technology*, demonstrates this method of reverse engineering of a 3-D-printed glass-fiber reinforced polymer filament that, when 3-D-printed, has a dimensional accuracy within one-third of 1% of the original part.

The investigators, including NYU Tandon graduate students Kaushik Yanamandra, Guan Lin Chen, Xianbo Xu, and Gary Mac show that the printing direction used during the 3-D-printing process can be captured from the printed part's fiber orientation via micro-CT scan image. However, since the fiber direction is difficult to discern with the naked eye, the team used ML algorithms trained over thousands of micro CT scan images to predict the fiber orientation on any fiber-reinforced 3-D-printed model. The team validated its ML algorithm results on cylinder- and square-shaped models finding less than 0.5° error.

Gupta said the study raises concerns for the security of intellectual property in 3-D-printed composite parts, where significant effort is invested in development but modern ML methods can make it easy to replicate them at low cost and in a short time.

"Machine learning methods are being used in the design of complex parts but, as the study shows, they can be a double-edged sword, making reverse

engineering also easier," said Gupta. "The security concerns should also be a consideration during the design process and unclonable toolpaths should be developed in future research."

More information: Kaushik Yanamandra et al. Reverse engineering of additive manufactured composite part by toolpath reconstruction using imaging and machine learning, *Composites Science and Technology* (2020). DOI: 10.1016/j.compscitech.2020.108318

Provided by NYU Tandon School of Engineering