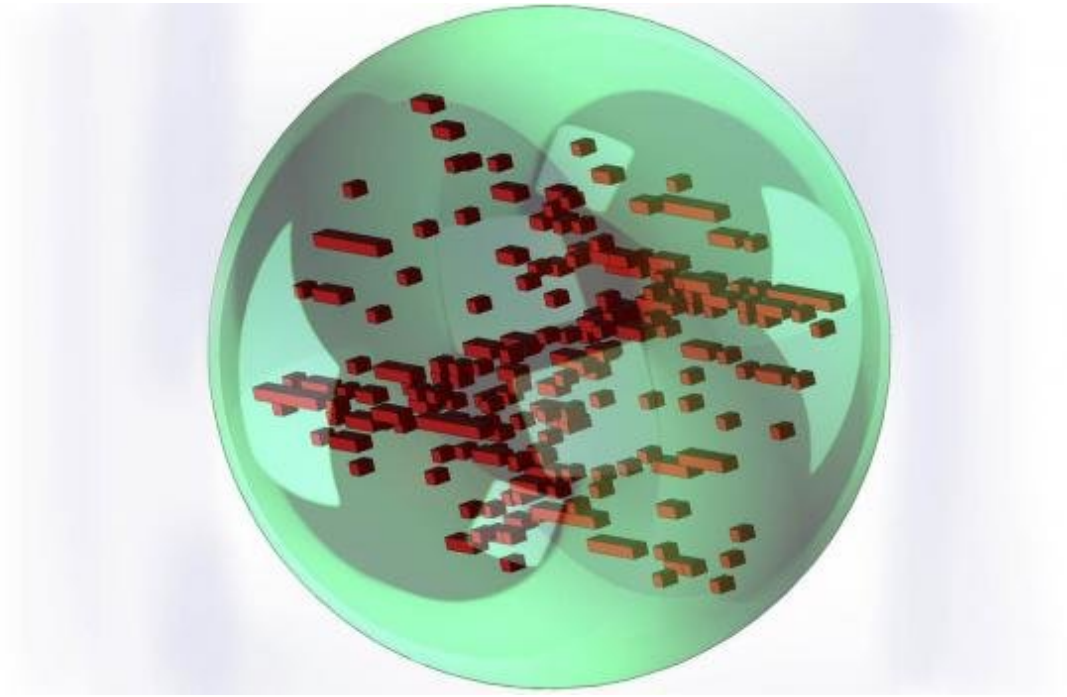
Researchers turn tracking codes into unclonable 'clouds' to authenticate genuine 3-D printed parts

August 20 2018



Nikhil Gupta, an associate professor of mechanical engineering, and collaborators exploited the layer-by-layer AM printing process to “explode” QR codes within computer-assisted design (CAD) files so that they present several false faces — dummy QR tags — to a micro-CT scanner or other scanning device. Credit: NYU Tandon School of Engineering

The worldwide market for 3-D-printed parts is a $5 billion business with

a global supply chain involving the internet, email, and the cloud—creating a number of opportunities for counterfeiting and intellectual property theft. Flawed parts printed from stolen design files could produce dire results: experts predict that by 2021, 75 percent of new commercial and military aircraft will fly with 3-D-printed engine, airframe, and other components, and the use of AM in the production of medical implants will grow by 20 percent per year over the next decade.

A team at NYU Tandon School of Engineering has found a way to prove the provenance of a part by employing QR (Quick Response) codes in an innovative way for unique device identification. In the latest issue of *Advanced Engineering Materials*, the researchers describe a method for converting QR codes, bar codes, and other passive tags into three-dimensional features hidden in such a way that they neither compromise the part's integrity nor announce themselves to counterfeiters who have the means to reverse engineer the part.

Noted materials researcher Nikhil Gupta, an associate professor of mechanical engineering at NYU Tandon; Fei Chen, a doctoral student under Gupta; and joint NYU Tandon and NYU Abu Dhabi researchers Nektarios Tsoutsos, Michail Maniatakos and Khaled Shahin, detail how they exploited the layer-by-layer AM printing process to turn QR codes into a game of 3-D chess. Gupta's team developed a scheme that "explodes" a QR code within a computer-assisted design (CAD) file so that it presents several false faces—dummy QR tags—to a micro-CT scanner or other scanning device. Only a trusted printer or end user would know the correct head-on orientation for the scanner to capture the legitimate QR code image.

"By converting a relatively simple two-dimensional tag into a complex 3-D feature comprising hundreds of tiny elements dispersed within the printed component, we are able to create many 'false faces,' which lets us hide the correct QR code from anyone who doesn't know where to look,"

Gupta said.

The team tested different configurations—from distributing a code across just three layers of the object, to fragmenting the code into up to 500 tiny elements—on thermoplastics, photopolymers, and metal alloys, with several printing technologies commonly employed in the industry.

Chen, the study's lead author, said that after embedding QR codes in such simple objects as cubes, bars, and spheres, the team stress-tested the parts, finding that the embedded features had negligible impact on structural integrity.

"To create typical QR code contrasts that are readable to a scanner you have to embed the equivalent of empty spaces," she explained. "But by dispersing these tiny flaws over many layers we were able to keep the part's strength well within acceptable limits."

Tsoutsos and Maniatakos explored threat vectors to determine which AM sectors are best served by this security technology, a step that Gupta said was crucial in the research.

"You need to be cost efficient and match the solution to the threat level," he explained. "Our innovation is particularly useful for sophisticated, high-risk sectors such as biomedical and aerospace, in which the quality of even the smallest part is critical."

A 2016 article by Gupta and a team of researchers that included Maniatakos and Tsoutsos in *JOM*, *The Journal of the Minerals, Metals & Materials Society* explored how flaws caused by printing orientation and insertion of fine defects could be foci for AM cyber-attacks. The paper was the most-read engineering research that year among Springer's over 245 engineering journals. In a paper last year in *Materials and Design*, Gupta detailed methods of inserting undetectable flaws within CAD files

so that only a trusted printer could correctly produce the parts.

More information: Fei Chen et al. Embedding Tracking Codes in Additive Manufactured Parts for Product Authentication, *Advanced Engineering Materials* (2018). DOI: 10.1002/adem.201800495

Provided by NYU Tandon School of Engineering