Anti-counterfeiting technology performs reliable AI authentication under extreme conditions

22 December 2020

DeepKey—reliable AI authentication under extreme conditions. Credit: National University of Singapore

Researchers from the National University of Singapore (NUS) have invented a new method of anti-counterfeiting called DeepKey. This security innovation uses two dimensional (2-D)-material tags and artificial intelligence (AI)-enabled authentication software.

Compared to conventional anti-counterfeiting technologies, DeepKey works faster, achieves highly accurate results, and uses durable identification tags that are not easily damaged by environmental conditions such as extreme temperatures, chemical spills, UV exposure, and moisture. This new authentication technology can be applied to different high-value products, ranging from drugs, jewelry, and electronics. For example, DeepKey is suitable for tagging COVID-19 vaccines to enable rapid and reliable authentication, as some of such vaccines need to be stored at the ultra-cold temperature of −70°C.

Led by Asst Prof Chen Po-Yen and Asst Prof Wang Xiaonan from the Department of Chemical

and Biomolecular Engineering at NUS Faculty of Engineering, the team's 2-D-material secure tags exhibit Physically Unclonable Function patterns (PUF patterns), which are randomly generated by systematically crumpling the 2-D-material thin films. The complex 2-D-material patterns with multi-scale features can then be classified and validated by a well-trained deep learning model, enabling reliable (100 percent accurate) authentication in less than 3.5 minutes.

Current anti-counterfeiting technologies using PUF patterns normally face several bottlenecks, including complicated manufacturing, specialized and tedious readout process, long authentication time, insufficient environmental stability, as well as being costly to make.

"With this research, we have tackled several bottlenecks that other techniques encounter," said Asst Prof Wang. "Our 2-D-material PUF tags are environmentally stable, easy to read, simple and cheap to make. In particular, the adoption of deep learning accelerated the overall authentication significantly, pushing our invention one step further to practical application."

The researchers published their results in scientific journal *Matter* on 2 December 2020. This study was conducted in collaboration with researchers from Anhui University of Technology and Nanyang Technological University.

A stable, simple and scalable process to create PUF tags

Remarkably, the researchers do not need any special equipment to create the secure tags. They can simply be made with a balloon, a bottle of 2-D-material dispersion, and a brush.

"First, we inflate the balloon and brush over its surface with viscous 2-D-material ink. After air drying overnight, we deflate the balloon. Because of the interfacial mechanical mismatch between the 2-D-material and latex substrate, large-area, crumpled PUF patterns are generated during the contraction. These PUF patterns can be cut to the required size afterwards, and normally, hundreds of them can be made at one time," said Dr. Jing Lin, a member of the research team.

Next, the researchers take a quick image of the PUF tag with an electron microscope, which is then synced to their innovative software to go through the deep learning "classification and validation" process. "The whole process takes less than 3.5 minutes, most of which is spent waiting for the readout from the electron microscope. The authentication itself is very fast, in less than 20 seconds," explained Dr. Jing.

Fast authentication using AI deep learning algorithms

All PUF key-based technologies have ultra-high encoding capacities because of the huge numbers of distinct patterns that can be theoretically produced. However, the high encoding capacity also leads to long authentication time, as the "search and compare" pattern validation has to be conducted within a huge database. This trade-off between high encoding capacity and long authentication time often restricts such PUF-based anti-counterfeiting tags from practical applications.

"With our new technology, we are breaking this long-lasting trade-off between high encoding capacity and long authentication time by using classifiable 2-D-material PUF tags and deep learning algorithms," said Asst Prof Wang.

First, the researchers used various 2-D materials to fabricate PUF tags with AI recognizable features. Second, they trained a deep learning model to conduct a two-step authentication mechanism. "We used the deep learning model to pre-categorize the PUF patterns into subgroups, and so the search-and-compare algorithm is conducted in a much smaller database, which shortens the overall authentication time," Asst Prof Wang explained.

Currently, the only available technologies similar to this NUS innovation, are polymer wrinkle-based tags. Wrinkled polymer tags are authenticated based on the surface patterns just like the novel 2-D-material tags. However, their authentication presently requires one-by-one feature extraction and matching, which is slow and shows only 80 percent reliability. The NUS team's authentication is boosted by deep learning, and is therefore much faster, and reaches nearly 100 percent validation precision.

In addition, compared to the wet chemistry preparation of polymer wrinkle-based tags, which involves the use of harmful organic chemicals and UV light, the NUS researchers' fabrication technique is significantly faster and safer.

Next steps

The NUS team has filed a patent for their invention and is now planning to push this technology one step further. "We are searching for better, faster, and more robust readout and authentication approaches for our PUF tags," said Asst Prof Wang.

The team has already begun to conduct research on other readout techniques to further shorten the processing time. "In addition, such naturally encoded information by the PUF tags could be further secured by being kept on blockchain, so that the whole supply chain and quality control can be transparently tracked," Asst Prof Wang added.

Provided by National University of Singapore