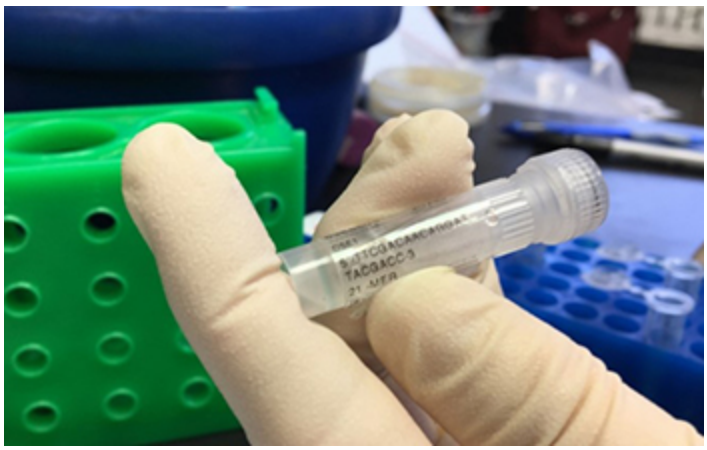
Research News

Genetic barcodes can ensure authentic DNA fingerprints

Researchers propose a way of ensuring that genetic samples arrive at the lab unaltered



Genetic 'barcodes' added to DNA samples could ensure they arrived at a lab unaltered.

Credit and Larger Version (/discoveries/disc_images.jsp?cntn_id=300663&org=NSF)

May 29, 2020

Engineers at Duke University (/cgi-bin/good-bye?https://pratt.duke.edu/about/news/genetic-barcodes) and New York University have demonstrated a method for ensuring that an increasingly popular method of genetic identification called DNA fingerprinting remains secure against inadvertent mistakes or malicious attacks in the field.

The National Science Foundation <https://www.nsf.gov/awardsearch/showAward?AWD_ID=1833622&HistoricalAwards=false> -funded method relies on introducing genetic "barcodes" to DNA samples as they are collected and then securely sending information crucial to identifying these barcodes to technicians in the laboratory. The system shows one way to guarantee that a sample taken in the field, transported to a lab, and processed for genetic identification, is genuine.

The results appear in the journal *IEEE Transactions on Information Forensics and Security* (/cgi-bin/good-bye?https://ieeexplore.ieee.org/document/9093855).

"If you think about conventional encryption techniques, like security for a smartphone, there's usually a passcode that only one person knows," said Mohamed Ibrahim, a system-on-chip design engineer at Intel and previously at Duke. "Our idea is to inject non-harmful material into genetic samples immediately when they

are collected in the field that act as a similar password. This would ensure that the samples are authentic when they reach the processing stage."

DNA fingerprinting is a method of identifying a specific person, organism or disease based on only a small amount of genetic material. As the popularity of DNA fingerprinting and the polymerase chain reaction technology underlying it increases, multiple companies are in a race to simplify the process and create cheaper solutions.

As these devices become smaller, more complex and more automated, they may create more vulnerabilities for the process to be attacked. Recent studies suggest that these vulnerabilities raise unprecedented security concerns, creating a whole new category of potential weaknesses that has been dubbed "cyberbiosecurity threats."

"Researchers have identified a diverse array of cyberbiosecurity threats over the past few years," said Krishnendu Chakrabarty of Duke. "Our main goal is to become a part of the community trying to address these threats by focusing on one of the most vulnerable time periods, which is before a sample even gets to the lab."

Added Sandip Kundu, a program officer in NSF's Division of Computer and Network Systems, "These investigators have demonstrated that even biological samples are not immune to security threats from mishandling and tampering. They developed techniques to embed a DNA-based barcode into biological samples to attest to their authenticity. This is a significant milestone for biological information forensics."

-- NSF Public Affairs, researchnews@nsf.gov (mailto:researchnews@nsf.gov)
