Real or fake? Creating fingers to protect identities

September 20 2017

MSU's biometrics expert Anil Jain and his Ph.D. student Joshua Engelsma have, for the first time, designed and created a fake finger containing multiple key properties of the human skin. Commonly called a spoof, this fake finger is being used to test fingerprint readers to help determine their resilience to spoof attacks and which will lead to more resilient fingerprint readers. Credit: Michigan State University

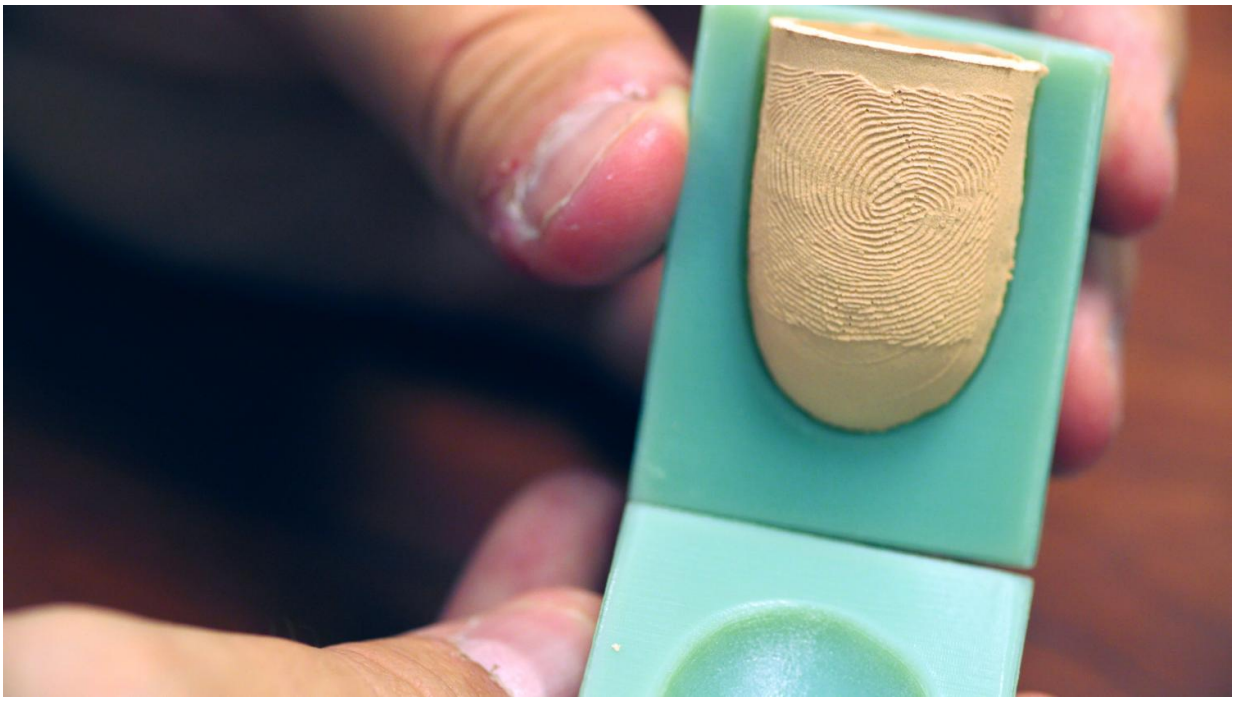
Do you know how safe it is to use your finger as a security login? And

have you wondered how your cell phone knows if your finger is real or a fake?

Michigan State University biometric expert Anil Jain and his team are working to answer these questions and solve the biggest problems facing fingerprint recognition systems today: how secure they are and how to determine whether the finger being used is actually a human finger.

In an effort to test and help solve this problem, Jain, a University Distinguished Professor, and doctoral student Joshua Engelsma have for the first time designed and created a fake finger containing multiple key properties of human skin. Commonly called a spoof, this fake finger has been used to test two of the predominant types of fingerprint readers to help determine their resilience to spoof attacks.

The fake fingers developed at MSU were created using a combination of carefully chosen materials, including conductive silicone, silicone thinner and pigments. In addition to determining the materials, the entire fabrication process, using a molding and casting technique, was designed and implemented by the team.



MSU's biometrics expert Anil Jain and his Ph.D. student Joshua Engelsma have, for the first time, designed and created a fake finger containing multiple key properties of the human skin. Commonly called a spoof, this fake finger is being used to test fingerprint readers to help determine their resilience to spoof attacks and which will lead to more resilient fingerprint readers. Credit: Michigan State University

"What makes our design unique is that it mimics a real finger by incorporating basic properties of human skin," said Jain. "This new spoof has the proper mechanical, optical and electrical properties of a human finger. Compared to current fake fingers that only contain one or two of these properties, our new version could prove much more challenging to detect. It will help motivate designers to build better fingerprint readers and develop robust spoof-detection algorithms."

Developing more resilient fingerprint readers is important because they

are now abundantly used for authentication in cell phones, computers, amusement parks, banks, airports, law enforcement, border security and more.

One specific way the synthetic fingers will be used is for testing the recognition accuracy between different types of fingerprint readers. The readers differ based on the type of sensors used to record the digital fingerprints, such as optical (using light rays to capture an image) or capacitive (using electrical current to create an image).

Currently, recognition accuracy declines when the same fingerprint taken using two different types of fingerprint readers is compared. For example, if a capacitive reader was used to capture a fingerprint, but an optical fingerprint reader was used later to authenticate that same fingerprint, it's less likely the print will be accurately identified. By using MSU's new spoof, companies could develop methods to improve the accuracy.

"Given their unique characteristics, we believe our fake fingers will be valuable to the fingerprint recognition community," said Jain. "Consumers need to know their fingerprints and identity are secure, and vendors and designers need to demonstrate to the consumers the technology is not only accurate but also resilient to spoof attacks."

Jain and his team have begun work on the next phase of this research: designing and building a fingerprint reader to test spoof-detection capabilities. Once ready, this low-cost reader could be easily built in a couple of hours by others in the fingerprint recognition community to test for real versus fake fingerprints. Jain's lab is additionally working on algorithms that will make this fingerprint reader more resilient to spoof presentation attacks.