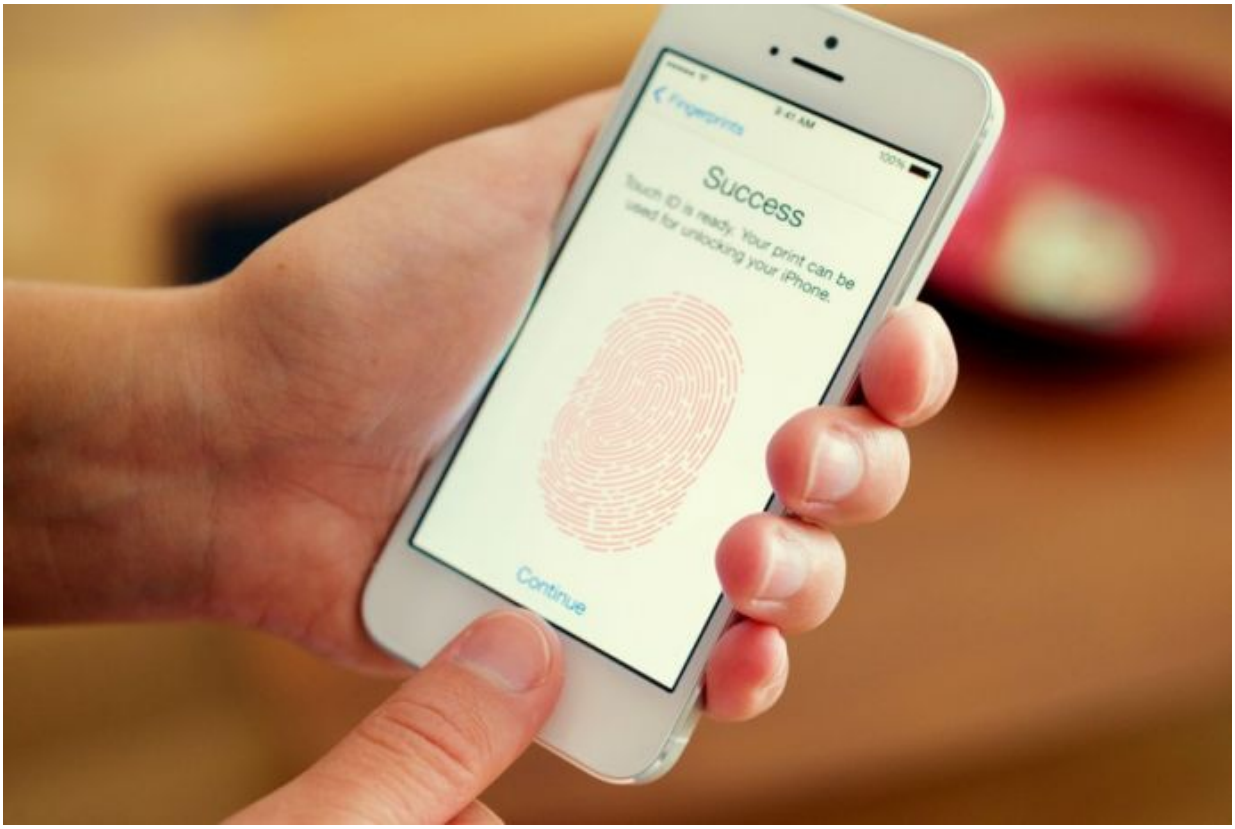
So you think you can secure your mobile phone with a fingerprint?

April 11 2017



Credit: NYU Tandon School of Engineering

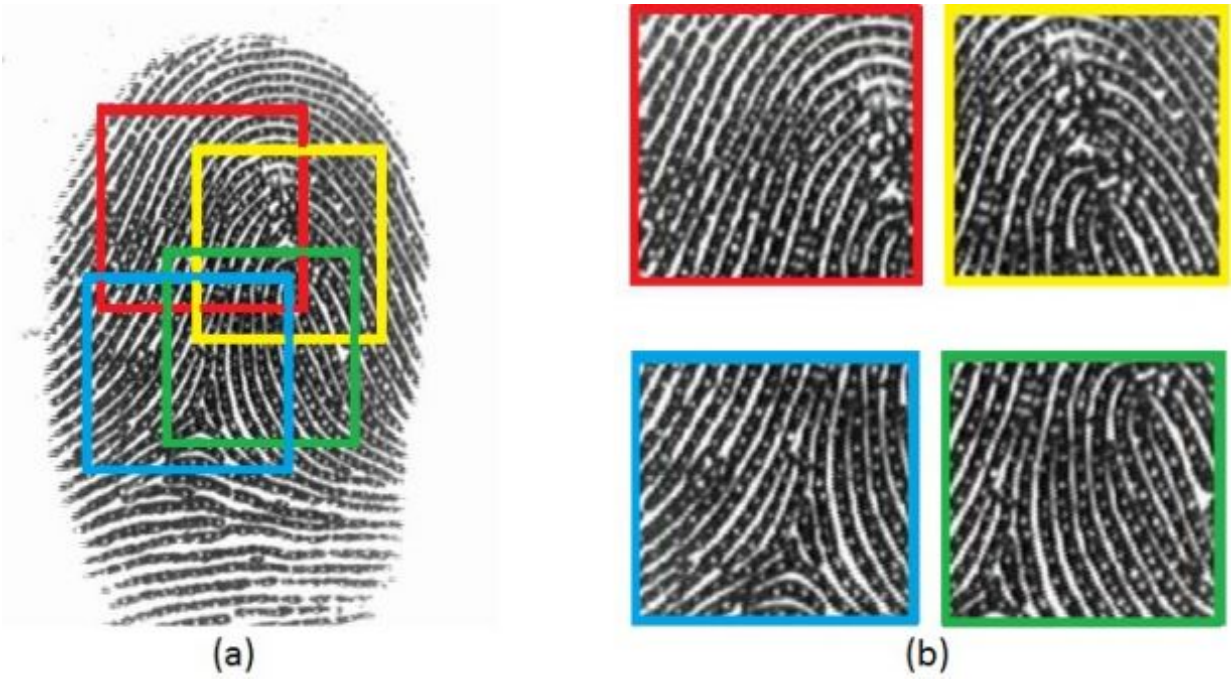
No two people are believed to have identical fingerprints, but researchers at the New York University Tandon School of Engineering and Michigan State University College of Engineering have found that

partial similarities between prints are common enough that the fingerprint-based security systems used in mobile phones and other electronic devices can be more vulnerable than previously thought.

The vulnerability lies in the fact that fingerprint-based authentication systems feature small sensors that do not capture a user's full fingerprint. Instead, they scan and store partial fingerprints, and many phones allow users to enroll several different fingers in their authentication system. Identity is confirmed when a user's fingerprint matches any one of the saved partial prints. The researchers hypothesized that there could be enough similarities among different people's partial prints that one could create a "MasterPrint."

Nasir Memon, a professor of computer science and engineering at NYU Tandon and the research team leader, explained that the MasterPrint concept bears some similarity to a hacker who attempts to crack a PIN-based system using a commonly adopted password such as 1234. "About 4 percent of the time, the password 1234 will be correct, which is a relatively high probability when you're just guessing," said Memon. The research team set out to see if they could find a MasterPrint that could reveal a similar level of vulnerability. Indeed, they found that certain attributes in human fingerprint patterns were common enough to raise security concerns.

Memon and his colleagues, NYU Tandon Postdoctoral Fellow Aditi Roy and Michigan State University Professor of Computer Science and Engineering Arun Ross, undertook their analysis using 8,200 partial fingerprints. Using commercial fingerprint verification software, they found an average of 92 potential MasterPrints for every randomly sampled batch of 800 partial prints. (They defined a MasterPrint as one that matches at least 4 percent of the other prints in the randomly sampled batch.)



Smartphones typically capture a limited portion of the full fingerprint using small sensors. Multiple partial fingerprints are captured for the same finger during enrollment. The figure shows a set of partial fingerprints (b) extracted from the full fingerprint (a). Credit: NYU Tandon School of Engineering

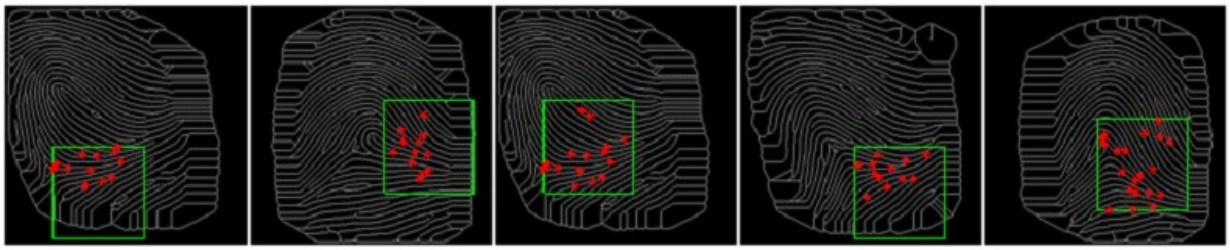
They found, however, just one full-fingerprint MasterPrint in a sample of 800 full prints. "Not surprisingly, there's a much greater chance of falsely matching a partial print than a full one, and most devices rely only on partials for identification," said Memon.

The team analyzed the attributes of MasterPrints culled from real fingerprint images, and then built an algorithm for creating synthetic partial MasterPrints. Experiments showed that synthetic partial prints have an even wider matching potential, making them more likely to fool biometric security systems than real partial fingerprints. With their

digitally simulated MasterPrints, the team reported successfully matching between 26 and 65 percent of users, depending on how many partial fingerprint impressions were stored for each user and assuming a maximum number of five attempts per authentication. The more partial fingerprints a given smartphone stores for each user, the more vulnerable it is.

Roy emphasized that their work was done in a simulated environment. She noted, however, that improvements in creating synthetic prints and techniques for transferring digital MasterPrints to physical artifacts in order to spoof a device pose significant security concerns. The high matching capability of MasterPrints points to the challenges of designing trustworthy fingerprint-based authentication systems and reinforces the need for multi-factor authentication schemes. She said this work may inform future designs.

"As fingerprint sensors become smaller in size, it is imperative for the resolution of the sensors to be significantly improved in order for them to capture additional fingerprint features," Ross said. "If resolution is not improved, the distinctiveness of a user's fingerprint will be inevitably compromised. The empirical analysis conducted in this research clearly substantiates this."



Credit: NYU Tandon School of Engineering

Memon noted that the results of the team's research are based on minutiae-based matching, which any particular vendor may or may not use. Nevertheless, as long as partial fingerprints are used for unlocking devices and multiple partial impressions per finger are stored, the probability of finding MasterPrints increases significantly, he said.

"NSF's investments in cybersecurity research build the foundational knowledge base needed to protect us in cyberspace," said Nina Amla, program director in the Division of Computing and Communication Foundations at the National Science Foundation. "Much as other NSF-funded research has helped identify vulnerabilities in everyday technologies, such as cars or medical devices, investigating the vulnerabilities of fingerprint-based authentication systems informs continuous advancements in security, ensuring more reliable protection for users."

"MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems" appears in *IEEE Transactions on Information Forensics & Security* at ieeexplore.ieee.org/document/7893784

Provided by NYU Tandon School of Engineering