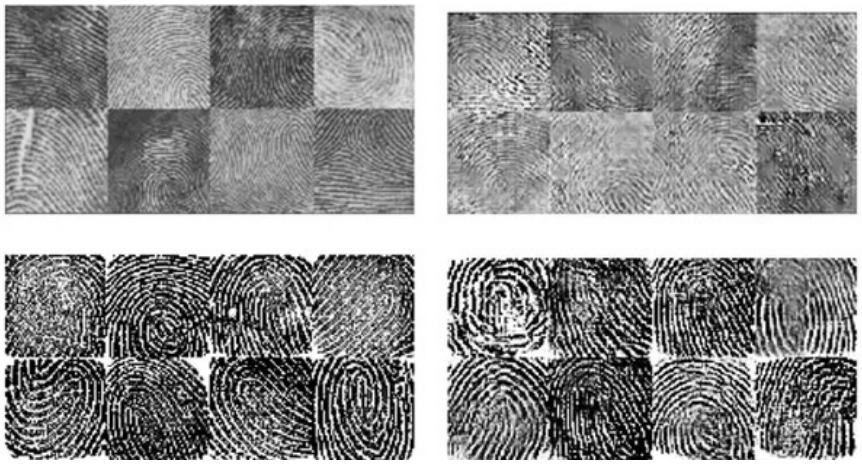
Fake fingerprints of AI are able to unlock the security of current smartphones

Recently, security researchers have announced the successful programming of artificial intelligence (AI) capable of creating universal false fingerprints based on machine learning power. This fake fingerprint is capable of opening up most smartphones using biometric sensors and has a certain success rate.

Recently, security researchers have announced the successful programming of artificial intelligence (AI) capable of creating universal false fingerprints based on machine learning power. This fake fingerprint is capable of opening up most smartphones using biometric sensors and "has a certain success rate".

In modern equipment, biometric security can be considered as the most perfect security method. Because each individual has a personal biometric (such as fingerprint, iris, .) and only that individual can unlock the device. However, according to the results of recent studies, the vast majority of biometric identification devices on the market can be fooled.



Researchers from New York University and University of Michigan have created successful artificial intelligence (AI) called DeepMasterPrints, able to self-study and create fake fingerprints, replacing most of the Fingerprints of 6,000 individuals are included in the research database. These artificial fingerprints work similarly to a universal key.

This system after analyzing the huge amount of fingerprints will create a fake fingerprint that is identical to all the fingerprint numbers in the database. An analytical network will check and evaluate whether the fake fingerprint is real or fake. If it is fake, the system will correct it so that the fake fingerprint is more realistic. And after thousands of corrections, the system eventually created a completely identical fake fingerprint and deceived the system.

Universal fingerprints can bypass most of the fingerprint recognition systems available on current smartphones. Security developers want the genuine identification on smartphones to happen faster, sacrificing absolute accuracy, using only a small portion of the user's fingerprint to identify. This has created a security gap that can be exploited.

The researchers used two types of fingerprint data, printed on paper and taken from a digital scanner system, to train the AI ??system. Universal fingerprint must pass three security levels.

Test results show that, at each level, there is a rate of FMR deviation, fingerprint sensor rate that identifies fake fingerprints as real, different. The failure rate of each security level is as follows: the error of the highest security level is only 0.01%, the average is 0.1% and the lowest security level is 1%.

At the lowest security level, the universal fingerprint deceives the system in 76% of the attempts. An amazing result, but the researchers also confirmed, currently there is no fingerprint sensor system operating at this low security level. At the most commonly used security level, the average, multimeter fingerprints surpass the system with 22% of attempts. And it only deceives the system by 1.2% of the attempts at the highest security level.

However, the researchers also affirmed that the figures do not show that the fingerprint security system can be easily bypassed. Users can still fully trust this biometric security system.

The researchers said they created universal fingerprints with the aim of reminding future security designers to consider sacrificing security for convenience, accepting system loopholes to Allows unlocking fingerprints faster.

See more:

1. The speed of fingerprint sensor under the screen on the Vivo X20 Plus UD and Face ID of iPhone X, which one is faster?
2. Find out how fingerprint security technology works
3. There are vulnerabilities that allow hackers to bypass the fingerprint security mechanism of Lenovo computers