Már az ujjlenyomat-olvasókban sem bízhatunk

Amerikai kutatóknak sikerült néhány kiskaput kihasználni, és bebocsátást nyerni ujjlenyomat-ellenőrző rendszerekbe gépi kód kreálta rajzolatokkal.

Az emberi ujjlenyomat összetettsége és egyedisége miatt kiváló alapanyag a biometrikus azonosításhoz. Ráadásul a felhasználóknál mindig kéznél van, sőt a jelszavakkal ellentétben el se tudják felejteni. Hogy azért itt sem árt az óvatosság, azt egy kutatócsapat bizonyította azzal, hogy képesek voltak átverni a biztonsági rendszert egy trenírozott mélytanuló algoritmussal.

Kirajzolódó átverés

A New York University tudósai egyfajta mesterkulcsot generáltak mesterséges intelligencia bevetésével. A neurális hálózat kísérletezéssel olyan ujjlenyomat-részleteket állított elő, amelyekkel egészen jó arányban tudtak fals pozitív eredményeket csiholni a beléptető rendszerből. A Los Angeles-i biztonsági konferencián bemutatott projekt anyaga szerint egy biometrikus adatbázisban található készlet több mint ötödéhez képes volt hamis, de a teszten átmenő rajzolatokat alkotni. Mindezt egy olyan rendszeren végezték el, amelyiknél a hibahatár egy ezrelék alatt van.

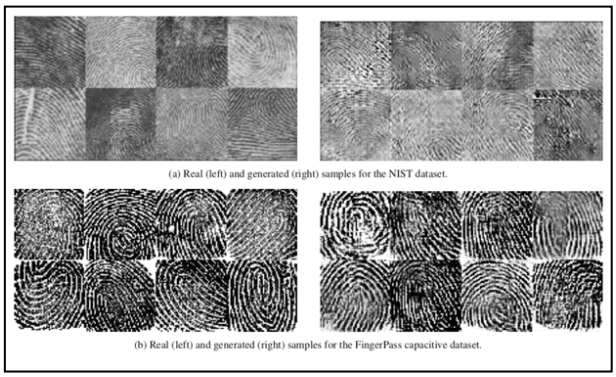
A kutatók az ilyen típusú azonosításnál rendszerint alkalmazott gyenge pontok kihasználásával voltak képesek ilyen jó eredményekre. Ezek egyike volt az, hogy a leolvasók egy-egy érintésnél csak az ujjlenyomat egy bizonyos részét tudják letapogatni, éppen ezért a rendszerek többségénél elég a zöld jelzéshez az is, ha a benne tárolt rajzolatok egy részével van egyezés. A másik kiskaput az jelenti, hogy bizonyos elrendeződések gyakrabban fordulnak elő az emberi ujjlenyomaton, mint mások. Éppen ezért azok a kreált rajzolatok, amelyek ilyeneket tartalmaznak, sokkal nagyobb valószínűséggel tudnak (részleges) egyezést mutatni a rendszerben tárolt adatokkal.

Ezekkel az ötletekkel felfegyverkezve, a tudósok beindítottak egy „generatív ellenséges hálózatot” (generative adversarial networks, GAN). A technológia lényege, hogy az algoritmusok versenyeznek egymással. Az első felel a képek megalkotásáért, a másodiknak pedig el kell bírálnia azt, hogy az mennyire hasonlít az adatbázisában található valamelyik mintára. Az algoritmusok a kapott eredmények alapján folyamatosan finomítanak saját döntéseiken, így egymást trenírozva, sokszoros iterációt követőn egyre jobb eredményeket kaphatunk. (Ugyanezt a módszert alkalmazta az az alkotócsapat is, amelynek képét nemrég óriási összegért árverezte el a Christie's.)

Az embereket is megtéveszti

Az algoritmus teljesítménye azért is tekinthető áttörésként, mivel korábbi metódusokkal sikerült már a gépi beléptetést bizonyos esetekben átverő mintázatokat alkotni, ám azok túlságosan mesterséges rajzolatok voltak, amelyekről egy humán ellenőrző személy azonnal meg tudta mondani, hogy nem emberi ujjlenyomatról van szó. Ahogy az alábbi fotón is jól látszik, a mesterséges intelligencia a valódi mintákból kiindulva első pillantásra teljesen "emberszerű" másolatokat produkált.

Az amerikai kutatók hekkelési kísérlete nagyban hasonlít a jelszavaknál alkalmazott szótárazós módszerre. Utóbbi lényege, hogy a támadók nem véletlenszerű karaktersorokkal tesztelik a védel-



Eredeti (bal oldal), illetve a gép által rajzolt ujjlenyomatrészek (forrás: NYU)

met, hanem lefuttatnak egy teljes szótári adatbázist, így ha értelmes szó volt a jelszó, akkor sokkal gyorsabban érnek célt. Ez általában nem alkalmas egy konkrét felhasználó elleni támadásra, de nagy mennyiségű célpont esetén már kellő arányban hozhat sikert ahhoz, hogy érdemes legyen próbálkozni vele.

Forrás: **https://bitport.hu/mar-az-ujjlenyomat-olvasokban-sem-bizhatunk**

Válogatta: Fonyó Istvánné