Nähtamatuse kuub: disainerid loovad mustreid, mida kaamerad ja AI ei märka

1 kuu tagasi - 09.08.2026 Autor: AM

Kesklinnas võib iga kolme meetri tagant jälgida sind mõni turvakaamera. Näojooned skaneeritakse, tehisintellekt raporteerib täpselt, kuhu edasi suundud. Sa ei ole andnud selleks nõusolekut, sind ei ole hoiatatud, kuid sinu nägu on juba süsteemis jälgimisel. Aga mis saaks siis, kui tavaline T-särk või kaelasall toimiks digitaalse nähtamatuse kuuena? Just sellise lahendusega on lagedale tulnud ühisrahastusplatvormil Kickstarter laineid lööv projekt noRecognition, mis lubab privaatsuse ihalejatele tagasi anda mingisuguse kontrolli oma isikuandmete üle.

Digitaalne panoptikon: sa pole klient, sa oled toode

USA-s on politsei näotuvastusvõrgustikes juba üle 117 miljoni inimese – umbes iga kolmas täiskasvanu.

Kaamerate tihedus mõnes piirkonnas on absurdne: näiteks Kansas Citys asub ühel ainusal ruutmiilil üle 125 nutika tänavavalgusti, kümned topeltkaameratega kioskikohad ja sajad hoonekaamerad.

> "Sa ei ole ühegi selle süsteemi klient. Sa oled toode," nendib projekti autor.

Mure pole aga ainult jälgimises endas, vaid ka süsteemide ebatäpsuses. Sõltumatud auditid näitavad pidevalt, et tumedama nahatooniga inimeste puhul teevad algoritmid valevasteid 10 kuni 100 korda sagedamini. Tarkvara eksib kõige rohkem just seal, kus politseikontroll on kõige rangem.

Miks varasemad "nähtamatud" riided ebaõnnestusid?

Mõte algoritmide eksitamisest riietuse abil pole täiesti uus, kuid senised katsetused on meenutanud pigem pusle kokkupanekut suletud silmadega. Näotuvastuse petmine ei ole üks lihtne ülesanne, vaid jaguneb kolmeks eraldi etapiks:

1. Isiku kohalolu tuvastamine (kas kaadris on inimene?)
2. Näo leidmine (kus asub nägu?)

3. Näo kokkuviimine isikuga (kellega on tegu?)

Enamik turul olevaid vaenulike ehk *adversarial*-mustritega riideid üritab lahendada vaid esimest sammu, kuid neid reklaamitakse kolmanda sammu vältimiseks. Veelgi hullem – laboritingimustes saadud 57-protsendiline edu tõhususes kukkus tegelikus elus ja väljaspool katseklaasi kolinal kuni 64 protsenti. Testimata kaitse müümine inimesele, kes võib sellele panustada oma turvalisuse, on ohtlik valelootuse andmine.

31,7 miljonit katsetust: tehisaru *vs* tehisaru

noRecognition taga seisab pikaajalise kogemusega küberturvalisuse ekspert – endine suurkontserni turvajuht (CISO) ja NSA lepingupartnerite niinimetatud punaste tiimide (*red team*) juht, kes on esinenud mainekatel konverentsidel DEF CON ja Black Hat.

Selle asemel et oletada, panustas tema tiim teaduslikku lähenemisse:

- Üks sülearvuti kasvas 40 vabatahtliku graafikakaardi (GPU) sõlmega hajutatud võrgustikuks.
- Mustreid söödeti simuleeritud riietel otse reaalsetesse videovalve mudelitesse.
- Läbi viidi 31,7 miljonit testi, mille käigus tuvastati 534 000 anomaaliat.

> "Privaatsus on õigus, mitte privileeg neile, kellel pole midagi varjata."

Märtsis koondati 82 gigabaiti katsandmeid 5,7 miljoniks sildistatud näiteks. Nende põhjal treeniti süva-sarrusõppe (*deep reinforcement learning*) mudelit. See ei ole pildipank, kust mustreid otsitakse, vaid tehisintellekt, mis genereerib geomeetrilisi mustreid, mis mõjuvad kaamerate algoritmidele nagu hallutsinogeenid.

Iga loodav muster peab läbima 11 tootmises oleva tehisintellekti mudeli tuleproovi (sh YOLOv8n, ArcFace, RetinaFace jpt). Tulemus? Katsealuse tuvastamise kindlus langeb algselt 88 protsendilt praktiliselt nullini.

Kuidas kangamuster algoritmi ära petab?

Kujuta ette, et tehisintellekt on nagu ülikiire pildiraamatu vaataja, kes otsib teatud kujundeid – näiteks kahte silma, nina ja suujoonestikku või inimese kehakuju. noRecognition riietele trükitud geomeetria toimib kui visuaalne

mürasüst. See "söödab" kaamerale ette visuaalseid konksu- ja kurvikombinatsioone, mis panevad algoritmi arvama, et tegemist on hoopis taustamüra, seina või määratlemata objektiga.

Muster töötab eri riideesemetel erinevalt:

- T-särk ja pusa: nende suur pindala halvab eelkõige inimese tuvastamise mudelid. Mudel ei saa aru, et kaadris on keha.
- Kaelasall (buff): see on liiga väike kehatuvastuse murdmiseks, kuid lõhub selgelt näotuvastuse. Kui nägu ei leita, pole midagi välja lõigata ega andmebaasiga võrrelda.

Praeguaseks on kickstarteri 5000-dollarine eesmärk juba ammu ületatud ja kogutud on üle 13 000 dollari lahenduse arenamiseks.

PLUSSID

- Testitud 11 reaalselt kasutusel oleva tehisintellekti mudeli vastu.
- Arendajad avaldavad nii edukad tulemused kui ka ebaõnnestumised (*negatives published*).
- Mudelit treeniti vaid enda katseandmetel; teiste kunstnike loomingut ega veebist kaabitud pilte pole kasutatud.
- Vähendab tuvastuse tõenäosust 88%-lt olematule tasemele.
- *Dye-sublimation* trükk: muster trükitakse otse kanga kiududesse, mitte ei kleebita peale.

MIINUSED

- Kui trükk nihkub kas või paari millimeetri võrra suuremaks või väiksemaks, kaotab see oma toimivuse (kuigi näeb ikka kena välja).
- Avalikkusele näidatavad pildid on tahtlikult nõrgemate näitajatega, et turvafirmad ei saaks algoritme nende vastu enne müüki treenida.
- Kuigi kangaproovid ja simulatsioonid on edukad, on laiaulatuslikud tänavakatsed alles käimas.

- Uudised

- Turvalisus
- Tehisintellekt

Pilt

SAME PERSON. SAME CAMERA.

Flock Falcon v2, the person detector running on tens of thousands of American streets
Identical coverage on both sides. Only the pattern changes.

PLAIN TEE, SAME COVERAGE
PERSON DETECTED 86%

SAME TEE, OUR PATTERN
NO DETECTION

Demonstration pattern. The design that ships is previously unreleased, and stronger.