PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 3963 di lunedì 06 marzo 2017

Come ingannare i sistemi di riconoscimento facciale

Uno studio compiuto da alcuni specialisti universitari americani ha messo in evidenza che gli attuali sistemi di riconoscimento facciale possono essere ingannati con relativa facilità. Di Adalberto Biasiotti.

Credo che sia difficile trovare un sistema di riconoscimento biometrico più semplice nell'uso e meno invasivo nei confronti del soggetto coinvolto, rispetto ad un sistema di riconoscimento facciale. In fondo tutti noi giriamo per le vie della città portando in bella mostra il nostro volto e centinaia di persone lo possono osservare.

Questo fatto non ci arreca disturbo e quindi il fatto che un dispositivo elettronico possa analizzare il nostro volto ed effettuare analisi e confronti con altri volti non turba più di tanto il senso di privacy di un cittadino.

Oggi sono disponibili sistemi di riconoscimento facciale, utilizzati all'ingresso di centri elaborazione dati od altre attività ad alto rischio, che costano poco più di qualche centinaio di euro e possono riconoscere alcune centinaia di volti. La stessa autorità garante ha riconosciuto che queste particolari tipologie di apparati, in grazia della bassa invasività, possono essere usate senza troppi problemi.

Non vi saranno forse problemi dal punto di vista della protezione dei dati personali, ma sembra invece che esistano problemi circa la capacità di questi applicativi di riconoscere davvero un volto.

Il problema diventa ancora più complesso quando questi applicativi sono collegati a sistemi di videosorveglianza, che controllano aree critiche all'imbarco dei passeggeri in zone aeroportuali, oppure addirittura al movimento dei passeggeri lungo le scale della metropolitana.

Negli Stati Uniti numerosi corpi di polizia hanno deciso di avventurarsi su questo percorso, nella speranza di rendere più efficiente ed efficace l'opera degli agenti. Se il software, collegato alle telecamere, cattura l'immagine del volto di un ricercato, e questo ricercato può essere bloccato, non v'è dubbio che tutti siano soddisfatti.

La situazione non è diversa da quella che si incontra utilizzando le moderne telecamere, installate a bordo della polizia locale, che catturano la targa di un autoveicolo ed effettuano automaticamente un confronto con il data base delle coperture assicurative e delle revisioni. Un comando di polizia locale dell'Italia centrale, che ha cominciato ad installare , due o tre di queste telecamere sulle autovetture di pattuglia ha potuto erogare la bellezza di poco più di 10.000 sanzioni nel giro di un paio di giorni, ed il tutto in forma assolutamente automatica!

Ma la domanda che adesso ci poniamo è la seguente quanto sono affidabili i sistemi di riconoscimento facciale?

Gli studiosi americani, sopraccitati, hanno cominciato ad analizzare le modalità con le quali operano questi applicativi ed hanno messo a punto delle semplici tecnologie, che possono ingannare questi dispositivi in modi diversi:

- il primo inganno è legato al fatto che il software non è neppure in grado di capire che si trova davanti ad un volto umano,
- il secondo inganno è legato al fatto che il software non è capace di riconoscere correttamente un volto umano,
- il terzo inganno è legato al fatto che il software scambia un volto umano per un altro.

Il primo inganno viene chiamato "face deletion", il secondo inganno viene chiamato "face dodging", il terzo inganno viene chiamato "face impersonation".

Per mettere a punto queste tecniche occorre inoltre prendere alcune cautele; ad esempio, se uno si pone una maschera bianca davanti al volto certamente il software non riconoscerebbe la presenza del volto, ma non credo che un soggetto, che giri per la città con questa maschera bianca sul volto, possa camminare a lungo, prima di attirare l'attenzione dei passanti e delle forze dell'ordine.

Ecco perché le tecniche che debbono essere utilizzate per ingannare gli applicativi di riconoscimento facciale devono essere tali da non presentare delle caratteristiche che possano insospettire i presenti.

In altre parole, queste tecniche devono essere oltremodo discrete e non devono essere tali da alterare il volto in modo tale, da attirare l'attenzione di terzi.

Vediamo adesso come funzionano questi sistemi di inganno dei software di riconoscimento facciale.

Esistono due grandi famiglie di software di riconoscimento facciale, che sostanzialmente funzionano scomponendo un volto in una serie di pixel ed effettuando un confronto fra i pixel così acquisiti e pixel afferenti ad un volto, che è stato precedentemente memorizzato nell'archivio del software. Uno dei più diffusi software di riconoscimento facciale si chiama Face ++. Lo studio degli specialisti si è concentrato sulla analisi delle modalità di funzionamento di questo software e soprattutto sulla individuazione di quale potrebbe essere il minimo numero di pixel, che occorre perturbare, per impedire al software di funzionare regolarmente.

Se è possibile, modificando soltanto il tre percento delle caratteristiche del volto di un soggetto, fare in modo che il volto del soggetto non venga più riconosciuto, l'obiettivo viene raggiunto. Sarà poi da vedere come sia possibile, fra le tre tipologie di inganno sopra illustrate, orientare il software verso una particolare categoria di inganno, rispetto ad un'altra.

Orbene, gli specialisti hanno potuto appurare che, ad esempio indossando un paio di occhiali con una montatura disegnata in modo particolare, e con la montatura stessa colorata con vari colori, si introduce una perturbazione dell'immagine catturata, che è sufficiente per ingannare il software. Sono stati fatti diversi esperimenti, che praticamente sempre hanno dato un ottimo risultato, sia impedendo al software di riconoscere la presenza di un volto umano, che corrisponde alla tipologia di inganno di sparizione di un volto, sia inducendo il software a riconoscere un volto umano, che non era quello del soggetto che si era presentato per il riconoscimento.

Anche la terza varietà di inganno è stata portata a termine con relativa facilità, effettuando, grazie ad un software specializzato, un confronto tra le caratteristiche facciali del volto del soggetto che deve essere riconosciuto, e le caratteristiche facciali del soggetto che invece si voleva far riconoscere al software.

In diversi casi, è stato sufficiente mettere un berretto in testa al soggetto in causa, oltre ad un paio di occhiali, specialmente progettati, per indurre il software a riconoscere erroneamente la persona in questione, affermando invece che la persona riconosciuta era tutt'altra.

È facile capire come una tale situazione possa portare a rischi concreti nell'effettuazione di indagini sul comportamento di persone sospette.

Se il volto della persona sospetta non viene correttamente riconosciuto, è possibile che egli si muova nell'ambito cittadino, coperto dagli applicativi di riconoscimento facciale, senza che resti alcuna traccia probatoria dei suoi movimenti.

Il primo tipo di inganno, che è quello che fa letteralmente sparire una faccia del campo ripreso dalla telecamera, potrebbe essere utilizzato da chi non desidera che la telecamera tracci i suoi movimenti; si tratta evidentemente di una situazione diversa da chi invece vuole che i suoi movimenti siano tracciati, ma non corrispondano ai movimenti effettivamente compiuti.

Lo studio è accompagnato da numerosi esempi pratici, che illustrano come le tecniche di inganno possano essere attuate utilizzando delle stampanti 2D, oppure stampanti 3D, a colori. Con queste stampanti è possibile realizzare degli occhiali, che vengono posti sul volto del soggetto che vuole ingannare l'applicativo di riconoscimento facciale.

Una particolare sagomatura della montatura degli occhiali e particolari colorazioni della montatura stessa permettono di perturbare i pixel dell'immagine catturata, anche solo per qualche percento, creando poi un effetto a valanga, che fa saltare tutti i criteri di riconoscimento.

La faccenda diventa un poco più complicata se si vuole invece che il software riconosca una specifica faccia, che non è quella che è stata inquadrata. In questo caso la costruzione di montature di occhiali è alquanto più complessa, ma gli esperimenti praticamente condotti hanno dimostrato che più di una volta il software ha riconosciuto il volto di un celebre attore, mentre il volto effettivamente presentato, camuffato con la montatura degli occhiali, era completamente diverso.

Per capire come sia possibile realizzare questo inganno, occorre tener presente che il software analizza pixel e non ha la minima idea del volto che ha davanti, come invece l'avrebbe un essere umano. Questi software lavorano con applicativi cosiddetti di ML, cioè machine learning, che sono gli stessi che vengono utilizzati per guidare le automobili senza pilota, oppure per individuare metastasi nel corpo umano.

L'analisi dei pixel non ha quindi nessun collegamento con la realtà effettiva, ma solo con una realtà virtuale, costruita dalla macchina.

Sono convinto che è bene che i lettori siano al corrente di questi studi, che stanno proseguendo nella direzione corretta, vale a dire nella direzione nella quale si evitano le debolezze degli attuali software e si cercano di introdurre degli elementi di correzione.

Adalberto Biasiotti
