PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4519 di Lunedì 29 luglio 2019

Gli applicativi di riconoscimento facciale

La crescente diffusione degli applicativi di riconoscimento facciale ha destato le vive preoccupazioni dei tutori della protezione dei dati personali.

Gli applicativi di riconoscimento facciale stanno trovando un campo di applicazione sempre più allargato. Il fatto che i più moderni smartphone siano già dotati di questo dispositivo mette in evidenza come la praticità d'uso possa essere oltremodo attraente per l'utente, perfino più attraente rispetto al più tradizionale riconoscimento dell'impronta digitale.

Il fatto che questi applicativi possano essere utilizzati anche su larga scala, ad esempio installandoli sugli impianti di videosorveglianza di ampie zone cittadine o di zone localizzate, come ad esempio le scale di salita e discesa della metropolitana, li rendono assai attraenti per le forze dell'ordine. Recentemente, la polizia di Stato ha presentato un tale applicativo, che può essere installato all'ingresso delle manifestazioni sportive, in modo da riconoscere automaticamente persone fisiche, nei cui confronti sia stato applicato il cosiddetto DASPO.

Questi applicativi sono quindi assai utili, quando lavorano on-line, ma sono anche utili a posteriori, quando ad esempio le forze dell'ordine recuperano le immagini provenienti da impianti di videosorveglianza, che hanno ripreso un evento delittuoso. L'esame delle immagini registrate, utilizzando un applicativo di riconoscimento facciale, può permettere di confrontare i volti ripresi con un data base di volti di soggetti, potenzialmente o effettivamente coinvolti nell'evento delittuoso.

Le crescenti preoccupazioni nei tutori della privacy hanno trovato una prima risposta nella città di San Francisco, una delle più avanzate al mondo in termini di utilizzo di strumenti computerizzati, adatti a gestire una smart city. Gli amministratori di questa città hanno deciso che non si possono utilizzare questi applicativi sugli impianti di videosorveglianza di zone pubbliche, ma solo a posteriori e con specifiche modalità garantistiche.

Poiché è noto che fatta la legge, si trova l'inganno, alcuni studiosi hanno cominciato a esaminare la possibilità di ingannare gli applicativi di riconoscimento facciale, con alcune tecniche relativamente semplici.

I lettori certo ricordano che anche i lettori di impronta digitale, od almeno alcune tipologie di essi, possono essere ingannati da riproduzioni fotografiche di un'impronta digitale o addirittura da una riproduzione tridimensionale, ottenuta con calchi in resina. Gli studiosi hanno analizzato le modalità di cattura della stringa biometrica, collegata ad un volto ed hanno cominciato a ipotizzare possibili manipolazioni.

Ricordo ancora una volta ai lettori che questi applicativi non riconoscono il volto, come se fosse una fotografia, ma catturano una immagine del volto e la sottopongono ad un processo di digitalizzazione vettoriale, che ad esempio misura la distanza fra le pupille, la larghezza della bocca, la distanza fra le pupille e gli angoli della bocca e via dicendo. Si crea così una stringa che viene archiviata a futuro riferimento. Quando viene sottoposto un nuovo volto, viene effettuato lo stesso calcolo vettoriale e la stringa risultante viene confrontata con quella di riferimento.

È proprio giocando su questo fatto che gli esperti di informatica hanno cercato di individuare quali possano essere gli interventi, che potrebbero permettere ad un soggetto di non essere riconosciuto. È evidente che se egli porta una maschera, il problema non si pone, ma d'altro canto non sempre è agevole aggirarsi per le vie cittadine con il volto coperto da una maschera.

Gli esperti hanno quindi cominciato a vedere come potrebbe essere possibile introdurre lievi alterazioni del volto, che però potrebbero portare al calcolo di una stringa biometrica profondamente modificata, tale da compromettere un efficace confronto. Ad esempio, potrebbe bastare tenere in bocca il gambo di una pallina di caramella, che sporge all'estremità della bocca, per creare una alterazione della stringa biometrica, sufficiente per impedire il riconoscimento.

Gli specialisti della Cornell university hanno sviluppato questo studio per mettere in evidenza possibili debolezze, cui si dovrebbe porre rimedio, e non certo per fornire ai malviventi uno strumento di de-identificazione.

Un'altra tecnica di mascheramento, illustrata dagli studiosi, prevede che il soggetto, che non vuole essere riconosciuto, tenga un giornale ripiegato vicino al volto, con aria indifferente, creando anche in questo caso una modifica del volto ripreso, che porta al calcolo di una stringa biometrica non corretta.

Alcuni specialisti affermano che si potrebbe porre rimedio a questo inconveniente utilizzando algoritmi tridimensionali di riconoscimento facciale; questa tecnica è già disponibile, ma comporta alcuna complessità che ne impediscono per il momento l'utilizzo su larga scala.

Per ulteriori informazioni su questo tema raccomando al lettore la lettura del documento che segue:

Fooling automated surveillance cameras: adversarial patches to attack person detection

Simen Thys, Wiebe Van Ranst, Toon Goedemé

Adalberto Biasiotti

www.puntosicuro.it