PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4822 di Lunedì 23 novembre 2020

E' ormai provato: i software di riconoscimento facciale sono razzisti!

Il Government accounting Office-GAO, ha pubblicato recentemente un'analisi, svolta insieme al NIST, che ha esaminato i risultati di utilizzo su larga scala di software di riconoscimento facciale. I risultati lasciano alquanto perplessi.

Gli Stati Uniti hanno una agenzia specializzata nella protezione dei confini, chiamata custom Border protection- CBP. A questa agenzia è attribuita la responsabilità di verificare anche i movimenti dei passeggeri aerei, utilizzando, se possibile, tecnologie avanzate. In questo quadro la CBP ha deciso di attivare, in una trentina di aeroporti degli Stati Uniti, un Varco, ove viene effettuato il riconoscimento facciale del passeggero. Ricordo ai lettori che in Italia varchi di questo tipo, ma funzionanti su principi leggermente diversi, erano già attivi a Fiumicino da parecchi anni. Il passeggero si presenta al varco, appoggia il suo passaporto su un lettore e nel contempo una telecamera cattura una foto del suo volto.

Indi, almeno negli Stati Uniti, vengono effettuati due confronti:

- un confronto viene effettuato tra la fotografia presente sul passaporto od altro documento di riconoscimento, e la foto scattata al tornello;
- un altro confronto viene effettuato fra la foto scattata al tornello e un database di alcuni milioni di volti, messo a disposizione dalle autorità per la sicurezza degli Stati Uniti.

I varchi attivati nei vari aeroporti sono stati tenuti sotto controllo per parecchi mesi e l'organo ispettivo nazionale, GAO, ha analizzato i risultati di questa sperimentazione. In parallelo, il NIST (National istitute for standards and technology) ha effettuato un'analisi approfondita sul grado di efficienza ed efficacia del riconoscimento facciale, effettuato sul posto ed effettuato per confronto con un data base nazionale di volti. Come regola generale, NIST ha trovato che i ratei di falsi positivi erano da 10 a 100 volte meno accurati per alcune categorie demografiche. Specificamente per i ratei di falsi positivi, gli algoritmi erano assai meno accurati quando venivano confrontati volti di africani della costa occidentale o della costa indiana, indiani americani, africani americani e, in generale, la popolazione asiatica. Gli applicativi erano invece assai più accurati nell'analisi dei volti di soggetti appartenenti all'Europa centrale ed orientale. Per quanto riguarda i ratei di falsi positivi, il NIST ha trovato che gli algoritmi erano assai meno accurati analizzando i volti di donne, persone anziane e bambini. Un elemento veramente sorprendente, sempre rilevato dal NIST, è da ricondurre al fatto che gli algoritmi di riconoscimento facciale sviluppati in Cina avevano un rateo di falsi positivi assai più bassi, il che significa che erano assai più accurati, nel riconoscere i volti delle popolazioni asiatiche. Ciò significa che la qualità del riconoscimento facciale è solo dovuta allo sviluppo di appropriati algoritmi ed all'utilizzo di test condotti su una base sufficientemente allargata di volti. Non vi è infatti alcun motivo per il quale un software, sviluppato negli Stati Uniti, possa essere meno accurato, nel riconoscere un volto orientale, rispetto ad un software sviluppato in Cina.

Ricordo al proposito, che l'espressione "falso positivo" viene utilizzata quando un sistema di riconoscimento facciale stabilisce una correlazione tra due volti, che invece appartengono a due persone diverse. Al converso, si usa l'espressione "falso negativo" quando un sistema di riconoscimento facciale non è in grado di abbinare due immagini, che riprendono lo stesso soggetto.

Un altro aspetto molto interessante riguarda il confronto effettuato con il già menzionato data base di milioni di volti, messi a disposizione da vari enti degli Stati Uniti, come ad esempio le autorità che rilasciano le patenti di guida, le foto segnaletiche scattate dalle forze dell'ordine su soggetti imputati di vari crimini e via dicendo.

Uno studio approfondito ha messo in evidenza che una delle cause più frequenti di errore era da addebitare al fatto che la telecamera, posta al varco di sicurezza, non operava in condizioni soddisfacenti, da un punto di vista di contrasto della scena e luminosità ambientale, oppure che questi parametri non avevano valori costanti nell'ambito della giornata. Il secondo elemento, che portava ad uno scarso valore dei riconoscimenti facciali, era da imputare alla modesta qualità dell'immagine catturata al varco di sicurezza, rispetto all'elevata qualità delle fotografie scattate per il rilascio di patenti di guida o in fase di compilazione della scheda afferente a soggetti sospetti di atti criminali.

Da questi elementi si può trarre una ragionevole conclusione, che deve indurre gli sviluppatori di applicativi di riconoscimento facciale a svolgere in maniera un poco più accurata il proprio lavoro, concentrando la propria attenzione su un data base più allargato di individui da riconoscere.

Adalberto Biasiotti

www.puntosicuro.it