PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4395 di Mercoledì 30 gennaio 2019

Quanto sono intelligenti i software intelligenti?

Ormai gli applicativi intelligenti di analisi del segnale video sono sempre più diffusi. Un applicativo particolarmente attraente è quello che permette il riconoscimento facciale di persone fisiche.

Che gli applicativi intelligenti di analisi del segnale video rappresentino oggi un aspetto fondamentale, nel mettere a punto una qualsiasi strategia di messa in sicurezza di un insediamento, protetto da sistemi di videosorveglianza, è fatto non contestabile.

Per contro, da diverse parti si avanzano dubbi circa l'affidabilità di questi applicativi: un applicativo che ha attirato particolare attenzione riguarda l'applicativo di riconoscimento facciale.

Questo è motivo per cui il Dipartimento del commercio degli Stati Uniti, nel novembre 2018, ha condotto una approfondita analisi della capacità di riconoscimento di un certo numero di applicativi di riconoscimento facciale.

Il mercato oggi è pieno di aziende che offrono questi applicativi, ma non sono in realtà in grado di offrire un documento oppure una metodologia, che oggettivamente possa permettere di valutare l'affidabilità del riconoscimento. Ecco il motivo per cui il Dipartimento del commercio ha ritenuto opportuno affidare all'ormai famoso National Institute of Standard technology ? NIST, uno studio approfondito proprio sul livello di affidabilità di un certo numero di applicativi.

In sintesi, il rapporto afferma che la affidabilità di questi applicativi è cresciuta in maniera straordinaria negli ultimi tempi e che oggi un gran numero di applicativi si comporta molto meglio, rispetto agli algoritmi che venivano utilizzati solo qualche anno fa. Ad esempio, solo lo 0,2% di tutti gli algoritmi provati non ha raggiunto un livello soddisfacente, nel 2018, mentre nel 2014 solo il 4% dava risultati soddisfacenti.

Il motivo di questo drammatico e rapido miglioramento è legato all'utilizzo di reti neurali complesse, sviluppate dalle software house, che permettono di riconoscere i volti anche quando le immagini analizzate sono di bassa qualità.

Naturalmente, anche l'aumento della potenza di calcolo, a disposizione dei tecnici, ha contribuito a migliorare questi risultati.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[SWGDPR] ?#>

In questo test, il NIST ha valutato 127 algoritmi di identificazione facciale, sviluppati da 45 software house, distribuite in tutto il mondo. Alcuni applicativi hanno dato risultati assolutamente straordinari e ciò può indurre numerosi responsabili della sicurezza ad utilizzare questi applicativi, superando dei dubbi, che in passato erano a buon diritto presenti.

La metodologia di prova utilizzata da NIST è quella chiamata "uno contro molti". Ciò significa che gli sperimentatori hanno misurato l'abilità degli algoritmi di riconoscimento facciale di individuare il volto ricercato, in mezzo a una quantità di fotografie, in mezzo alle quali ve ne era una della persona ricercata, sperduta in mezzo a milioni di volti. Per questa ragione i tecnici di NIST hanno creato un database base di 26 milioni di volti, corrispondenti a 12 milioni di soggetti, per mettere alla prova l'algoritmo in esame. L'algoritmo viene valutato in maniera oggettiva, senza richiedere un particolare intervento da parte dell'azienda produttrice.

Una conseguenza diretta di questo drammatico miglioramento degli applicativi sta nel fatto che chi ha già in uso versioni precedenti deve provvedere ad un rapido aggiornamento, per sfruttare al meglio le nuove più avanzate prestazioni.

È bene comunque sottolineare che non è obbligatorio per un'azienda sottoporre il proprio algoritmo alle prove offerte da NIST e quindi, quando il produttore proclama le elevate qualità del proprio algoritmo, è bene chiedere in base a quali verifiche oggettive ed indipendenti questa elevata qualità è stata misurata.

Alcuni legislatori stanno addirittura pensando di rendere obbligatoria la verifica funzionale di questi applicativi, prima che possano essere utilizzati sul campo.

I difensori della protezione dei dati dei cittadini hanno però avanzato qualche perplessità, facendo presente che alcuni applicativi non sembrano essere sufficientemente evoluti per mettere in evidenza la differenza tra volti maschili di persone di razza bianca e afroamericani. Questo fatto potrebbe produrre dei problemi, quando l'applicativo viene utilizzato in indagini criminali, perché l'archivio dei volti di soggetti, che sono stati precedentemente schedati, è molto più ricco di volti di afroamericani, piuttosto che di persone di razza bianca.

In ogni modo, le previsioni di chi affermava che gli applicativi intelligenti di analisi del segnale video non potevano che migliorare sono state pienamente confermate e non v'è dubbio che questo miglioramento non è presente solo in applicativi di riconoscimento facciale, ma anche in applicativi di altra natura.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it