VareseNews

La professoressa che combatte i deepfake, Luisa Verdoliva a TrainING Varese

Pubblicato: Sabato 29 Maggio 2021

E se al posto di Jack Nicholson la *star* di Shining fosse stata Jim Carrey? Un utente di YouTube ha provato a immaginarlo, ricreando una celebre scena con un *deepfake*. Possibili grazie all'intelligenza artificiale, i ***deepfake*** sono video dove il volto di un personaggio è modificato per assomigliare a quello di un'altra persona, o in modo tale da fargli assumere espressioni e movimenti diversi dagli originali.

Strumenti spesso discussi, i *deepfake* appaiono in pubblicità e parodie, ma cosa succederebbe se si utilizzassero per diffondere video dove le persone più potenti al mondo pronunciano dichiarazioni false (ma estremamente realistiche)? Un grande rischio, ma per fortuna ci sono esperti che li combattono. **Luisa Verdoliva** insegna all'Università Federico II di Napoli e dirige diversi progetti di ***multimedia forensic*** con l'obiettivo di ideare tecnologie capaci di identificare immagini e video modificati. Venerdì 28 maggio ha raccontato il suo lavoro a **TrainING**, l'evento organizzato dall'**Ordine degli ingegneri di Varese** (tutti gli incontri si possono riguardare a questo link).

Che fosse per cambiare il ricordo di eventi del passato o per diffondere informazioni false, la pratica di modificare foto e video non è certo nuova. Se però un tempo era necessario un esperto e tante ore di lavoro, **con le ultime tecnologie produrre contenuti multimediali modificati è sempre più facile, veloce e alla portata di tutti**. Non solo, grazie a queste tecnologie si possono produrre anche vere e proprie "immagini sintetiche" di soggetti inesistenti.

Alla base della tecnologia dietro ai *deepfake* c'è il ***machine learning***: un sistema di apprendimento automatico, grazie al quale la macchina riesce a imparare in modo intuitivo attraverso l'analisi di grandi quantità di dati (in questo caso immagini o video), simulando il modo di imparare dell'essere umano. Per farlo la macchina sfrutta una rete neurale artificiale, che simula appunto i neuroni umani. Il passo successivo è il ***deep learning***: dove queste reti neurali sono organizzate in strati differenti secondo una gerarchia basata in base alla complessità dei concetti elaborati.

Grazie a queste tecnologie si possono produrre video e immagini modificate sempre più realistiche, tanto da essere indistinguibili per la maggior parte degli osservatori, velocemente e con la possibilità di diffonderle a un pubblico molto ampio attraverso il web.

Come riconoscere quindi *deepfake* e immagini modificate? La *multimedia forensic* ha tanti assi nella manica e a volte gli stessi strumenti utilizzati da chi produce foto e video falsi possono essere usati contro di loro. Si può infatti utilizzare l'intelligenza artificiale per realizzare programmi capaci di distinguere immagini reali da quelle modificate, sfruttando ad esempio i dati contenuti in grandi database. Un'altra soluzione può essere invece studiare il movimento del corpo della persona che appare nel video da analizzare. Se il modo di muoversi è troppo differente, allora ci sono buone probabilità che si tratti di un *deepfake*.

Alessandro Guglielmi
aleguglielmi97@gmail.com