Universitas Mercatorum

Università telematica delle Camere di Commercio Italiane

NOME PROGETTO

Metodi per la rilevazione di deepfake in scenari open-set e nella cinematografia

P.I.

Prof. Roberto Caldelli

CODIFICA

4-FIN/RIC

CLASSE FINANZIAMENTO

Avanzato

FASCIA

Ordinario

S.S.D.

ING-INF/05

GSD

09/IINF-05

S.C.

09/H1

STRUTTURA AFFERENZA

Facoltà di Scienze Tecnologiche e dell'Innovazione, Università Telematica Universitas Mercatorum

OBIETTIVI PROGETTO DI RICERCA

Il progetto VIDI-FAKE ha avuto come obiettivo lo studio e l'analisi delle metodologie basate su deep learning per la rilevazione di contenuti multimediali deepfake, immagini e video manipolati che ritraggono soggetti in contesti in cui non sono mai stati o che pronunciano frasi che non hanno mai detto. I metodi per rilevarli (basati su dominio spazio-temporale, dominio frequenziale e così via) si concentrano sull'identificazione di anomalie a livello di pixel, guardano il movimento anomalo delle labbra o l'ammiccamento incoerente, tentano di identificare ad esempio un'illuminazione incoerente, difetti nei tratti somatici e facciali e così via.

Per effettuare l'operazione di deepfake detection, si ricorre all'uso di rete neurali (e.g. CNN - Convolutional Neural Network) che richiedono grandi quantità di dati per l'addestramento composti sia da video (immagini) originali che ottenuti mediante tecniche deepfake. L'obiettivo del progetto è stato quello di studiare nuove soluzioni che consentano di migliorare le capacità di generalizzazione di queste metodologie in scenari applicativi più orientati al "mondo reale" quali la produzione multimediale su Internet e la cinematografia. In particolare, l'attività si è concentrata ad esempio sull'illuminazione delle superfici e la loro conseguente riflessione in relazione al posizionamento della camera. Si è analizzate se tale tipologia di feature potesse veicolare una sufficiente distintività tra immagini (video) reali e fake così da favorire la fase di rilevazione.

RISULTATI RAGGIUNTI

I principali risultati raggiunti sono i seguenti:

- Realizzazione di uno state-of-the-art della letteratura scientifica nel settore della rilevazione dei deepfake con particolare attenzione alle recenti soluzioni proposte in ambito video.
- Studio e sviluppo di una metodologia (composta da una serie di varianti implementative e applicative) basata sull'estrazione di feature relative al contesto di acquisizione del contenuto digitale (immagine/video).
- Sono stati realizzati tre articoli sottomessi ad importanti conferenze internazionali (vedi successiva sezione Produzione Scientifica).
- Realizzazione di un applicativo software (interfaccia dimostrativa) scritta in Python con libreria PyQt (vedi screenshot dell'interfaccia).

PRODOTTI DELLA RICERCA

Partecipazione a convegni nazionali

1. GTTI-MMSP (Thematic Meeting on Multimedia Signal Processing, Andalo (TN), 21-23/01/2024.
2. Open Day UNIFI, Firenze, 08/04/2024.
3. Salone del Libro, Torino, 11/05/2024.

Pubblicazioni su riviste scientifiche

L'attività di ricerca ha portato alla realizzazione di articoli sottomessi ad importanti conferenze internazionali inerenti tematiche quali l'artificial intelligence, image/signal processing, multimedia forensic and security.

1. "Temporal surface frame anomalies for deepfake video detection", A. Ciamarra, R. Caldelli, Del Bimbo, accepted for publication in 2nd Workshop and Challenge on DeepFake Analysis and Detection at CVPR 2024 (DFAD 2024) CVPR-W, 17-21 June, Seattle (USA).
2. "Inconsistencies in local camera surface frames to detect deepfakes", A. Ciamarra, R. Caldelli, A. Del Bimbo, submitted to ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec 2024), 24-26 June, Baiona, Spain.

Elementi per il consolidamento

1. "Detecting deepfakes through inconsistencies in local camera surface frames", A. Ciamarra, R. Caldelli, A. Del Bimbo, submitted to Security and Privacy of Machine Learning-based Vision Processing in Autonomous Systems at ICIP2024 (SPVis 2024), ICIP-W, 27-30 October, Abu Dhabi, UAE (under-review).