Intelligenza Artificiale e Analisi Visuale per la Cyber Security

Claudio Vairo, Giuseppe Amato, Luca Ciampi, Fabrizio Falchi, Claudio Gennaro, Fabio Valerio Massoli

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo" (ISTI)
Consiglio Nazionale delle Ricerche (CNR)
{nome.cognome}@isti.cnr.it

Abstract

Negli ultimi anni la Cyber Security ha acquisito una connotazione sempre più vasta, andando oltre la concezione di semplice sicurezza dei sistemi informatici e includendo anche la sorveglianza e la sicurezza in senso lato, sfruttando le ultime tecnologie come ad esempio l'intelligenza artificiale. In questo contributo vengono presentate le principali attività di ricerca e alcune delle tecnologie utilizzate e sviluppate dal gruppo di ricerca AIMIR dell'ISTI-CNR, e viene fornita una panoramica dei progetti di ricerca, sia passati che attualmente attivi, in cui queste tecnologie di intelligenza artificiale vengono utilizzare per lo sviluppo di applicazioni e servizi per la Cyber Security.

1 Attività Scientifica

Il gruppo AIMIR (Artificial Intelligence for Multimedia Information Retrieval) è un gruppo di ricerca dell'ISTI-CNR molto attivo nel campo della Cyber Security che ha acquisito una notevole esperienza nell'utilizzo di tecniche di intelligenza artificiale applicate allo sviluppo di applicazioni e servizi di Cyber Security. In particolare, vengono sfruttate, e in alcuni casi sviluppate, reti neurali convoluzionali (CNN) addestrate con approccio Deep Learning sia per classificazione diretta di media, sia per l'estrazione di descrittori visuali (features) dai media analizzati. Questi descrittori visuali vengono poi utilizzati per eseguire ricerche, classificazione, riconoscimento anche su larga scala (ad esempio ricerche per contenuti su milioni di immagini) usando tecniche di indicizzazione e classificatori. Il gruppo ha sviluppato applicazioni o servizi in diversi campi: monitoraggio di parcheggi, riconoscimento facciale, re-identificazione di persone, intrusion detection, sicurezza pubblica.

Nella sezione seguente, vengono brevemente presentati i progetti di ricerca in cui il gruppo è stato o è attualmente coinvolto.

2 Progetti

Energia da Fonti Rinnovabili e ICT per la Sostenibilità Energetica

È un progetto nazionale finanziato dal CNR nel contesto delle smart cities e dell'utilizzo dell'ICT per il risparmio energetico. Nell'ambito di questo progetto, il gruppo AIMIR ha sviluppato due applicazioni: l'applicazione Smart Parking e l'applicazione Smart Surveillance.

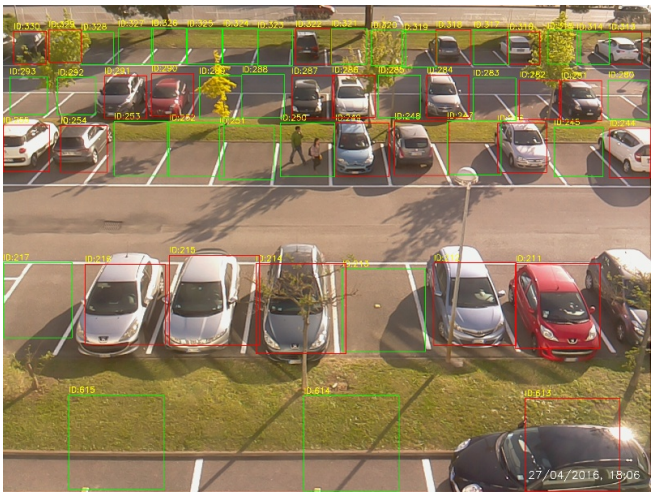

Figura 1: Monitoraggio visuale dello stato di occupazione degli stalli del parcheggio dell'area di ricerca di Pisa tramite l'applicazione Smart Parking.

L'applicazione Smart Parking [Amato *et al.*, 2016][Amato *et al.*, 2017] [Ciampi *et al.*, 2018] sfrutta delle telecamere intelligenti (cioè dotate di capacità di analisi dell'immagine acquisita), su cui è stata installata una CNN per monitorare visivamente lo stato di occupazione del parcheggio dell'area di ricerca di Pisa (vedi Figura 1). Sia le telecamere intelligenti che la rete neurale installata a bordo, sono state realizzate dal gruppo AIMIR. Una cosa importante da notare è che tutta l'elaborazione viene effettuata a bordo della camera. L'unica informazione trasmessa all'esterno, sia per motivi di traffico dati, che per motivi di privacy, è l'informazione testuale sullo stato di occupazione dei singoli stalli.

L'applicazione Smart Surveillance [Amato *et al.*, 2018a] [Barsocchi *et al.*, 2018] [Kavalionak *et al.*, 2018] è un sistema di video sorveglianza in grado di rilevare, tramite riconoscimento facciale, intrusioni di persone non autorizzate in ambienti monitorati. Il sistema sfrutta delle telecamere installate all'interno di alcuni uffici dell'area di ricerca di Pisa e una CNN pre-addestrata a riconoscere facce con tecniche

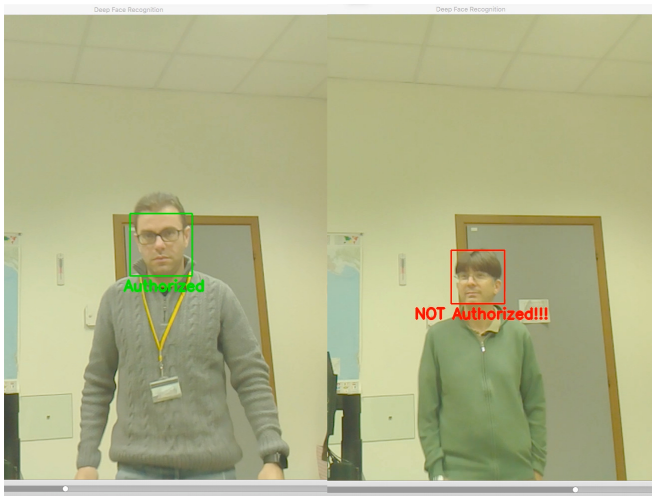

Figura 2: Intrusion Detection in ambiente monitorato tramite riconoscimento facciale.

di Deep Learning. In particolare, vengono acquisite delle immagini delle persone autorizzate, da cui vengono estratte, tramite la CNN, dei descrittori visuali che vengono associati alla persona e memorizzati. A tempo di esecuzione, quando una persona entra nell'ambiente monitorato, viene rilevato il suo volto da cui si estrae il relativo descrittore visuale che viene confrontato con quelli delle persone autorizzate. Se nessun match viene trovato, si genera una notifica di accesso non consentito (vedi Figura 2).

SECURE!
È un progetto che è stato finanziato dalla regione Toscana nell'ambito del programma POR CREO FESR 2007-2013, linea di intervento 1.5.a-1.6 che ha avuto l'obiettivo di fornire una piattaforma intelligente basata su tecnologie crowdsourcing e crowdsensing per la prevenzione di eventi critici nel campo della sicurezza pubblica-privata e della protezione civile.

CRAIM
Il Centro Ricerca e Analisi Informazioni Multimediali (CRAIM) istituito tramite una Convezione Operativa fra CNR e Dipartimento della Pubblica Sicurezza prevede lo sviluppo di strumenti e metodologie avanzate per l'analisi delle informazioni di natura testuale e multimediale provenienti da fonti aperte con l'obiettivo di far fronte ai nuovi scenari investigativi emergenti e di adattarsi ai rapidissimi mutamenti della "rete". Il gruppo AIMIR ha contribuito fornendo un sistema che è in grado di analizzare automaticamente e in tempo reale grandi quantità di immagini con lo scopo di rilevare volti e riconoscere se tra i volti rilevati ci sono quelli di persone che si vuole cercare e riconoscere. Il sistema sviluppato è anche in grado di processare flussi video anche di svariate ore, in modalità offline, generando dinamicamente un report con le eventuali similarità trovate che può essere analizzato mentre l'esecuzione procede. Inoltre, è stata svolta attività di ricerca per servizi di classificazione e tagging di luoghi e oggetti presenti nelle immagini, per riconoscere dei luoghi di interesse o segnalare immagini contenti oggetti specifici come ad esempio armi.

COST Action MULTI-FORESEE
Il gruppo AIMIR è attualmente coinvolto nella COST Action 16101 "MULTI-modal Imaging of FOREnsic SciEnce Evidence (MULTI-FORESEE) - tools for Forensic Science" che ha lo scopo di promuovere tecnologie innovative per il supporto all'analisi forense. Nell'ambito di tale Action, il gruppo AIMIR ha sperimentato diverse tecniche di face detection e sviluppato tecniche di estrazione dei descrittori visuali da immagini di volti, sia sfruttando reti neurali convoluzionali [Amato *et al.*, 2018b], sia sfruttando dei punti di interesse del viso (facial landmarks) come quelli che delimitano occhi, naso e bocca [Amato *et al.*, 2018c]. È stato inoltre costruito un dataset di volti di persone utilizzato per eseguire gli esperimenti di validazione delle tecniche proposte.

VIDEMO
Visual Deep Engines for MOnitoring (VIDEMO) è un progetto finanziato dalla regione Toscana che ha lo scopo di realizzare un sistema di sicurezza intelligente, interamente basato su reti convoluzionali, in grado di identificare volti basandosi sull'informazione estratta da foto anche a basse risoluzioni.

Riferimenti bibliografici

[Amato *et al.*, 2016] G. Amato, F. Carrara, F. Falchi, C. Gennaro, e C. Vairo. Car parking occupancy detection using smart camera networks and deep learning. In *Computers and Communication (ISCC), 2016 IEEE Symposium on*, pages 1212–1217. IEEE, 2016.

[Amato *et al.*, 2017] G. Amato, F. Carrara, F. Falchi, C. Gennaro, C. Meghini, e C. Vairo. Deep learning for decentralized parking lot occupancy detection. *Expert Systems with Applications*, 72:327–334, 2017.

[Amato *et al.*, 2018a] G. Amato, P. Barsocchi, F. Falchi, E. Ferro, C. Gennaro, G. R. Leone, D. Moroni, O. Salvetti, e C. Vairo. Towards multimodal surveillance for smart building security. In *Multidisciplinary Digital Publishing Institute Proceedings*, volume 2, page 95, 2018.

[Amato *et al.*, 2018b] G. Amato, F. Carrara, F. Falchi, C. Gennaro, e C. Vairo. Facial-based intrusion detection system with deep learning in embedded devices. In *2018 International Conference on Sensors, Signal and Image Processing (SSIP)*, pages 64–68. ACM, 2018.

[Amato *et al.*, 2018c] G. Amato, F. Falchi, C. Gennaro, e C. Vairo. A comparison of face verification with facial landmarks and deep features. In *International Conference on Advances in Multimedia (MMEDIA)*, pages 1–6, 2018.

[Barsocchi *et al.*, 2018] P. Barsocchi, A. Calabrò, E. Ferro, C. Gennaro, E. Marchetti, e C. Vairo. Boosting a low-cost smart home environment with usage and access control rules. *Sensors*, 18(6):1886, 2018.

[Ciampi *et al.*, 2018] L. Ciampi, G. Amato, F. Falchi, C. Gennaro, e F. Rabitti. Counting vehicles with cameras. In *SEBD*, 2018.

[Kavalionak *et al.*, 2018] H. Kavalionak, C. Gennaro, G. Amato, C. Vairo, C. Perciante, C. Meghini, e F. Falchi. Distributed video surveillance using smart cameras. *Journal of Grid Computing*, Oct 2018.