Alessia Saggese(*)

Analisi comportamentale basata su analisi video: dove?

Gli algoritmi di analisi video oggi disponibili sul mercato consentono di analizzare le immagini e di ottenere informazioni sui comportamenti degli oggetti che popolano la scena, ottenendo risultati che fino a qualche anno fa erano impensabili: ma cosa possono davvero rilevare? Quale affidabilità possono realisticamente garantire? E in che scenari applicativi possono essere utilizzati?

(*) Project Manager di A.I. Tech **www.aitech.vision**

Centinaia e centinaia di telecamere di sorveglianza che riprendono una scena in una metropolitana o in un aeroporto; un operatore umano addetto al monitoraggio di una smisurata quantità di monitor; un sistema intelligente capace di analizzare le informazioni acquisite e di segnalare situazioni di potenziale pericolo o semplicemente di accumulare informazioni in modo automatico per motivi statistici: uno scippo in aeroporto o una rissa in metropolitana; un'anziana signora che urla perché minacciata durante una rapina in banca; un incendio che divampa in una galleria o in lontananza su una montagna; un'autovettura che sfreccia a velocità eccessiva ignorando i limiti di velocità, un'altra che imbocca l'autostrada contromano minacciando l'incolumità degli altri veicoli o che effettua un'inversione ad U in prossimità di una curva pericolosa. La vetrina che attrae il maggior numero di visitatori all'interno di un centro commerciale e quella di fronte alla quale si fermano soprattutto le donne piuttosto che gli uomini. Questi e molti altri sono gli eventi che un sistema di video analisi intelligente oggi è in grado di rilevare. Tentiamo di distinguere i differenti scenari applicativi in cui i sistemi di video analisi, e in particolare l'analisi comportamentale, può essere proficuamente utilizzata. Tentiamo cioè di rispondere alla domanda "Analisi comportamentale basata su analisi video: dove?" Tre sono ad oggi i principali domini applicativi che possiamo identificare: la **business intelligence**, la gestione del **traffico** e il mondo della **security**. Entriamo più nel dettaglio al fine di comprendere meglio cosa si intende e quali sono i vantaggi che la video analisi può portare in ciascuno di questi settori.

Figura 1: Un esempio di funzionamento dell'applicazione di video analisi per il riconoscimento di fumi e incendi, AI-Fire (http://www.aitech-solutions.eu/ai-fire/): non appena è identificato un evento di interesse, un allarme (il rettangolo rosso) viene inviato e il relativo evento viene memorizzato per consentire una visualizzazione event-based del filmato.

SECURITY

Nel mondo della sicurezza l'elaborazione del video consente di estrarre numerosi eventi di interesse: dalla più tradizionale intrusione in aree non consentite al rilevamento di bagagli incustoditi in un aeroporto piuttosto che di spazzatura abbandonata sul ciglio della strada; dal rilevamento di incendi (**Figura 1**) al rilevamento di anomalie (persone, ad esempio, che camminano nella direzione opposta ad una folla). Il rilevamento automatico di tali eventi contribuisce ad un significativo cambiamento nel modo in cui l'operatore umano interagisce con i video: da una modalità time-based si passa infatti ad una event-based: senza un sistema di video analisi, infatti, l'operatore umano addetto al controllo dovrebbe visualizzare interamente il video, giorno e notte, ora dopo ora (time-based appunto), senza possibilità di trascurare anche solo un minuto di filmato, che potrebbe rivelarsi fondamentale. È ovvio come questa attività, oltre che noiosa, sia estremamente time consuming. Un approccio event-based stravolge il modo di approcciare al video: da un lato tali sistemi generano, in tempo reale, un allarme al verificarsi di un evento di interesse, in modo da risvegliare l'attenzione dell'operatore umano addetto al controllo. Dall'altro lato, consentono di visualizzare in sequenza i soli istanti di tempo associati a tutti

Figura 2: Due spire virtuali (una rossa e una blu, con differenti versi di percorrenza) disegnate dall'utente per il conteggio di veicoli: non appena un veicolo attraversa una spira nella direzione selezionata dall'utente, il contatore associato viene incrementato. Per maggiori informazioni sui sistemi di conteggio dei veicoli si può far riferimento ad AI-ROAD (http://www.aitech-solutions.eu/ai-road/), il prodotto di A.I. Tech per il monitoraggio del traffico.

gli eventi di interesse rilevati in precedenza, producendo così un notevole risparmio di tempo, e quindi una notevole riduzione nei costi di gestione degli impianti.

GESTIONE DEL TRAFFICO

In tale ambito l'analisi comportamentale è orientata a identificare quelle manovre dei veicoli che possono essere pericolose per gli altri veicoli o per i pedoni: l'attraversamento di una strada contromano, un'inversione a U o ancora una sosta in un'area proibita. Oltre che per il **monitoraggio** del traffico, gli applicativi di video analisi possono essere evidentemente utilizzati anche per la **caratterizzazione** del traffico: la stima del numero di veicoli (**Figura 2**), eventualmente divisi per tipologia (auto, motocicli, camion ecc), la stima della densità del traffico, o ancora lo stato dei posti liberi e occupati all'interno di un parcheggio. Anche in questo caso, è evidente come l'adozione di un sistema di video analisi permetta di conseguire una notevole riduzione dei costi di manutenzione, un incremento della flessibilità e una semplificazione dell'infrastruttura tecnologica della soluzione, non richiedendo alcun tipo di sensore aggiuntivo.

BUSINESS INTELLIGENCE

Tale termine si riferisce a tutti quei processi adottati nello sviluppo di un'attività produttiva per raccogliere dati ed analizzare informazioni strategiche. L'obiettivo è duplice: infatti, da un lato si intende analizzare la storia passata, al fine di comprendere gli elementi che hanno determinato le performance conseguite; dall'altro lato si desidera invece stimare le prestazioni future del business, attraverso analisi di serie storiche e/o mediante simulazione di diversi scenari. I sistemi di analisi video diventano pertanto fondamentali: l'operatore umano può visualizzare infatti in un'unica dashboard[1] ogni tipo di informazioni statistica a cui è interessato: il numero e la tipologia di persone (divise sulla base di sesso, età e razza) che popola il centro commerciale, le zone di principale interesse, i percorsi preferenziali e così via.

Sebbene ciascuno dei prodotti discussi in precedenza (dal conteggio delle persone al rilevamento dei bagagli incustoditi, dal rilevamento di manovre di veicoli pericolose al rilevamento di intrusioni in aree sterili) debba essere dotato di una propria intelligenza (e cioè di un algoritmo progettato per risolvere il particolare problema), è evidente come la maggior parte degli applicativi sia accomunata da una base comune, o meglio da un "**come**" comune: è necessario cioè che gli oggetti in movimento siano correttamente identificati e che le loro traiettorie siano correttamente estratte: hanno cioè bisogno di utilizzare algoritmi di detection e tracking, trattati nei precedenti numeri di questa rubrica sulla FormAZIONE! Ovviamente, migliori sono tali algoritmi di basso livello (detection e tracking appunto), migliori saranno le prestazioni degli algoritmi di più alto livello, orientati cioè a risolvere i particolari problemi. Facciamo un semplice esempio per chiarire meglio tale affermazione, applicato

[1] Il termine dashboard si riferisce a quelle applicazioni in cui tutti i dati di interesse confluiscono e sono fruibili attraverso un'interfaccia unificata e di semplice uso. Un esempio di dashboard è AI-Glance (http://www.aitech-solutions.eu/ai-glance/), il cruscotto interattivo realizzato da A.I. Tech.

al problema del riconoscimento delle intrusioni. L'obiettivo di un sistema antintrusione è riconoscere tutte (e sole) le intrusioni di una particolare classe di oggetti (tipicamente persone) all'interno di una regione definita dall'utente, quella che viene tipicamente chiamata area sterile. Un passaggio dell'oggetto di interesse per un certo periodo di tempo all'interno dell'area sterile deve generare un allarme; allo stesso tempo, il movimento di un oggetto non di interesse (ad esempio un gatto che si muove per casa) non deve generare alcun allarme. Per distinguere le due tipologie di oggetti (persona e gatto) la fase di detection è evidentemente fondamentale: se la detection non identificasse correttamente tutte le parti di una persona (ma magari solo un piccolo pezzo), un algoritmo di video analisi, seppur intelligente, sarebbe portato a confondere la persona con il gatto e quindi a non generare un allarme sebbene a transitare nell'area sia la persona (**Figura 3**). D'altro canto, un algoritmo di tracking poco affidabile che non sia in grado di estrarre in modo affidabile l'intera traiettoria della persona porterebbe il sistema antintrusione a sbagliare, poiché analizzerebbe in modo separato i due pezzi di traiettorie, la cui lunghezza (e quindi evidentemente il cui tempo di persistenza all'interno della regione) potrebbe non essere sufficientemente elevato per rilevare l'intrusione e quindi per generare l'allarme.

IN CONCLUSIONE

Abbiamo visto come i sistemi di video analisi finalizzati all'analisi comportamentale si stanno oggi affermando sul mercato nei diversi settori applicativi, dal monitoraggio e la caratterizzazione del traffico alla sicurezza fino alla business intelligence. Ciò è sicuramente dovuto alla crescente affidabilità di tali prodotti, sviluppati sempre più spesso in collaborazione con laboratori universitari o centri di ricerca che fanno della ricerca e dell'innovazione tecnologica la loro mission. Adesso è il tuo turno. Non ti resta che fidarti di tali sistemi e scoprire i benefici che ne puoi ricavare. Provare per credere.

Figura 3: Uno dei fotogrammi estratti dal dataset iLIDS (https://www.gov.uk/imagery-library-for-intelligent-detection-systems). Sulla sinistra vi è un esempio del sistema antintrusione AI-INTRUSION (http://www.aitech-solutions.eu/ai-intrusion/) che funziona correttamente: la persona viene rilevata e l'allarme antintrusione, come visibile dal rettangolo rosso, viene generato. Al contrario, nel fotogramma a destra vi è un esempio di algoritmo antintrusione che non funziona correttamente a causa di un errore nella fase di detection: la persona viene infatti spezzata in due parti (identificata ciascuna dal rettangolo bianco), ma nessuna di tali parti assume la forma di una persona. Pertanto, l'allarme non può essere generato.