INTRODUZIONE ALLA *IMAGE / VIDEO FORENSICS*

di Sebastiano Battiato e Fausto Galvan

❶ *Introduzione*

La crescente diffusione di dispositivi di *imaging* a basso costo e la conseguente disponibilità di grosse quantità di foto e filmati digitali, rende l'attività investigativa e di verifica su tali tipologie di dati sempre più frequente. A tale scopo risulta fondamentale riuscire ad individuare con esattezza modalità di analisi e di studio di tali reperti al fine di non lasciare nulla di intentato nella ricerca di fonti di prova spesso decisive. Le potenzialità indotte dall'uso consapevole delle informazioni contenute in un segnale digitale (immagine/video, ecc.) sono notevoli a patto però di conoscere i fondamenti tecnici di base della disciplina. **L'*Image/Video Forensics* comprende tutte le attività di analisi delle immagini (e dei video) svolte oramai prevalentemente in ambito digitale, volte ad estrapolare dati e informazioni ad uso forense**.

Con il termine *Image / Video Forensics* ci si riferisce ad una specifica area della *Digital Forensics* che si occupa dello studio e dell'analisi di immagini (e di video) per la loro validazione e utilizzo in ambito forense. Questa disciplina, che ha visto la luce negli ultimi anni del secolo scorso e la cui continua evoluzione segue i ritmi incalzanti dello sviluppo tecnologico odierno, può essere a sua volta divisa nei seguenti filoni specifici[(1)]:

- ***Image Forgery Identification***: identificazione di presunte manipolazioni, ovvero di inserimento o di cancellazione di particolari per fini fraudolenti (es. alibi, contraffazione, ecc.);
- ***Image Source Identification***: individuazione della sorgente che ha generato l'immagine, sia dal punto di vista del modello (tipo di macchina fotografica) sia dal punto di vista del tipo di apparecchiatura (scanner, fotocamera);
- ***Image Reconstruction***: restauro di immagini deteriorate al fine di identificare, anche parzialmente, il contenuto originale e/o recuperare informazioni;
- ***Video Analysis***: analisi dinamiche o comportamentali volte ad esempio ad individuare comportamenti sospetti oppure l'abbandono/furto di oggetti;
- **Ricostruzione 3D**: estrazione delle informazioni tridimensionali contenute all'interno della scena per ricavare misure o grandezze di riferimento (l'altezza di un individuo, oppure la velocità di un mezzo).;
- **Steganografia**: individuazione di informazioni nascoste all'interno di un'immagine, ad esempio mediante la modifica del bit meno significativo nel numero che definisce il colore di un pixel, ecc.

Sebbene i primi due settori abbiano assunto particolare rilevanza nella comunità scientifica di riferimento, nondimeno gli altri ambiti sono ugualmente rilevanti sia nel campo della sicurezza (es. Video Sorveglianza) che a fini investigativi, per così dire più tradizionali, quando risulta necessario mettere in evidenza particolari ed informazioni contenute nell'immagine. Come ampiamente evidenziato[(1,5)], tali metodologie di analisi possono essere usate per estrarre le relative evidenze forensi solo se l'informazione è effettivamente presente (sia pur in maniera labile e appena accennata come evidenziato ad esempio in figura 1), ma non possono "inventarsi" dei dati di qualsiasi natura qualor-

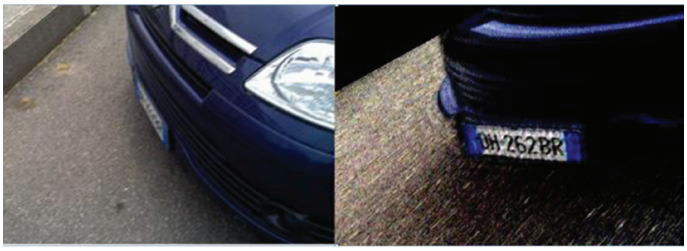

Figura 1 – Esempio di rettificazione. Si può apprezzare come tale trasformazione prospettica evidenzi l'informazione relativa alla targa dell'autovettura, altrimenti non visibile, sebbene presente nel dato originale.

questi non ci siano. Un esempio in questo senso (purtroppo ancora molto frequente) riguarda immagini acquisite da dispositivi di videosorveglianza, che, pur registrando l'evento criminoso, risultano inutilizzabili a causa della scarsa qualità del sistema di ripresa (scarsa risoluzione, rumore, ecc.).

❷ *Fondamenti di Elaborazione delle Immagini*

Le immagini digitali possono essere rappresentate come un segnale discreto bidimensionale (e cioè rappresentabile mediante dei numeri finiti e con una certa precisione detti *pixels*) in grado di replicare la sensazione percettiva legata alla visione di una scena reale[(3)]. Diversamente da una macchina fotografica tradizionale, una fotocamera digitale utilizza, al posto della pellicola, un sensore costituito da milioni di elementi fotosensibili in grado di catturare l'immagine e trasformarla in un segnale elettrico di tipo analogico. Gli impulsi elettrici catturati dal sensore, la cui intensità varia a seconda della luce che colpisce il singolo fotorecettore, vengono convertiti e trasformati in un flusso di dati digitali. Questo procedimento è detto campionamento spaziale e determina la cosiddetta "risoluzione" degli apparati di acquisizione, che viene solitamente misurata in *MegaPixels*. All'aumentare della risoluzione corrisponde una migliore accuratezza nella rappresentazione dei dettagli. Prima che la luce della scena fotografata raggiunga il sensore, essa attraversa un sistema di lenti e di filtri che consente ad ogni *pixel* di catturare informazioni riguardanti ciascuna delle tre componenti di colore (rosso-verde-blu) in cui la luce della scena da acquisire viene scomposta.

Nel passo successivo, per ricostruire il colore originale, il *software* interno della fotocamera ricalcola le componenti primarie su ogni *pixel* usando varie strategie ed algoritmi (interpolazione del colore o *demosaicing,* bilanciamento del bianco, correzione gamma) e vari altri metodi di ottimizzazione del colore. Infine l'immagine digitale è salvata sul dispositivo di memorizzazione della fotocamera nel formato selezionato dall'utente (tipicamente il JPEG) con opportuni parametri di compressione.

I video digitali sono una naturale generalizzazione e possono essere definiti o come un segnale discreto che attua un campionamento temporale della scena reale (ovvero ad ogni istante la scena è "fotografata") oppure attraverso la successione di istantanee appositamente composte. Tale sequenza è quindi costituita da una serie di *frame*, cioè dalle singole immagini

che compongono il video, dette anche fotogrammi. Oltre che dalla necessità di contenere le dimensioni dei dati, al fine sia di memorizzarli che di trasmetterli, la compressione nel caso di sequenze video trae origine dalla necessità di garantire la riproduzione delle sequenze in maniera adeguata. Il *framerate* o *frame* (o immagini) per secondo, è l'unità di misura della frequenza di visualizzazione delle singole immagini che compongono il video. I parametri fondamentali da tenere in considerazione in quanto consentono (o meno) all'analista di estrarre le relative evidenze forensi sono: la risoluzione spaziale (che corrisponde al livello di dettaglio), il *framerate* (l'unità di misura della frequenza di visualizzazione delle singole immagini) ed il livello di compressione.

❸ *Contraffazioni: definizioni ed esempi*

Figura 2 - (Maggio 2011). Nelle ore successive alla morte di Osama Bin Laden si diffuse nella rete l'immagine di destra, presentata come prova dell'avvenuto decesso del terrorista. Poco dopo si apprese che si trattava di un fotomontaggio, ottenuto unendo la parte sottostante dell'immagine di sinistra, resa lievemente più scura, con la parte sovrastante dell'immagine centrale.

Come già accennato uno dei temi sicuramente più rilevanti del settore riguarda il trattamento e la verifica di autenticità di reperti multimediali. Contrariamente a quanto si può immaginare, i primi esempi documentati di manipolazione delle immagini risalgono al 1860, cioè solo pochi decenni dopo la nascita della fotografia. A differenza di allora, la cui esecuzione era ad esclusivo appannaggio di pochissimi esperti, con l'avvento delle fotocamere digitali, videocamere e sofisticati *softwares* di *editing* fotografico, la manipolazione di immagini digitali sta diventando sempre più un'operazione alla portata dell'utente comune. Principalmente, le contraffazioni possono essere classificate in tre categorie:

1. elaborazione dell'immagine mediante metodi di *computer* -grafica (es. oggetti o particolari generati/modificati artificialmente);
2. alterazione del significato dell'immagine, senza modificarne il contenuto (es. variazioni cromatiche e/o di luminosità, *resizing*);
3. alterazione del contenuto dell'immagine, inserendo (es. copia e incolla) o eliminando (es. ritaglio, cancellazione) parti significative.

La figura 2 mostra un esempio di "*digital forgery*" realizzato e scoperto a mezzo *web*. Per un elenco più completo ed aggiornato si rimanda alle note **(1)** e **(2)**. Nell'ambito dei procedimenti penali, la presenza di immagini e video non autentici o semplicemente montati in modo "accorto" assume particolare rilevanza, in quanto tramite tali strumenti possono a volte essere creati alibi apparentemente inattaccabili.

❹ *Tecniche per l'Identificazione delle Contraffazioni*

Le tecniche utilizzate per individuare le manipolazioni (o *forgery*) si dividono essenzialmente in due categorie: metodi attivi e passivi. I metodi attivi prevedono l'inserimento di una segno distintivo (una sorta di "firma" detta anche *watermarking* digitale) nel dato digitale al momento della relativa acquisizione da parte del dispositivo. Uno dei problemi di tale approccio è costituito dalla difficoltà di inserimento in modo univoco in tutti i dispositivi esistenti mediante uno *standard* unico, oltre al fatto che tali "firme" si sono dimostrati poco resistenti a tentativi di rimozione fraudolenta.

Al contrario, i metodi passivi sfruttano le alterazioni del contenuto statistico dell'immagine provocate dalle contraffazioni, e a sua volta si suddividono **(1,4)** in:

- **tecniche *pixel-based***: che individuano anomalie statistiche a livello di *pixels*;
- **tecniche *format-based***: che fanno leva sulle correlazioni statistiche contenute nelle tecniche di compressione "*lossy*" (con perdita di dati);
- **tecniche *camera-based:*** che sfruttano gli artefatti introdotti in generale dall'*hardware* o dal *software* che interviene durante le varie fasi della formazione dell'immagine;
- **tecniche *physically-based***: che mettono in evidenza le incoerenze tra le caratteristiche fisiche delle immagini reali ed i modelli fisico-matematici che li riproducono;
- **tecniche *geometric-based***: che sfruttano le nozioni della teoria della formazione dell'immagine per confrontare misure fisiche di oggetti reali e le loro posizioni rispetto alla fotocamera.

❺ *Conclusioni*

Le tecniche d*i Image / Video Forensics* costituiscono sicuramente un ulteriore strumento di indagine a disposizione degli investigatori per poter estrarre ed inferire, utili informazioni dalle immagini (e dai video) digitali**(5)**. Sono stati anche introdotti alcuni concetti di base, necessari per poter comprendere i dettagli tecnici degli algoritmi presentati, con particolare riferimento alle manipolazioni (o *forgery*). Per essere in grado di recuperare o far emergere delle evidenze di prova è comunque necessaria una adeguata competenza specifica che richiede uno studio sistematico dei fondamenti della teoria dell'elaborazione delle immagini e dei video digitali. Gli stessi *softwares* oggi esistenti, di supporto al lavoro degli investigatori, non riescono per forza di cose ad automatizzare in maniera sistematica ed efficiente tali operazioni e richiedono l'ausilio di utenti esperti. ©

NOTE

1. S. Battiato, G. Messina, R. Rizzo – "Image Forensics. Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive" Chapter in IISFA Memberbook 2009.
2. http://www.cs.dartmouth.edu/farid/research/digitaltampering/.
3. R.C. Gonzalez, R.E. Woods,"Elaborazione delle Immagini Digitali" - Terza edizione - Pearson - Prentice Hall Italia, 2008.
4. J.A. Redi, W.Taktak, J.L. Dugelay - " Digital image forensics: a booklet for beginners " Multimedia Tools Application - 2011, 51:133-162.
5. S. Battiato, G.M. Farinella, G. Puglisi - " Image/Video Forensics: Casi di Studio " Chapter in IISFA Memberbook 2011.◊