Tra le conseguenze che l'informatizzazione globale ha sul mondo delle investigazioni, vi è il sempre maggior utilizzo di strumenti digitali per la creazione di alibi. In questo contesto, le immagini e/o i video opportunamente modificati sono molto sfruttati. Al fine di rivelare le manipolazioni dei documenti visivi, oltre ai metodi forniti dalla Image Forensics "classica" vengono qui considerati, in una visione più globale del fenomeno falsificatorio, gli approcci che analizzano la possibile presenza di falsi originali. Alcuni esempi tratti da casi reali completano la trattazione.

Sebastiano BATTIATO, professore associato in Informatica presso l'Università di Catania, insegna "Multimedia, Computer Vision e Computer Forensics" presso il Corso di Laurea in Informatica. Esperto di multimedia e imaging applicato alle investigazioni digitali.

Fausto GALVAN è Maresciallo Ordinario dell'Arma dei Carabinieri effettivo ad un reparto territoriale. Attualmente è dottorando in Informatica presso l'Università degli Studi di Udine.

VERIFICA DELL'ATTENDIBILITÀ DI UN ALIBI COSTITUITO DA IMMAGINI O VIDEO

di Sebastiano BATTIATO e Fausto GALVAN

❶ *Introduzione*

La mole di dati informatici prodotti ed utilizzati quotidianamente, dalla cosiddetta generazione dei "nativi digitali"[(1)] e non solo, è davvero notevole. L'ambito investigativo non fa eccezione: in pochissime indagini, al giorno d'oggi, non si presenta la possibilità di esaminare tracce digitali lasciate dall'indagato o dalla vittima, anche se il reato per cui si procede è apparentemente avulso dal contesto informatico[(2)].

Sebbene l'idea di crearsi un alibi da parte del colpevole di un crimine non rappresenti una novità, l'insieme degli strumenti per poter ottenere questo obbiettivo si arricchisce alla stessa velocità con la quale evolvono le "armi" tecnologiche in mano agli investigatori. Le descrizioni a riguardo non mancano[(3):(6)], ma in questo lavoro dedichiamo l'attenzione esclusivamente alle possibili operazioni di depistaggio effettuate mediante immagini. Per farlo ci avvaliamo di un caso di studio costruito *ad hoc*, che però ben si presta ad introdurre la relativa tematica.

❷ *Case study: verifica di alibi costituito da immagine catturata con uno smartphone*

Allo scopo di provare la propria innocenza, un sospettato consegna agli investigatori una immagine che lo ritrae in una località diversa da quella in cui è avvenuto il crimine di cui è accusato. Nel produrre l'alibi l'interessato precisa che la data e l'ora di scatto sono concordi con quelle dell'evento, e suggerisce che dall'esame dell'immagine sarà possibile ottenere riscontro alla sua tesi. L'interessato asserisce inoltre che lo scatto è stato effettuato con l'apparato fotografico di uno *smartphone*, che pone nella disponibilità degli inquirenti.

Appare quindi indispensabile rispondere ai seguenti interrogativi:

- Cosa si può dire in merito all'originalità del *file* che contiene l'immagine?
- Cosa si può dire in merito all'originalità della scena riprodotta?
- Dove sono reperibili e quale grado di affidabilità hanno le informazioni relative alla data ed ora di scatto, od altre di interesse per l'indagine?

Alcune preliminari tecnici di base si rendono necessari.

❸ *Diversi tipi di falsificazione*

Per manipolare il contenuto di una immagine e quindi comunicare un messaggio distorto, si possono utilizzare le classiche operazioni di "copia-incolla", ridimensionamento, variazione di colore, taglio di particolari, ecc. Queste operazioni coinvolgono l'uso di *software* di *editing* che modificano l'immagine digitale, lasciando al contempo tracce più o meno evidenti del loro utilizzo[(7)]. Nel nostro caso di studio si dovrà quindi intervenire attraverso l'utilizzo di tecniche di *Image Forensics* con l'obiettivo di smascherare le eventuali "*digital forgeries*". Ma se l'esito di questi accertamenti dovesse essere negativo, il lavoro non potrà dirsi concluso. Bisogna infatti esaminare anche la possibilità che ci si trovi di fronte ad uno dei cosiddetti **falsi originali**. Si tratta di immagini che sono portatrici di un messaggio falso, pur essendo costituite dall'esatta sequenza di bit prodotta dall'apparato al momento dell'acquisizione.

La problematica dei falsi originali merita una trattazione separata rispetto alla *Image Forensics* "moderna", sia per le differenti procedure realizzative, sia per i diversi approcci necessari al loro smascheramento (fanno eccezione, come vedremo, i metodi *physically based* e *geometric based*[(7)]), che spesso sono più simili a quelli dell'investigatore dell'era "pre-digitale". Tra gli strumenti utilizzabili per una analisi completa di un documento visivo, sia esso un video od una immagine still, si segnala ad esempio il *software* Authenticate[(8)] che offre la possibilità di evidenziare in un unico *framework* diversi aspetti legati alla presunta integrità del dato di *input*[(9)].

❹ *I falsi originali*

Come sopra anticipato, si parla di falsi originali quando il file che contiene l'immagine od il video, pur veicolando un messaggio errato è costituito dall'originale sequenza di bit prodotti dal dispositivo di acquisizione. In questo caso, la falsa informazione che caratterizza il documento visivo è stata inserita prima dello scatto o della ripresa che stiamo esaminando. Questo risultato può essere ottenuto seguendo due strade:

1. **Immagine ricatturata**: la foto viene acquisita dopo essere stata alterata. In fig.1 vengono riportati i passaggi tecnici ne-

cessari per compiere tale operazione: ad una foto originale, ad esempio acquisita con una fotocamera, sono stati aggiunti mediante una classica operazione di copia-incolla alcuni particolari, provenienti da una seconda immagine, magari acquisita con un diverso dispositivo. Il risultato viene successivamente stampato prima di essere nuovamente convertito in formato digitale mediante fotocamera o *scanner*. In tale situazione molte delle tecniche di *Image Forensics* non sono di alcun supporto, dato che l'immagine non conterrà tracce delle modifiche precedenti l'ultima conversione.

Una analisi visiva più sofisticata potrà comunque venire in aiuto degli investigatori. Ad esempio, stimando in tutti i soggetti ripresi la direzione di provenienza della luce, ed evidenziando le incoerenze negli esiti di questo controllo, è talvolta possibile ottenere risultati soddisfacenti (metodi di *Image Forensics physically based*[10]). Un altro tipo di analisi utilizzabile è la ricerca di inconsistenze nella geometria della scena (metodi di *Image Forensics geometric based*[11]): due soggetti diversi che all'interno della stessa immagine fanno riferimento a due diversi punti di fuga testimoniano una possibile manomissione.

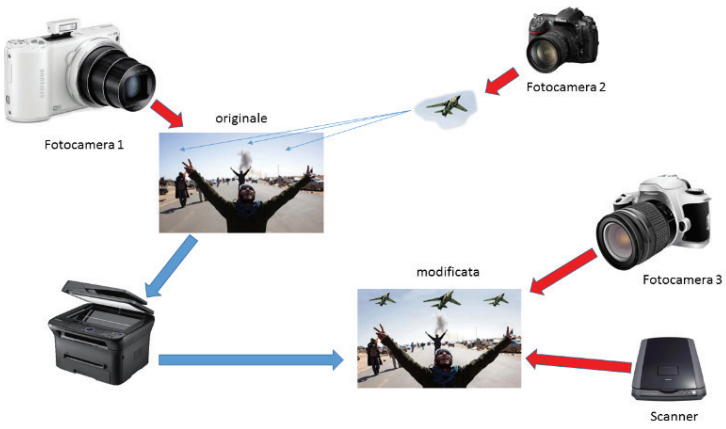

Fig.1: schema di formazione di una immagine ricatturata: una immagine viene modificata (nel caso in figura aggiungendo alcuni particolari), stampata e riacquisita mediante scanner o fotocamera. Le tracce dell'immagine originale non sono recuperabili, a meno di errori in fase di composizione.

2. **Messa in scena**: l'immagine in questo caso non ha subito alcuna alterazione, ma raffigura una scena ricreata (potremmo dire "recitata") per trasmettere il falso messaggio. Ad esempio l'immagine in fig.2 (effettuata durante una pause delle riprese del film "Lo Squalo"[12]) non rappresenta certo un fatto realmente accaduto.

Nessuna analisi sulle statistiche dell'immagine potrà permetterci di smascherare la truffa, ed in questo caso non otterremo nulla nemmeno dalla ricerca di eventuali inconsistenze di tipo geometrico e/o di illuminazione. Questo perché non si è operato sul documento, ma a monte della creazione dello stesso. Si dovrà allora cercare di accertare la consistenza di altri particolari. Ad esempio, per scene in esterno, ci possiamo domandare:

- → Il tempo atmosferico del giorno ed ora a cui dovrebbe riferirsi l'immagine (rilevabile da opportune raccolte, anche *on line*[13]) è coerente con quello visibile nella scena?
- → La direzione dell'ombra (ad es. proiettata al suolo dalle persone) in quella posizione geografica, è coerente con l'ora e la data comunicati?
- → I particolari riprodotti (ad es. l'abbigliamento dei soggetti ripresi, il periodo storico di commercializzazione degli oggetti presenti nella scena) sono in sintonia con la data comunicata?

Fig.2: una messa in scena è ottenuta fotografando una situazione creata ad hoc in base alle esigenze. In questo caso i metodi classici di Image Forensics non sono di alcuna utilità in quanto l'immagine in questione è in tutto e per tutto l'originale.

Oltre a ciò sono senz'altro utili le informazioni raccolte con i metodi di *intelligence* classici.

5 *L'utilità dei metadati*

L'*header* del *file* che contiene l'immagine (fig.3), è costituito di solito da informazioni preziose e di facile consultazione[14], i cosiddetti *metadati* [15].

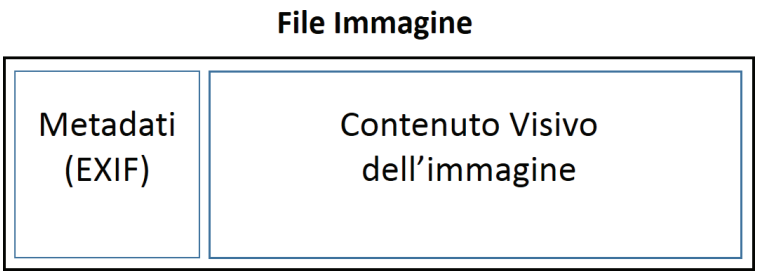

Fig.3: Un file JPEG è un particolare "contenitore" composto da una serie di 0 ed 1 organizzati in modo da poter distinguere una parte iniziale in cui sono conservati (con un livello di dettaglio variabile a seconda versione del software) i dati relativi allo scatto ed alle modalità di compressione. Di seguito si trovano le informazioni in merito al contenuto visivo della scena ripresa. L'assenza dei metadati è un segnale della manomissione del file.

Tra le varie informazioni reperibili, la data e l'ora dello scatto possono rivelarsi preziose sia per negare che per confermare una tesi. La loro assenza ad esempio, di per sé costituisce un primo segnale che può farci dubitare dell'originalità del *file* in esame, dato che tutti i dispositivi di acquisizione incapsulano *metadati* nel *file* prodotto. Anche le informazioni relative alla georeferenziazione (quando presenti) sono di grande utilità: le fotocamere provviste di modulo GPS infatti, inseriscono nei *metadati* le coordinate del luogo in cui è stata scattata l'immagine, spesso all'insaputa dell'utilizzatore che raramente è al corrente di tutte le caratteristiche del proprio apparato. È inutile dire quale valore abbiano queste informazioni

nel contesto di una indagine, una volta verificata la loro autenticità. A questo proposito è bene sottolineare che, a dispetto della loro indubbia utilità, l'attendibilità dei *metadati* è molto bassa. Infatti numerosi *software* (anche gratuiti) permettono di modificarli e di inserire facilmente al loro posto l'informazione voluta. Se l'assenza di dati EXIF è prova di manomissione quasi certa, la loro presenza va quindi attentamente valutata ed i dati estratti devono essere sempre incrociati con altre risultanze investigative.

Ad esempio, nel *case study* sopra citato sarebbe stato possibile verificare con precisione l'affidabilità di alcune informazioni ricavate dei *metadati* effettuando un controllo incrociato con le risultanze prodotte dai tabulati telefonici (ricordiamo che l'immagine proveniva da un cellulare). La posizione geografica della cella che aveva in gestione il telefono nell'orario in cui è stata scattata la foto, ad esempio, sarebbe potuta servire per accertare se l'apparato si trovasse nel luogo dichiarato dal proprietario.

6 Uno sguardo ai casi reali

Di seguito riportiamo due casi di studio tratti da situazioni reali. Nel primo caso potremo apprezzare l'effetto dell'unione tra acume investigativo e conoscenze tecniche, nel secondo vedremo come talvolta nemmeno queste ultime permettano di rispondere con certezza alle domande poste.

a) Validazione di alibi costituito da filmato contenuto in una videocassetta tipo MiniDV

Nell'ambito di un procedimento penale veniva prodotta dalla difesa una videocassetta, tipo MiniDV, in cui l'imputato per un grave delitto era ripreso mentre, proprio il giorno dell'accadimento del fatto, festeggiava una ricorrenza con i parenti. Per dirimere alcuni dubbi in merito all'originalità del filmato, il Giudice incaricava un perito di analizzare la fonte di prova. Esaminiamo gli accertamenti compiuti.

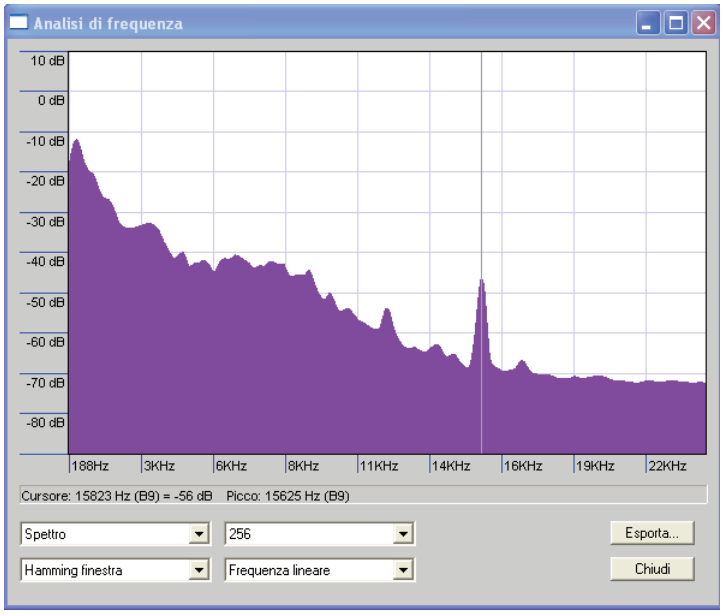

Fig.4: schermata prodotta dall'analisi dello spettro di frequenza del segnale audio del filmato. Il picco a 15625 Hz, caratteristico di un segnale di tipo analogico ma anomalo in un segnale audio digitale, pone un interrogativo sulla affidabilità del filmato.

I *metadati* "classici" del filmato in oggetto sono stati analizzati attraverso opportuni strumenti *software*[16].

Parte di questa analisi, diretta ad individuare eventuali errori di codifica, ha permesso inoltre di appurare che il video contenuto nel supporto era suddiviso in due parti, caratterizzate da una differente codifica audio. E' stata quindi analizzata la traccia della parte interessata. Lo spettro in frequenza (fig.4) evidenziava un picco localizzato a 15625Hz corrispondente alla frequenza di riga del segnale televisivo analogico (625 linee x 25 q/sec). Ma il video era stato consegnato in formato digitale.

Il segnale video presentava un'ulteriore anomalia visibile in tutti i fotogrammi della parte di filmato sotto analisi: la prima linea era completamente nera, mentre nella metà sinistra della seconda si evidenziava un tratteggio bianco e nero (fig.5). Si trattava del codice WSS, utilizzato da alcuni dispositivi che trasmettevano video analogici in formato PAL per comunicare informazioni.

Fig.5: le prime due righe del filmato presentano un pattern caratteristico della codifica analogica, che non dovrebbero essere presenti in un video digitale.

Un dispositivo digitale non genera questo tipo di linee in quanto le informazioni sono già presenti nei *metadati* e non è necessario aggiungerle al segnale. Sollevando l'etichetta adesiva presente su un lato della cassetta, si appurava inoltre che il codice riferito al lotto di produzione del supporto risultava abraso. Tale risultanza ha insospettito ulteriormente gli investigatori, spingendoli a controllare presso la casa produttrice l'anno di fabbricazione della videocassetta. La risposta è stata di notevole impatto sull'esito degli accertamenti, perché si è appreso che il modello di videocassetta presentata era stata posta in commercio due anni dopo l'evento per cui si procedeva.

Ciò permetteva di concludere che il video contenuto nella cassetta MiniDV consegnata non poteva essere stato registrato su quel supporto nel giorno e nell'ora sostenuti dalla difesa.
È importante citare questo episodio in quanto evidenzia come, al di là di tutti gli accertamenti tecnici esperiti, la vicenda si sia risolta in modo definitivo grazie ad uno spunto investigativo "classico" (tentativo di verificare il lotto di produzione della cassetta – verifica della asportazione di tale riferimento – accertamento presso la casa produttrice).

b) Image Enhancement e Biometria per la validazione di un alibi video

Un detenuto agli arresti domiciliari era sospettato di uscire abitualmente dalla propria dimora per andare a svolgere attività illecite.

Per avvalorare tale ipotesi veniva acquisito il filmato proveniente da una telecamera, precedentemente posizionata di fronte all'ingresso dell'abitazione del soggetto. Nelle riprese effettivamente si poteva notare una persona che usciva dallo stabile in orario concorde a quello del reato per cui si procedeva, ma (come purtroppo spesso accade) la qualità ed il posizionamento dell'apparato di

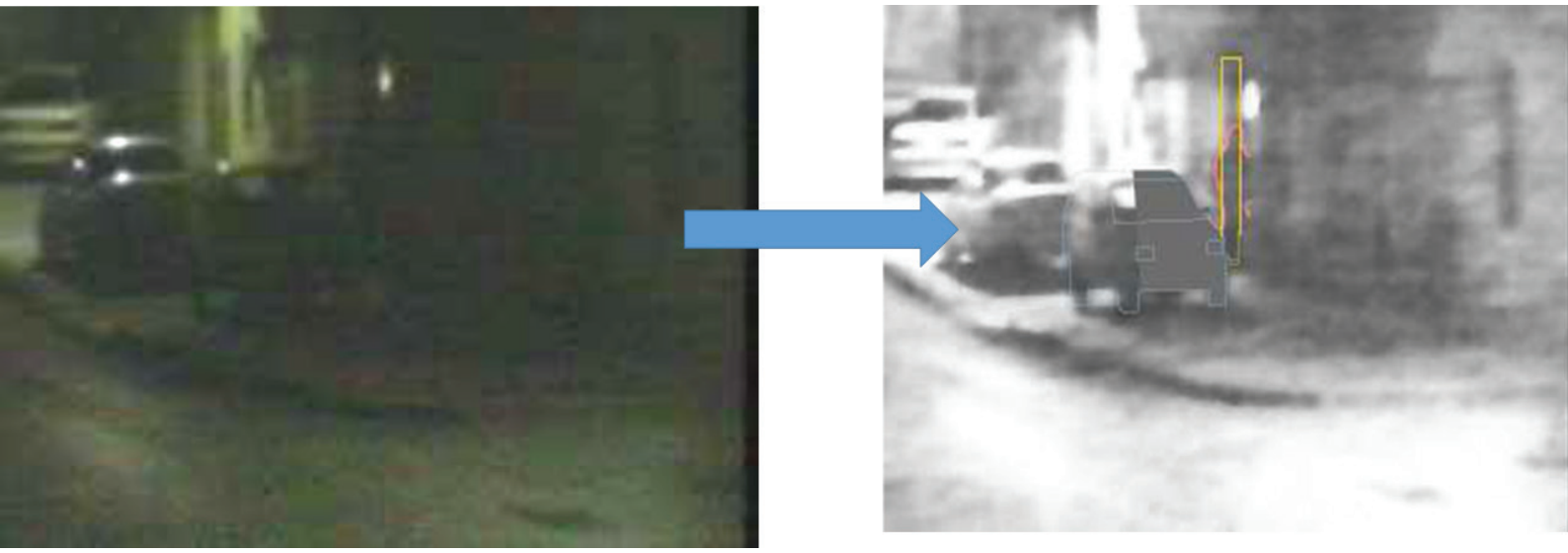

Fig.6: Per la verifica della permanenza nella propria abitazione di un sospettato viene visionato il filmato ripreso da telecamere posizionate di fronte alla casa. Il filmato, data la pessima risoluzione, deve essere prima migliorato, e successivamente si potranno valutare le misure della sagoma che si nota uscire dal portone.

videoripresa erano assolutamente non adeguate allo scopo. Era necessario quindi capire se si poteva trattare della persona ipotizzata. Le immagini (fig.6) necessitavano quindi di essere migliorate e successivamente analizzate.

Dopo una fase di *Image Enhancement*, si procedeva ad evidenziare tramite algoritmi di *Edge Detection* (estrazione dei contorni) la sagoma della persona che usciva dall'abitazione. Infine si cercava di valutare le misure antropometriche del sospettato, tenendo conto dell'errore causato dai summenzionati problemi tecnici e dalla prospettiva, che distorce la percezione delle dimensioni[(11)]. In questo caso non si è potuto confermare le generalità della persona, ma quantomeno si è riusciti di inferire una stima degli intervalli entro cui si potevano verosimilmente collocare le misure della sagoma evidenziata.

7 Conclusioni

Le accortezze tecniche da adottare nel caso si debba validare l'alibi di un sospettato mediante l'esame di documenti visivi, rivestono primaria importanza nel contesto investigativo. Per agevolare la trattazione sono stati considerati più scenari operativi, alcuni derivanti da accadimenti reali, altri creati su misura. Le *best practices* di *Image Forensics* vanno spesso integrate dall'esperienza e dalle capacità di esperti investigatori. A nostro parere, come dimostra anche la cronaca di questi giorni[(17)], sarà sempre più frequente il caso in cui ci si dovrà confrontare con questo tipo di problematiche.©

NOTE

1. Prensky, Marc. "*Digital natives, digital immigrants*." http://www.marcprensky.com/writing/Prensky (2012).
2. "Procedure Investigative sui primi accertamenti di Polizia Giudiziaria in materia di reati informatici", Pool Reati Informatici della Procura della Repubblica di Milano (2011).
3. D. Di Nucci, F. Palomba, S. Ricchiuti - "Implementazione di un falso alibi digitale su Mac OS X". Facoltà di Scienze MM.FF.NN. Università degli Studi di Salerno. Corso di Sicurezza (2010).
4. V. Calabrò, G. Costabile, S. Fratepietro, M. Ianulardo, G. Nicosia - "L'alibi informatico. Aspetti tecnici e giuridici". Chapter in IISFA Memberbook (2010).
5. Beyer, Stefanie, et al. "*Towards Fully Automated Digital Alibis with Social Interaction*." In Tenth Annual IFIP WG 11.9 International Conference on Digital Forensics. (2014).
6. A. De Santis - "Strumenti e tecniche per la creazione di un falso alibi digitale". Università degli Studi di Salerno. Dipartimento di Informatica (2014).
7. S. Battiato, F. Galvan: "Introduzione alla Image/Video Forensics", Sicurezza e Giustizia n. I /MMXIII - pp. 42-43 (2013).
8. http://ampedsoftware.com/authenticate (visitata il 23/05/14).
9. S. Battiato, F. Galvan, M. Jerian, M. Salcuni - "Linee guida per l'autenticazione forense di immagini". Chapter in IISFA Memberbook (2013).
10. Kee Eric, and Hany Farid. "*Exposing digital forgeries from 3-D lighting environments*." Information Forensics and Security (WIFS), IEEE International Workshop on. IEEE, (2010).
11. S. Battiato, F. Galvan: "Ricostruzione di informazioni 3D a partire da immagini bidimensionali", Sicurezza e Giustizia n. IV /MMXIII - pp. 12-14 (2013).
12. http://www.ilgiornaledeimarinai.it/squali-tutta-la-verita/ (visitata il 16/05/14).
13. http://www.ilmeteo.it/portale/storico-meteo (visitata il 10/06/14).
14. http://www.impulseadventure.com/ (visitata il 19/05/14).
15. CIPA DC-008, "*Exchangeable image file format for digital still cameras: EXIF Version 2.3*", (2012).
16. http://www.avpreserve.com (visitata il 21/05/14).
17. http://www.ilroma.net/node/24664 (visitata il 22/05/14).◊