Capitolo VIII

LINEE GUIDA PER L'AUTENTICAZIONE FORENSE DI IMMAGINI

Sebastiano Battiato - Fausto Galvan - Martino Jerian - Matteo Salcuni

Sommario:
1. Introduzione - 1.1 Un'immagine vale più di mille parole? - 2. La prova visiva - 2.1 Il Principio di Scambio di Locard - 2.2 Prova analogica e prova digitale - 2.3 Autenticità (ed integrità) di un'immagine digitale - 3. L'analisi forense di immagini - 4. Ricostruire la storia di un'immagine - 4.1 Formazione delle immagini digitali - 4.2 Un segno ad ogni passo - 4.3 Caratteristiche intrinseche della scena - 4.4 Tracce lasciate durante la fase di acquisizione - 4.5 Tracce lasciate dal software di elaborazione interno alla fotocamera - 4.6 Tracce lasciate dopo il primo salvataggio - 5. Modifica al contenuto informativo di un'immagine - 6. Linee guida per l'analisi di un'immagine digitale - 6.1 Analisi generale - 6.1.1 Analisi visiva dell'immagine - 6.1.2 Analisi generale del file - 6.2 Analisi del file - 6.2.1 Analisi dei metadati - 6.2.2 Analisi di thumbnail e preview - 6.2.3 Analisi del formato JPEG - 6.2.4 Analisi binaria - 6.3 Analisi globale dell'immagine - 6.3.1 Analisi dei coefficienti DCT - 6.3.2 Analisi della correlazione dei pixel - 6.3.3 Analisi di intensità e colori - 6.4 Identificazione del dispositivo - 6.4.1 Analisi globale del PRNU - 6.5 Analisi locale dell'immagine - 6.5.1 ELA - 6.5.2 Mappa DCT - 6.5.3 Mappa di probabilità - 6.5.4 Mappa del rumore - 6.5.5 Analisi locale del PRNU - 6.5.6 Analisi dei cloni - 6.6 Analisi dettagliata della scena - 6.6.1 Analisi dell'illuminazione - 6.6.2 Analisi della geometria - 6.7 Analisi conclusive - 7. Un caso di studio -7.1 Analisi generale - 7.1.1 Analisi visiva dell'immagine - 7.1.2 Analisi generale del file - 7.2 Analisi del file - 7.2.1 Analisi di thumbnail e preview - 7.2.2 Analisi del formato JPEG - 7.2.3 Analisi binaria del file - 7.3 Analisi globale dell'immagine - 7.3.1 Analisi della correlazione dei pixel - 7.3.2 Analisi di intensità e colori - 7.4 Identificazione del dispositivo - 7.5 Analisi Locale - 7.5.1 ELA - 7.5.2 Mappa DCT - 7.5.3 Mappa di probabilità - 7.5.4 Mappa del rumore - 7.5.5 Analisi locale del PRNU - 7.5.6 Analisi dei cloni - 7.6 Analisi dettagliata della scena - 7.7 Analisi conclusive - 8. Analisi di un'immagine analogica - 8.1 Presenza del negativo - 8.2 Mancanza del Negativo - 9. Conclusioni.

1. INTRODUZIONE

Il numero di immagini create dai nostri dispositivi e spesso trasmesse sul web è in costante aumento. Nel 2008 il numero di telecamere installate nel mondo ammontava a circa 11 milioni, mentre per il 2013 ci si attende che il loro numero sia più che triplicato. Nel 2012, sono state caricate su YouTube circa 2,5 milioni di ore di filmati riguardanti accadimenti ripresi dagli utenti in ogni parte del mondo, su Facebook sono state inserite circa 300 milioni di fotografie digitali [1]. Da ciò risulta evidente l'importanza crescente che la comunicazione visiva sta assumendo, sia nel trasmettere sensazioni, ricordi o pensieri, che per fissare un accadimento. È naturale quindi che questo mutamento nelle modalità di fruizione dell'informazione abbia delle ripercussioni anche in ambito giudiziario (sia civile che penale); è sempre più improbabile che un evento delittuoso possa essere consumato senza che la scena del crimine o parte di essa venga ripresa da un sistema di videosorveglianza prima, durante o dopo la commissione del reato.

Affinché "un documento visivo" possa essere utilizzato in un procedimento giudiziario, è necessario che ne sia provata l'originalità (si noti che nel prosieguo del documento si utilizzeranno in maniera equivalente i termini "autenticità" e "originalità"). Attualmente l'uso di software di fotoritocco o di editing video (disponibili anche gratuitamente), rende possibile la manipolazione del contenuto di un filmato o di un'immagine con estrema facilità. L'attendibilità di una fonte di prova diventa quindi argomento delicato, perché necessita di nozioni tecnico-scientifiche che, anche per la loro continua evoluzione, mal si prestano ad essere catalogate all'interno di una normativa.
Il sito dello "Scientific Working Group on Imaging Technology" [2] riporta in proposito la seguente definizione:
"The application of image science and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria. These criteria usually involve the interpretability of the data, and not simple format changes that do not alter the meaning or content of the data."
In questo capitolo ci si pone l'ambizioso compito di definire questi "criteri" alla luce delle tecnologie attuali e delle metodologie di analisi studiate e presenti nella letteratura di settore.

1.1 Un'immagine vale più di mille parole?

In figura 1 è rappresentato uno scorcio di una strada estrapolato dal programma StreetView di Google [3]. Attraverso tale esempio dimostreremo come un documento apparentemente innocuo possa rivelare un gran numero di informazioni di rilievo. È possibile infatti utilizzare tali dati, non solo per ricostruire la storia dell'immagine (il luogo, la data, l'ora e il proprietario dello scatto) ma anche per inferire un profilo dell'utente che ha salvato la foto sul proprio computer. Ad esempio, dall'immagine si possono dedurre:

- Informazioni sulla vettura di Google (la cosiddetta Google-car) [3] che ha ripreso la scena. Questa infatti si è "autoripresa" (la si nota nello specchio circolare).
- Il fatto che la foto sia stata scattata nel Novembre 2011 (la data è in basso a sinistra nella foto).
- Il luogo esatto, molto probabilmente vicino alla scena in figura, da cui è partito il "viaggio virtuale" dell'utente su StreetView (indicata in alto a sinistra).
- Informazioni sulla geometria 3D della scena [4].
- Informazioni sulla data di acquisizione (giorno ed ora in basso a destra).

Per quanto riguarda il soggetto che ha salvato l'immagine deduciamo:

- Il suo nome (in alto a destra).
- Che utilizza Mozilla Firefox come browser per internet.
- Che utilizza Gmail per gestire la posta elettronica (in alto a sinistra).

- Che ha un profilo su Google+ (in alto a destra).
- Che utilizza Skype (icone in basso).
- Che utilizza Matlab (un software che integra funzioni di calcolo matematico, visualizzazione grafica e programmazione), LateX (un editor di testo utilizzato in ambito accademico) e due software di elaborazione di immagini (icone in basso); è quindi probabile che scriva articoli scientifici, e che tra i suoi interessi vi sia l'elaborazione delle immagini. È presumibile che abbia frequentemente bisogno di tradurre in altre lingue (icona di Google Translator in alto a sinistra).
- Che utilizza Dropbox (icona in basso a destra).

La mole di informazioni che si possono estrarre è veramente notevole, ed è strettamente legata alla risoluzione dell'immagine ed ai metodi di acquisizione della stessa.

Figura 1. Analizzando quest'immagine estrapolata da Google StreetView, si possono dedurre numerose informazioni sul luogo ripreso ed anche sul soggetto che utilizzava il computer al momento del salvataggio dell'immagine.

Al pari di tutti i reperti utilizzabili come prove in un procedimento giudiziario, anche le immagini e i filmati per essere dichiarati validi, e quindi ammissibili, devono essere acquisiti, elaborati e conservati rispettando le giuste procedure. Anche nel contesto delle tecnologie analogiche, preponderanti fino a poco più di 10 anni fa, questo problema era noto, ma a quel tempo la modifica di una foto o di un video richiedeva l'intervento di esperti e raramente non lasciava tracce facilmente identificabili. In ambito digitale invece, un utente che abbia una rudimentale conoscenza di Photoshop o di altri software di fotoritocco può effettuare modifiche su un'immagine senza che siano percepibili ad occhio nudo.

2. LA PROVA VISIVA

Nel saggio di V. Denti: "Scientificità della prova e libera valutazione del giudice" (1972) si legge che: *i metodi scientifici non possono offrire nuove categorie di prove, ma possono servire ad una migliore ricerca della verità*. [5]. Partendo da questo assunto ci limitiamo a segnalare

che l'art. 189 cod. proc. pen. prevede espressamente le prove non disciplinate dalla legge (c.d. prove *atipiche*) e che la giurisprudenza costante della Corte di Cassazione riconosce alle immagini fotografiche e filmate valenza di documento figurativo, del tipo testimoniale e diretto [6].
Data la necessità di circoscrivere lo scenario in cui ci stiamo addentrando, è opportuno citare la seguente definizione di prova relativa al contesto digitale: *digital data that establish that a crime has been committed can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator* [55].

2.1 Il Principio di Scambio di Locard

Nell'ambito delle scienze forensi, **il principio di scambio di Locard** (dal Dr. Edmond Locard, pioniere della scienza forense) afferma che *"chi commette un crimine lascerà sempre sulla scena qualcosa di sé. Contemporaneamente porterà con sé tracce di quel luogo."* Entrambi questi comportamenti possono essere usati per risalire alla sua identità. Paul L. Kirk amplia ed estende questo principio nel modo seguente [7]: *"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it can diminish its value."*
Sebbene questo brano, limitando la tipologia di prove al mondo "analogico", risenta dei 60 anni che lo separano dalla realtà odierna, indica chiaramente un approccio operativo da seguire alla ricerca di prove. Allo stesso modo vedremo come le tracce digitali lasciate (o rimosse) durante un'operazione di falsificazione di contenuti, possano fornire elementi per l'accertamento della storia di quel documento.

2.2 Prova analogica e prova digitale

È necessario innanzitutto fare una distinzione tra prova analogica e digitale di tipo multimediale (cioè contenente audio, foto o video). Il primo e più importante elemento caratterizzante la prova analogica è che le copie non sono mai una replica esatta dell'originale. Da ciò segue che è sempre possibile distinguere l'originale tra una serie di copie simili. Inoltre, nel caso analogico, le procedure di copia hanno l'effetto di degradare progressivamente la qualità del documento. Al contrario, essendo il dato digitale solo una sequenza più o meno lunga di bit, due o più copie del medesimo file contengono la medesima informazione, sia che provengano da un'unica copia, sia che siano esito di copie di copie, e così via. In questo senso non esiste distinzione tra dato informatico originale e duplicato, se non per la differente data di creazione e modifica

a livello di file system (informazioni comunque esterne al file stesso). È chiaro che distinguere tra originale e copia ha senso solo in termini temporali se ad esempio in un gruppo di foto uguali definiamo come originale "quella che è stata generata prima". Il punto fondamentale è che quest'unica forma di distinzione non ha più senso se identifichiamo la prova fotografica con il contenuto visivo che questa trasporta, il quale rimane inalterato. Ciò non si applica a formati compressi (JPEG, MPEG, ecc,) dove i ripetuti salvataggi provocano un progressivo deterioramento del contenuto visivo. Tale fenomeno, sebbene di diversa natura rispetto a quello che si verifica in un'immagine analogica, può permettere di distinguere (in termini di valori di luminosità assunti dai pixel) diverse generazioni di un'immagine. In questo caso però non si può parlare di copia in senso stretto.

2.3 Autenticità (ed integrità) di un'immagine digitale

La verifica di autenticità di un documento visivo digitale avviene in due fasi:

1) **Verifica dell'autenticità del file**: il processo volto a confermare che il dato presentato è completo ed è rimasto inalterato fin dal momento della sua acquisizione. Significa poter rispondere affermativamente al quesito: *"si è in grado di dimostrare che il file contenente l'immagine è stato creato da una determinata macchina fotografica e non è mai stato alterato da un altro software o dispositivo successivamente all'acquisizione iniziale?"* Tale certificazione rappresenta il massimo grado di originalità attribuibile ad un'immagine in quanto implica l'autenticità sia del "contenuto" (la sola immagine) che del "contenitore" (l'immagine + i metadati). Ci sono solo due casi in cui il fatto che il file sia autentico non implica che il contenuto dell'immagine lo sia:

- **Immagine ricatturata**: l'immagine è stata ottenuta acquisendo in qualche modo l'immagine di partenza dopo averla opportunamente alterata. A titolo esemplificativo osserviamo l'immagine a sinistra nella figura 2: una foto (originale) è stata modificata con l'aggiunta di un alligatore; il tutto è stato fotografato nuovamente con una fotocamera diversa da quella che ha scattato l'immagine iniziale. In tal caso un'analisi dell'immagine evidenzierebbe tracce riconducibili unicamente alla macchina che ha acquisito l'immagine dopo la modifica e nulla che possa ricondurre alla fotocamera da cui proviene l'immagine di partenza.

Figura 2.
A sinistra un'immagine ricatturata, a destra una messa in scena.

- **Messa in scena**: l'immagine è autentica, ma è il contenuto ad essere "falso" o "costruito" ad hoc e può essere usato a vario titolo (ad esempio: l'opera "Information Leak" di Richard Evans [8] raffigurata a destra nella figura 2 vuole rappresentare il sovraccarico di informazioni nella società di oggi).

2) **Verifica dell'autenticità** del contenuto: il contenuto visivo deve corrispondere a quello della scena originale. A tale fine si può (anche parallelamente):

- Individuare un testimone che certifichi che l'immagine rappresenta esattamente la scena catturata (ad esempio lo stesso utente "fotografo"). Si noti che questo approccio non risolve il problema, ma lo sposta da "accertare se la foto è autentica" a "accertare se il testimone dice il vero".
- Adottare tecniche analitiche per dimostrare in maniera oggettiva che l'immagine non sia stata alterata.

A questo proposito, mutuando una definizione di autenticità di un file audio da parte dell'AES (Audio Engineering Society) [56], possiamo affermare che:
"È possibile attestare che un'immagine è autentica quando si può accertare che è stata realizzata simultaneamente con l'evento visivo che si propone di avere registrato, ed in un modo completamente consistente con il metodo di acquisizione riferito dalla parte che ha raccolto l'immagine; un'immagine sprovvista di artefatti, aggiunte, cancellazioni o modifiche varie."

3. L'ANALISI FORENSE DI IMMAGINI

L'analisi forense di immagini è una scienza forense praticata fin dagli albori della fotografia. In particolare, già nel 1851 Marcus A. Root condusse il primo esempio documentato di autenticazione forense delle immagini: tramite un esame al microscopio, Root rivelò che il processo di colorazione di immagini messo a punto dal Reverendo Levi Hill era in effetti il prodotto di una colorazione a mano, non il risultato di un progresso nella fotografia (Davis et al. 1995). Le prime "elaborazioni fotografiche" sono datate 1860 come riportato in [9].
Dal sito dell'FBI [10], leggiamo che la *"Forensic Image Analysis is the application of image science and domain expertise to interpret the content of an image or the image itself in legal matters"*.
Da questa definizione possiamo individuare i punti salienti che devono caratterizzare l'approccio forense all'analisi di un'immagine. Quest'ultima, infatti, deve essere affidata a personale con un'adeguata preparazione tecnica nel campo dell'image processing, ma che sappia anche interpretare le informazioni estratte alla luce del contesto dell'ambito forense e giudiziario.
L'analisi forense di immagini è suddivisa nelle seguenti categorie:

- **Image forgery identification**: identificazione di manipolazioni in un'immagine, finalizzata all'inserimento o alla rimozione di parte del contenuto informativo di un'immagine.

- **Source camera identification**: identificazione del dispositivo che ha generato l'immagine. Il primo passo è la discriminazione tra immagini naturali o artificiali (Computer Generated). Nel primo caso si passa all'individuazione della sorgente che ha generato l'immagine, dapprima accertando il tipo di apparecchiatura (scanner, fotocamera, fotocopiatrice, stampante) e successivamente cercando di determinare il particolare dispositivo di acquisizione.
- **Image reconstruction/restoration/enhancement**: restauro di immagini deteriorate e miglioramento della qualità al fine di identificare, anche parzialmente, il contenuto originale e/o recuperare informazioni [45].
- **Image/video analysis**: analisi dinamiche o comportamentali volte, ad esempio, ad individuare la consecutio temporum di un evento d'interesse.
- **Ricostruzione 3D e comparazione**: estrazione delle informazioni bi/tridimensionali contenute all'interno della scena per ricavare misure o grandezze di riferimento (ad esempio l'altezza di un individuo) e per la comparazione tra immagini (ad esempio per verificare l'identità di un soggetto noto con l'autore di un reato, ripreso da un sistema di videosorveglianza).
- **Steganalisi**: individuazione di informazioni nascoste all'interno di un'immagine con tecniche steganografiche (ad esempio mediante la modifica del bit meno significativo nel numero che definisce il colore di un pixel).

Nonostante negli ultimi anni sia cresciuto il numero di pubblicazioni scientifiche e divulgative su tali argomenti (si veda ad esempio [11] [12], [13], [14]), non è ancora stato proposto uno studio volto a unificare in maniera coerente i diversi approcci scientifici, allo scopo di costituire delle linee guida comunemente accettate per dimostrare l'autenticità di un documento multimediale.

4. Ricostruire la storia di un'immagine

All'analista forense di immagini è spesso richiesto di accertare più dettagliatamente possibile la storia di un documento visivo. Prima di esaminare le varie tipologie di tecniche che possono essere utilizzate nella manipolazione di foto o di video, bisogna chiarire gli aspetti connessi alla formazione di un'immagine digitale. Ogni dispositivo fotografico, ad esempio, definisce un'impronta *(fingerprint)* che lo caratterizza in modo univoco a livello statistico e che può essere utilizzata per caratterizzare le fotografie digitali provenienti da un altro esemplare dello stesso modello o da modelli diversi. Capire come viene generata una foto, può quindi essere utile a comprendere tutte i tipi di problematiche che compongono la Image Forensics.

4.1 Formazione delle immagini digitali

Il procedimento *(pipeline)* che porta alla memorizzazione di una scena reale in un file immagine è illustrata in figura 3. Esso può essere suddivi-

so in tre fasi principali [15]: acquisizione, elaborazione e memorizzazione. Nella fase di acquisizione la luce proveniente dalla scena attraversa il sistema di lenti che la indirizza verso il sensore della fotocamera (costruito con tecnologia CCD o CMOS). Quest'ultimo è composto da un alto numero di elementi fotosensibili che catturano l'energia della luce convertendola in corrente elettrica e che riescono in tal modo a determinare il valore di luminosità di ciascun pixel.

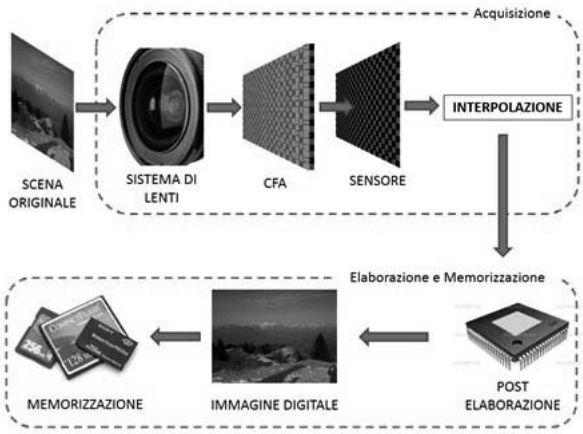


Figura 3.
La pipeline di formazione dell'immagine all'interno di una moderna fotocamera digitale.

Per acquisire immagini a colori è necessario scomporre la luce visibile nelle tre componenti fondamentali, corrispondenti alla lunghezza d'onda del rosso, del verde e del blu. In linea di principio bisognerebbe avere un sensore per ognuno dei colori da catturare, facendo lievitare oltremodo il prezzo delle fotocamere e introducendo svariate complicazioni tecniche. I dispositivi comunemente in commercio adottano invece un'altra soluzione: sopra il sensore viene applicata una sottile pellicola fotosensibile, detta CFA (Color Filter Array), che ha il compito di filtrare la luce e di separarla nei tre colori fondamentali in modo che ogni singolo pixel sia specializzato nella cattura selettiva di ciascuno di questi colori. In questo modo si ottiene una griglia di valori in cui ogni pixel registra il segnale relativo ad una sola componente cromatica. Il modello più diffuso di CFA è il Bayer Pattern, rappresentato dalla scacchiera multicolore visualizzata in figura 3. L'impiego dei CFA permette di utilizzare un solo sensore per l'acquisizione a colori, ma richiede la ricostruzione delle due componenti mancanti mediante un algoritmo di interpolazione (demosaicing). Di solito questa elaborazione viene eseguita dal processore della fotocamera prima della memorizzazione della foto, unitamente ad altre operazioni di post-processing quali: il bilanciamento del bianco, l'elaborazione del colore, la correzione di pixel difettosi, la soppressione delle "dark currents", il miglioramento del contrasto e la correzione gamma. L'immagine ottenuta viene quindi compressa in uno dei formati disponibili sul dispositivo secondo la configurazione dell'utente. L'algoritmo di compressione utilizzato dalla maggior parte delle fotocamere in commercio (circa il

95%) è il JPEG [46], che esamineremo in dettaglio nel capitolo seguente. Molti dispositivi, specie quelli di fascia medio/alta, permettono di salvare l'immagine in formato TIFF, oppure in formato RAW. Quest'ultimo è un formato definito in maniera indipendente per ogni produttore e salva i dati grezzi come acquisiti dal sensore, permettendo al fotografo un controllo assoluto e preciso su tutta la fase di sviluppo digitale dell'immagine.

4.2 Un segno ad ogni passo

Vediamo ora di caratterizzare le tracce lasciate sull'immagine nelle varie fasi della sua formazione. Esse possono essere suddivise in:

- Caratteristiche intrinseche della scena;
- Tracce lasciate durante la fase di acquisizione;
- Tracce lasciate dal software di elaborazione interno alla fotocamera;
- Tracce che derivano dalla fase di elaborazione subita dall'immagine successivamente alla sua creazione e al primo salvataggio in memoria.

È di fondamentale importanza conoscere tali segni, in quanto ogni manipolazione (malevola o meno) ha come conseguenza l'alterazione di almeno uno di essi. Inoltre le incongruenze tra *quello che ci dovrebbe essere* e *quello che non è presente* forniscono indizi per ricostruire la storia dell'immagine.

Nei paragrafi successivi esamineremo in dettaglio le varie tipologie di tali tracce, mentre nei capitoli successivi illustreremo come utilizzare questi elementi per eseguire un'analisi dell'immagine finalizzata a individuare il dispositivo che ha generato l'immagine (Image Source Identification) e a determinare la presenza di eventuali manipolazioni nell'immagine (Image Forgery Identification)

4.3 Caratteristiche intrinseche della scena

GEOMETRIA DELL'IMMAGINE. Il modello teorico classico *(pinhole camera model)* [20] prevede che, durante la formazione dell'immagine, i punti $\mathbf{X}_i$ nel mondo reale 3D vengano *proiettati* nel piano bidimensionale dell'immagine nei corrispondenti punti $\mathbf{X}_i$. Questi ultimi sono individuati dall'intersezione del piano immagine con il segmento di retta che unisce il centro ottico **O** della fotocamera ed il punto $\mathbf{X}_i$ della scena ripresa (figura 4).

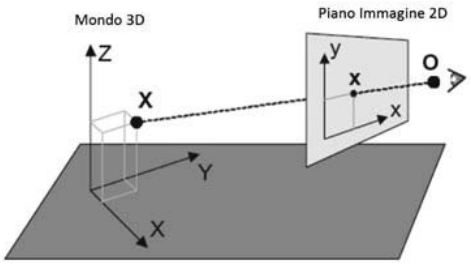


Figura 4.
La formazione dell'immagine all'interno della fotocamera è modellata come una proiezione di punti del mondo 3D in punti 2D del piano immagine.

La prospettiva ha come effetto quello di distorcere le dimensioni degli elementi presenti sulla scena in maniera più o meno accentuata a seconda della loro distanza dal piano del sensore di ripresa. Data un'immagine, quindi, è possibile ricavare alcune elementi caratteristici della scena come punti e linee di fuga che possono essere rilevati in maniera precisa con dei metodi matematici [21]. Un altro elemento di riferimento della prospettiva di un'immagine è il punto principale, che rappresenta la proiezione del centro ottico della fotocamera sul piano immagine ed è il punto in cui convergono tutte le rette ortogonali al piano stesso.

LUCI ED OMBRE. La luminosità di ogni pixel che compone un'immagine digitale è proporzionale alla quantità di luce che la superficie a cui si riferisce il pixel riflette verso la fotocamera. Il modello semplificato prevede che la fonte di illuminazione di una scena esterna durante il giorno possa essere modellata come un punto infinitamente lontano. Questa semplificazione, a volte, permette di stimare con sufficiente precisione la direzione della fonte di luce e, al tempo stesso, di ottenere informazioni sulle caratteristiche dell'immagine sfruttando le ombre prodotte dai soggetti presenti. In condizioni più complesse (scena interna, luce notturna proveniente da illuminazione artificiale) le prestazioni risentono della difficoltà nel modellare il contesto ambientale.

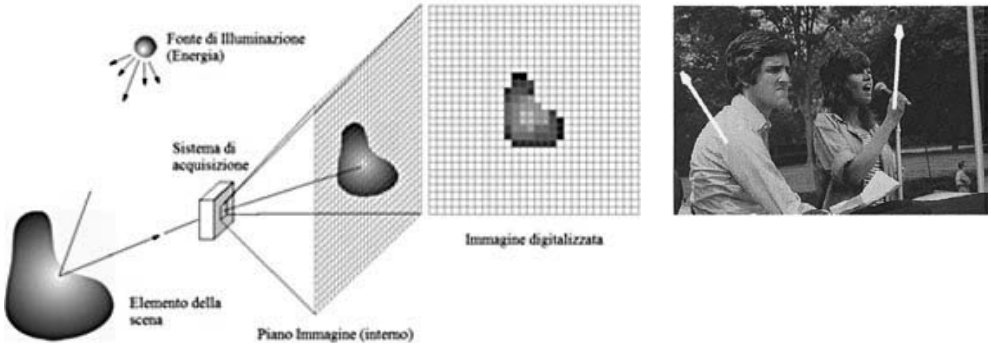


Figura 5.
A sinistra il modello classico di illuminazione di una scena. A destra, una famosa immagine resa pubblica durante le primarie per la nomination democratica alle elezioni presidenziali USA del 2004. Ritraeva l'allora Senatore John Kerry assieme a Jane Fonda mentre, diversi anni prima, condividevano il palco in una riunione pubblica per manifestare contro la guerra. In realtà questa immagine è un falso ottenuto componendo una foto del Sen. Kerry del 1971 con una dell'attrice, datata 1972 [9]. Le diverse direzioni di provenienza della luce nei due soggetti (frecce) hanno messo poco tempo dopo in evidenza tale manipolazione.

4.4 Tracce lasciate durante la fase di acquisizione

LENTI. Ogni tipo di macchina fotografica ha il proprio sistema di lenti. I difetti introdotti nell'ottica di acquisizione, che vediamo rappresentati in figura 6, possono essere generalmente di due tipi: la distorsione geometrica radiale [47] e le aberrazioni cromatiche [48]. Il primo è un fenomeno che deforma le linee rette in modo da farle apparire curve mano a mano che si allontanano dal centro ottico dell'immagine; mentre, il secondo è provocato dalle imperfezioni delle lenti e provoca una deviazione nel punto in cui il sensore riceve la luce.

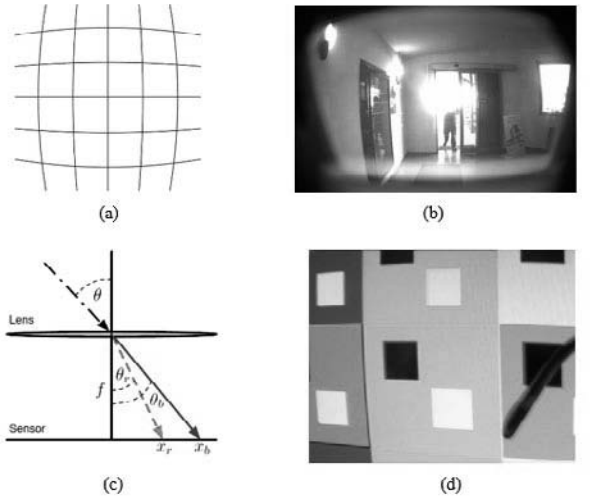


Figura 6.
Difetti provocati dal sistema di lenti di una fotocamera: nella riga superiore vediamo il fenomeno denominato *distorsione a barile*, schematizzato (a) e come appare in realtà (b). Nella riga inferiore, sono illustrati gli effetti dell'*aberrazione cromatica*, schematizzati (c) e come appaiono in realtà (d).

SENSORE. Il processo di fabbricazione del sensore e la disomogeneità del silicio introducono delle imperfezioni nel sensore, che sono diverse per ogni singolo esemplare [49]. Le disuniformità si traducono in una differente sensibilità alla luce tra le diverse zone. Ciò produce una "firma" *(pattern)*, unica per ogni sensore di ogni dispositivo, che può essere identificata estraendo una componente specifica del rumore chiamata PRNU *(Photo Response Non Uniformity)*.

Questo tipo di disturbo ha numerosi "pregi", tra cui i più importanti sono:

- Essere stabile nel tempo.
- Non dipendere dalla temperatura.
- Sopravvivere alla compressione JPEG (entro certi limiti).
- Sopravvivere a operazioni di ridimensionamento (entro certi limiti).
- Sopravvivere a operazioni di modifica di luminosità, contrasto, gamma, colori, etc. (entro certi limiti).

Trattando opportunamente l'immagine per estrarre il PRNU è possibile discriminare in modo piuttosto affidabile diversi dispositivi [17], [18],

[19]. L'estrazione del PRNU dipende dalla quantità di luce acquisita, ad esempio è del tutto assente in aree dell'immagine sature. Le regioni dell'immagine con molti dettagli tendono a nasconderlo, mentre quelle omogenee permettono di acquisirlo e quindi identificarlo meglio.

4.5 Tracce lasciate dal software di elaborazione interno alla fotocamera

CFA INTERPOLATION. Come si è accennato precedentemente, è necessario ricomporre il segnale catturato dal CFA del sensore al fine di ottenere un'immagine RGB a risoluzione piena [50]. I valori di luminosità mancanti vengono ottenuti applicando una procedura d'interpolazione all'immagine relativa a ciascuna componente R, G e B che è stata estratta dal CFA. Esistono di versi metodi d'interpolazione, tuttavia essi sono accomunati dal fatto che stimano i valori dei pixel mancanti combinando quelli dei pixel vicini mediante una funzione interpolante comune.

METADATI EXIF. Una volta acquisita l'immagine, la macchina fotografica "incapsula" lo stream di bit corrispondenti ai valori di luminosità dei tre canali colore in un file composto da un'intestazione *(header)* ed un corpo principale contenente l'immagine vera e propria (figura 7). L'intestazione di un file immagine contiene numerosi dati sull'immagine *(metadati)* in un formato chiamato formato EXIF [22], [23]. Come vedremo, numerosi software (ad esempio JPEGsnoop [24]) permettono di leggere il contenuto dell'intestazione.

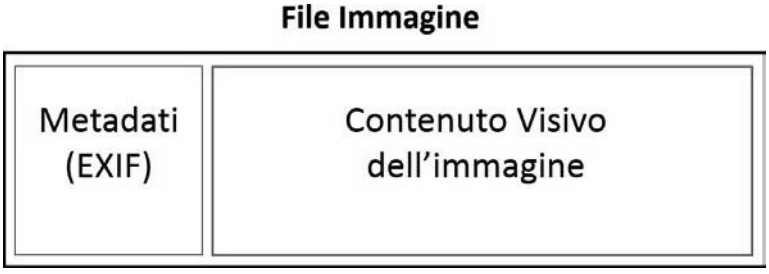


Figura 7. Diagramma dei vari tipi di elaborazione cui può essere sottoposta un'immagine.

THUMBNAIL E PREVIEW. La maggior parte dei dispositivi moderni salva all'interno dell'immagine principale una o due immagini secondarie, dette thumbnail (miniatura) e preview (anteprima). La thumbnail è una versione a bassa risoluzione dell'immagine principale, tipicamente con dimensioni nell'ordine di 160x120 pixel. Essa può essere utilizzata, ad esempio, da una macchina fotografica per presentare le immagini disponendole a griglia sul display o come anteprima a livello di *file system*. Quasi tutti i dispositivi attuali salvano una miniatura e la sua posizione all'interno dello *stream* è definita nello standard in uso. La *preview* è una versione ridotta dell'immagine principale, con una risoluzione maggiore della thumbnail, di solito nell'ordine di 640x480 pixel. Essa è utilizzata generalmente da una fotocamera per visualizzare rapidamente l'immagine sul suo display. Solo alcuni dispositivi salvano

un'anteprima e la sua posizione all'interno del file non è definita in nessuno standard, per cui la sua implementazione varia col produttore.

4.6 Tracce lasciate dopo il primo salvataggio

Diverse e variegate sono le possibilità di modificare un'immagine, così come differenti sono le motivazioni che spingono a farlo. A fattor comune tra i metodi utilizzati vi è la necessità, terminate le modifiche, di risalvare il risultato ottenuto. Questo doppio (o multiplo) salvataggio può essere rilevato, a prescindere da ciò che è stato modificato nella foto, mediante l'esame dei relativi istogrammi riferiti ai valori dei coefficienti DCT, come illustrato in seguito. Per una discussione esaustiva sui passi dell'algoritmo JPEG rimandiamo a [11]. Una volta avuto esito positivo al controllo, si è in grado di affermare che l'immagine non è quella originariamente generata dalla macchina al momento dell'acquisizione. Per accertare esattamente cosa è stato alterato e come, il punto di partenza consiste nel controllare quale, tra le tracce elencate nei paragrafi precedenti, è stata corrotta da tale operazione.

5. Modifica al contenuto informativo di un'immagine

Un'immagine può essere manipolata in modo innocuo o malizioso (figura 8). Nel primo caso, trattasi di solito di tecniche volte a migliorarne la resa visiva (ad esempio eseguendo un'espansione del contrasto), mentre, nel secondo caso, si fa ricorso a tecniche di editing che ne alterano il contenuto semantico (ad esempio rimuovendo e/o aggiungendo informazioni).

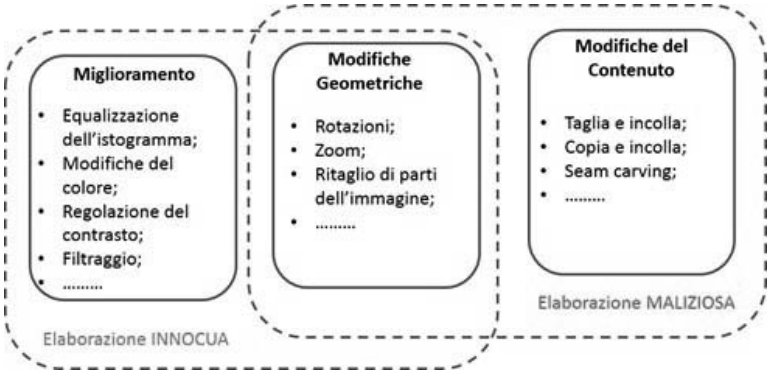


Figura 8. Esempio di image enhancement: per rendere un volto più cupo e minaccioso si può agire semplicemente sulla luminosità dell'immagine. L'immagine di sinistra visualizza una delle foto segnaletiche scattate subito dopo l'arresto di OJ Simpson (1994), quella di destra mostra la foto modificata.

Nel seguito vengono riportate alcune tecniche di manipolazione:

Regolazione dei valori dei pixel (image enhancement): sono le operazioni più semplici, che consistono nel variare l'intensità o i colori dell'immagine agendo direttamente sull'istogramma dei valori e modificandone il contrasto od applicando dei filtri opportuni. Tali modifiche non vanno sottovalutate poiché possono avere l'effetto di trasformare il messaggio trasmesso da un'immagine rendendo, ad esempio, il volto di una persona più minaccioso (figura 9).

Figura 9. Esempio di image enhancement: per rendere un volto più cupo e minaccioso si può agire semplicemente sulla luminosità dell'immagine. L'immagine di sinistra visualizza una delle foto segnaletiche scattate subito dopo l'arresto di OJ Simpson (1994), quella di destra mostra la foto modificata.

Taglia-incolla (splicing): è un'operazione che coinvolge due o più immagini e che consiste nel copiare il contenuto di un'immagine o di parte di essa su un'immagine diversa. Questo tipo di editing aggiunge informazione all'immagine.

Figura 10. Esempio di splicing: il contenuto della immagine di sinistra è modificato aggiungendo parte del contenuto di una seconda foto.

Ritaglio di parte dell'immagine (cropping): è un'operazione che consiste nel selezionare una parte di un'immagine (detta ROI – Region Of Interest) salvandola poi come immagine a se stante. Questo tipo di editing rimuove informazione dall'immagine.

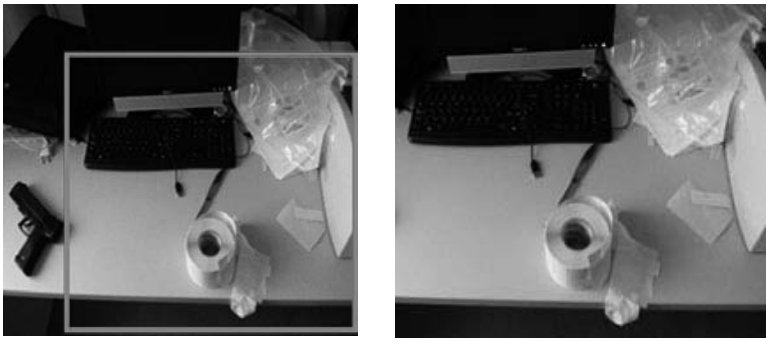


Figura 11. Esempio di ritaglio: il contenuto dell'immagine di sinistra è stato modificato togliendo la parte indesiderata; l'immagine risultante è visualizzata a destra.

Copia-incolla (cloning): consiste nel duplicare parti di un'immagine all'interno dell'immagine stessa. Questo tipo di operazione può aggiungere o rimuovere informazione.

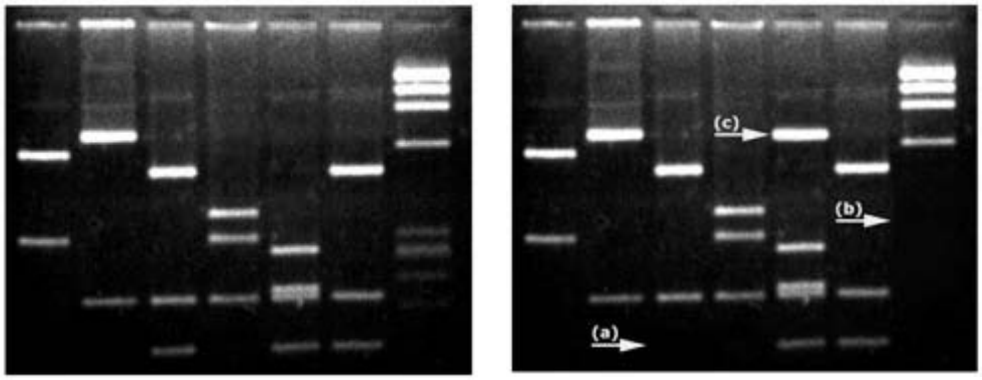


Figura 12.
Esempio di cloning per falsificare gli esiti di sperimentazioni: il contenuto della immagine di sinistra è stato modificato aggiungendo parte del contenuto della stessa immagine, nell'immagine di destra sono evidenziate le aree modificate.

6. LINEE GUIDA PER L'ANALISI DI UN'IMMAGINE DIGITALE

In questa sezione vengono fornite alcune linee guida generali per un'analisi sistematica di un'immagine digitale al fine di valutarne l'autenticità. La lista dei metodi presentati non è esaustiva ma include gli approcci che, secondo l'esperienza degli autori, risultano essere i più indicati a fini forensi nella casistica più comune. In letteratura esistono approcci differenti la cui validità è però limitata a casi molto particolari o ad una serie di ipotesi molto restrittive. Utilizzando quanto qui proposto è possibile valutare in maniera efficace gran parte delle situazioni che l'analista forense verosimilmente deve affrontare.

6.1 Analisi generale

Il primo passo da eseguire consiste nell'ispezione generale dell'immagine. Infatti, prima di tutto è sempre necessario comprendere il contesto in cui si opera e valutare le eventuali caratteristiche "sospette" che dovranno essere approfondite nelle fasi successive.

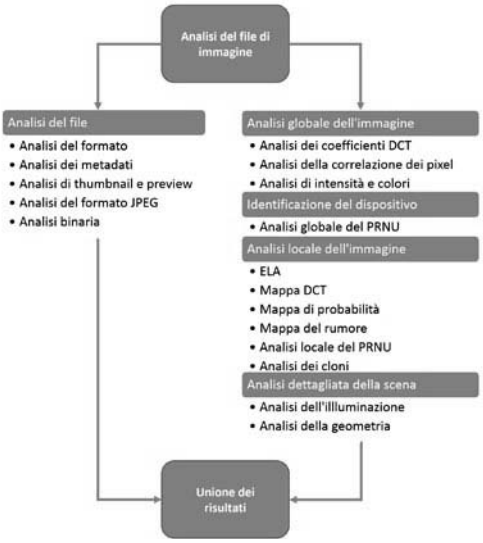


Figura 13.
La verifica di originalità di un'immagine è un processo complesso che coinvolge informazioni visuali e non.

Per capire come utilizzare al meglio i vari elementi a disposizione e fissare gli obiettivi dell'analisi, è necessario accertare quanto segue:

- TIPO DI ANALISI: si chiede di analizzare una o più immagini in maniera specifica, oppure una cartella con migliaia di immagini alla ricerca di eventuali file sospetti?
- PROVENIENZA DEL MATERIALE: la foto proviene da un determinato dispositivo, oppure si tratta di file che probabilmente non sono originali? Ad esempio, se si sta lavorando su file scaricati da Facebook si dovrà tener in conto del fatto che le immagini non provengono direttamente da un dato dispositivo ma sono state risalvate dal sistema in fase di caricamento utilizzando delle impostazioni predefinite.
- DISPONIBILITÀ DELLA FOTOCAMERA: è disponibile il dispositivo che si suppone abbia creato le immagini? Se sì, si tratta dello stesso esemplare specifico o di un altro esemplare dello stesso modello? In alternativa, sono disponibili altre foto di prova che si suppone siano state scattate con quella macchina fotografica?

Una volta compreso quanto sopra, l'obiettivo del lavoro potrà riguardare a seconda dei casi diversi aspetti. Ad esempio, giusto per citare alcuni possibili quesiti:

- Verificare che il file di immagine analizzato sia l'originale, scattato da una certa fotocamera e lasciato completamente inalterato senza alcuna modifica di formato.
- Verificare che il contenuto dell'immagine non presenti tracce di manipolazioni, nonostante il formato del file sia stato evidentemente modificato.
- Verificare che l'immagine sia stata scattata da uno specifico esemplare di macchina fotografica in possesso di un determinato soggetto *(camera ballistics)*.
- Comprendere il tipo di manipolazioni eventualmente applicate all'immagine.
- ...

6.1.1 Analisi visiva dell'immagine

Come premessa generale, è importante sottolineare che un'analisi visuale accurata permette talvolta di svolgere buona parte del compito. Infatti, in questa fase si possono riscontrare manipolazioni grossolane, inconsistenze, anacronismi ed altre problematiche che, da sole, possono far dubitare della genuinità del documento da analizzare (non necessariamente in formato digitale). Per avere un'idea delle possibili situazioni in cui è possibile utilizzare efficacemente l'analisi visuale, si vedano gli esempi riportati sul popolare sito web Photoshop Disasters [25]

6.1.2 Analisi generale del file

Questo tipo di analisi consente di individuare unicamente eventuali alterazioni a livello di formato: permette cioè di determinare l'au-

tenticità o meno del file, ma non del contenuto informativo in esso contenuto. L'analisi di formato può essere di tipo comparativo (ci si confronta cioè con analoghi dati) o assoluto.
Alcuni degli elementi principali da analizzare, per valutare l'autenticità del file mediante un'analisi di tipo assoluto, sono i seguenti:

- **Formato dell'immagine** di tipo JPEG, RAW o TIFF (difficilmente le macchine fotografiche acquisiscono in formato PNG o BMP).
- **Dimensioni delle immagini** che devono necessariamente essere riferite ad un range prestabilito (immagini troppo grandi o troppo piccole sono sospette).
- **Presenza dei metadati** EXIF (in particolare dei tag Make e Model).
- **Presenza di *keyword* sospette** all'interno dei metadati dell'immagine (la presenza di parole come "Adobe Photoshop" o "Lightroom" all'interno del tag Software è molto sospetta).
- **Compatibilità delle date** di creazione e modifica salvate nei dati EXIF con le date MAC *(Modified, Access, Creation)* del *file sytem*.
- **Presenza di immagini secondarie** quali thumbnail e preview (come visto precedentemente, quasi tutte le macchine fotografiche moderne salvano delle versioni ridotte dell'immagine principale).

Nell'analisi di tipo comparativo, invece, è possibile verificare la compatibilità del formato con un'altra immagine, a patto che si abbiano a disposizione immagini acquisite dallo stesso dispositivo (almeno lo stesso modello se non l'esemplare specifico che ha scattato la foto).

Alcuni esempi di analisi comparative sono riportati di seguito:

- **Formato dell'immagine** generabile dallo specifico modello di fotocamera (una compatta difficilmente scatterà in RAW).
- **Dimensioni dell'immagine** che sono supportate dallo specifico modello di fotocamera.
- **Numero di metadati EXIF** compatibile con il modello di fotocamera specifico.
- **Formato del file** (ad esempio tabelle di quantizzazione e codici di Huffman del JPEG) compatibile con il particolare modello di fotocamera.
- **Dimensioni** di thumbnail e preview **compatibili**.

La presenza di una specifica anomalia non conforme al formato non significa necessariamente che il file non sia autentico, ma l'elemento in questione dovrà essere sottoposto ad un'analisi più approfondita. Nel seguito faremo riferimento allo schema di figura 13.

6.2 Analisi del file

Nell'analisi del formato vengono analizzate in maniera dettagliata le caratteristiche del file contenente l'immagine, approfondendo eventuali

elementi dubbi che sono emersi dall'analisi generale. Anche in questa fase si analizza soltanto l'aspetto digitale e il formato dell'immagine, senza considerare minimamente il contenuto informativo, i valori dei pixel o altre caratteristiche dell'immagine.
Le considerazioni di cui al paragrafo precedente riguardo le analisi di tipo assoluto o comparativo valgono anche in questo caso. Infatti, l'analisi del formato si basa sulla ricerca dettagliata nel file di elementi sospetti, finalizzati a valutare la compatibilità delle caratteristiche dell'immagine analizzata con quelle delle immagini di riferimento, che sono state generate dallo stesso dispositivo con cui si suppone sia stata scattata la fotografia esaminata. A causa del gran numero di impostazioni configurabili dall'utente nei dispositivi moderni il problema principale di queste tecniche è valutare tutte le possibili combinazioni fino ad individuare, eventualmente, un formato completamente compatibile con quello in esame. Questa valutazione è molto semplice nel caso in cui il numero di impostazioni configurabili del dispositivo è limitato, come accade per maggior parte degli *smartphone* in commercio. Tuttavia, può essere una metodologia molto difficile (se non impossibile) da attuare nel caso di fotocamere compatte o reflex.
Il vantaggio principale di queste tecniche consiste nel fatto che sono, in generale, facilmente automatizzabili e interpretabili. Il loro punto debole, invece, risiede nel fatto che un'attaccante esperto potrebbe riuscire a replicare perfettamente il formato di una specifica fotocamera in maniera del tutto invisibile all'analista. Sebbene sia, come abbiamo detto, un'operazione non alla portata di tutti, è una possibilità che non si può escludere a priori.
Il metodo è tanto più robusto quante più sono le caratteristiche che vengono prese contemporaneamente in considerazione. Infatti, l'attaccante riuscirà ad ingannare l'analista se sarà capace di replicare coerentemente tutte le caratteristiche analizzate da quest'ultimo. D'altro canto, il compito dell'analista sarà trovare degli elementi (se esistono) che sono stati trascurati dall'attaccante.
Il limite intrinseco di queste tecniche sta nel fatto che permettono solo di verificare se il file è originale o meno, ma non possono dire nulla sulla genuinità dell'immagine in esso rappresentata, che dovrà essere accertata mediante tecniche di analisi locale.

6.2.1 **Analisi dei metadati**

Come già accennato, la stragrande maggioranza delle macchine fotografiche moderne inserisce automaticamente dei dati EXIF all'interno del file contenente l'immagine. Le specifiche EXIF definiscono sia dei campi comuni alla maggior parte dei produttori, che campi personalizzati. Per decodificare correttamente quest'ultimi, è necessario possedere i software proprietari o applicare delle operazioni di *reverse engineering*.

Un dispositivo moderno può salvare all'interno dei metadati diverse decine di informazioni [26], quali ad esempio:

- Produttore e modello di fotocamera;

- Diversi tipi di informazioni legate alla data e all'ora di generazione e di salvataggio del file;
- Un campo che determina il software usato per creare l'immagine. In un'immagine proveniente direttamente da una macchina fotografica, il campo è vuoto oppure riporta la versione del firmware (ad esempio "Ver. 1.10"); mentre, nel caso di una foto non originale, il campo potrebbe contenere il nome del software che è stato utilizzato per modificarla (ad esempio "Adobe Photoshop CS5 Windows"). Infatti, la maggior parte dei programmi di fotoritocco e di gestione di fotografie digitali riconoscono i dati EXIF conservandone la maggior parte, inserendo però una dicitura del campo "Software" quando risalvano l'immagine modificata;
- Informazioni sulle caratteristiche dell'immagine (risoluzione in pixel, dpi, profondità del colore, ecc.);
- Impostazioni di scatto (tempo di scatto, apertura, flash, modalità scena, ISO, focale, ecc.);
- Coordinate GPS;
- Informazioni sul copyright della foto, impostate direttamente nei settaggi della fotocamera;
- Seriale del dispositivo.

Oltre alle informazioni in formato EXIF, esistono altre tipologie di metadati strutturati in modo differente quali IMM *(Information Interchange Model)* e XMP *(Extensible Metadata Platform)*. I metadati IMM incorporati nelle immagini sono spesso indicati come "Intestazioni IPTC" e sono supportati sia dai formati JPEG e TIFF. Lo standard XMP, invece, è stato creato da Adobe per archiviare i dettagli delle operazioni svolte sull'immagine ed è molto usato nei PDF e in fotografia; ciononostante, è scarsamente supportato dalle fotocamere. Entrambi gli standard possono essere facilmente decodificati e visualizzati all'interno dello *stream* del file.
Oltre a ricercare l'evidenza di tracce lasciate dai software di fotoritocco [27], è possibile effettuare un'analisi di tipo comparativo fra l'immagine in esame e altre immagini di riferimento che sono state scattate con la fotocamera d'interesse. Non sempre il confronto è immediato, in quanto ci possono essere notevoli differenze fra due immagini create col medesimo dispositivo. Ci sono alcuni elementi che dovrebbero rimanere costanti, come produttore e modello, o al più variare in un certo intervallo, come le impostazioni di scatto. Ci sono, però, altri elementi che possono essere presenti o meno a seconda delle impostazioni dell'utente o del modello di fotocamera, come i dati GPS, o valori che è normale siano diversi, come la data di scatto.
Analogamente a tutte le altre tecniche basate sul formato, un attaccante competente può modificare abbastanza facilmente i dati EXIF con software gratuiti e accessibili a tutti (come EXIFTool [28] e PhotoMe [29]), quindi non bisogna fidarsi troppo del loro contenuto e utilizzarli solo come uno degli elementi dell'analisi. In particolare, è importan-

te considerarli nella loro totalità e non limitarsi ad analizzare solo alcuni valori. È molto semplice, ad esempio, modificare il dato EXIF contenente il nome del modello della fotocamera, ma è necessario modificare di conseguenza tutti gli altri campi EXIF (e le altre caratteristiche) dell'immagine per rendere la manipolazione completamente compatibile con la fotocamera che si vuole simulare. Effettuare questa operazione in maniera precisa e accurata non è impossibile, ma è piuttosto complesso.

6.2.2 **Analisi di thumbnail e preview**

Le immagini denominate thumbnail e preview nella maggior parte dei dispositivi moderni vengono salvate all'interno del file che contiene l'immagine principale. È possibile utilizzare tali immagini "secondarie" per effettuare diversi tipi di analisi [26]. Innanzitutto, l'assenza della *thumbnail* è considerata il più delle volte come un segnale sospetto, tuttavia può essere valutata come una caratteristica di un determinato modello di macchina fotografica. Inoltre, la risoluzione della miniatura, il suo rapporto con l'immagine principale e l'eventuale presenza di bande nere sono tratti distintivi di specifici modelli, quindi possono essere utilizzati in un'analisi comparativa.
Un'analisi molto utile riguarda, infine, il contenuto della thumbnail stessa. Se il contenuto dell'immagine principale è diverso da quello della thumbnail *(thumbnail mismatch)*, ciò può essere dovuto fondamentalmente a due motivi: 1) si è tentato di nascondere un'immagine all'interno di un'altra; 2) un errore del software di fotoritocco che non ha aggiornato correttamente la thumbnail in fase di salvataggio. Vecchie versioni di Adobe Photoshop [30] e Paint.NET [31] presentavano per l'appunto questo problema. Anche la versione corrente di IrfanView [32] ha lo stesso problema quando salva immagini RAW in JPEG.

6.2.3 **Analisi del formato JPEG**

Spesso dispositivi diversi salvano i file in formato JPEG con impostazioni differenti. Le principali fonti di variabilità sono le seguenti [26], [33]:

- Numero e valori delle tabelle di quantizzazione;
- Tabelle di Huffman;
- Sottocampionamento dei canali della crominanza.

Il principale fattore discriminante è la variabilità delle tabelle di quantizzazione [51], con il quale in pratica si determina il livello di compressione e di qualità dell'immagine. Sebbene lo standard IJG *(Independent JPEG Group)* suggerisca delle tabelle di quantizzazione da impiegare nel processo di codifica/decodifica del file [16], i diversi produttori sia hardware che software, implementano frequentemente delle tabelle ad-hoc per ogni modello, in maniera tale da massimizzare il rapporto qualità-compressione sulla base delle caratteristiche dei loro dispositivi. Se si possiede un database contenente le tabelle di quantizzazione per

ogni modello esistente, o si ha la possibilità di generare quelle di uno specifico dispositivo, allora si può identificare parzialmente, o quanto meno verificare il dispositivo/il software che ha generato l'immagine (come fa, ad esempio, il software JPEGsnoop [24]).
Questo metodo nonostante sia molto utilizzato, presenta alcune limitazioni:

- Diversi dispositivi possono utilizzare la stessa tabella di quantizzazione.
- Uno stesso dispositivo può utilizzare tabelle di quantizzazione differenti. Alcuni dispositivi utilizzano una singola tabella, altri ne utilizzano un numero limitato a seconda delle impostazioni e altri le generano dinamicamente in base alle caratteristiche della scena.
- Non è possibile realizzare un database esaustivo a causa della variabilità delle tabelle utilizzate da ogni dispositivo, ma soprattutto per la continua commercializzazione di nuove fotocamere e nuovi software.
- Come nel caso degl'altri metodi basati sul formato, un'attaccante sufficientemente esperto può ingannare l'analisi JPEG.
- In linea di massima si può verificare esclusivamente la compatibilità delle tabelle di quantizzazione con un certo dispositivo, l'univocità dell'informazione non è garantita; inoltre è complicato (se non impossibile) dimostrarne l'incompatibilità, a meno che non si sia riscontrato che il dispositivo in esame utilizza sempre e solo un set di tabelle ben specifico.

L'analisi delle tabelle di quantizzazione può essere facilmente automatizzata e combinata con l'analisi degli altri parametri della compressione JPEG (tabelle di Huffman e sottocampionamento), oltre che con la valutazione dei metadati EXIF e del formato. In questo modo si potranno compensare parzialmente le sue limitazioni.

6.2.4 **Analisi binaria**

L'analisi binaria consiste nell'esaminare a livello binario lo *stream* del file alla ricerca di determinati elementi di interesse. La verifica più semplice che si può eseguire sullo *stream* è ricercare i caratteri stampabili e, in particolare, identificare eventuali tracce di programmi di fotoritocco. Infatti, i software di *editing* salvano all'interno dell'immagine il proprio nome e, in alcuni casi, persino i dettagli dell'elaborazione. In un certo senso, un'analisi di questo tipo non fa altro che estrarre i metadati utilizzando i bit del file. Essa è molto utile perché consente di estrarre dei dati aggiuntivi che sono stati inclusi in campi non standard dell'immagine.
Un altro tipo di analisi molto interessante riguarda l'estrazione della struttura del file JPEG. Lo standard JPEG, o più precisamente JFIF *(JPEG Interchange Format)*, definisce alcuni *marker* specifici che delimitano le diverse parti del file sulla base delle informazioni che contengono. Ad esempio, ogni immagine all'interno del JPEG deve

cominciare con 0xFFD8 e terminare con 0xFFD9. Se all'interno del file è annidata un'altra immagine (una *thumbnail* o una *preview*), allora sarà visibile un'altra coppia 0xFFD8/0xFFD9.
Nello standard sono definiti altri *marker* che specificano segmenti diversi del file, quelli più comuni sono riportati nella tabella seguente.

Tabella 1. Descrizione delle principali caratteristiche di alcuni *marker* per il formato JPEG.

NOME ABBREVIATO	POSIZIONE (inizio, fine)	DIMENSIONE	NOME	DESCRIZIONE
SOI	0xFF, 0xD8	-	Start Of Image	
SOF0	0xFF, 0xC0	*Variabile*	Start Of Frame *(Baseline DCT)*	Indica che si tratta di un'immagine JPEG in modalità baseline e specifica: la larghezza, l'altezza, il numero di componenti nonché il fattore di sottocampionamento di ciascuna componente dell'immagine (ad esempio, 4:2:0).
SOF2	0xFF, 0xC2	*Variabile*	Start Of Frame *(Progressive DCT)*	Indica che si tratta di una JPEG in modalità *progressive* e specifica le stesse informazioni del segmento precedente.
DHT	0xFF, 0xC4	*Variabile*	Define Huffman Table(s)	Specifica una o più tabelle di Huffman.
DQT	0xFF, 0xDB	*Variabile*	Define Quantization Table(s)	Specifica una o più tabelle di quantizzazione.
DRI	0xFF, 0xDD	4 byte	Define Restart Interval	
SOS	0xFF, 0xDA	*Variabile*	Start Of Scan	Nelle immagini JPEG salvate in modalità baseline, è presente generalmente una singola scansione, quindi un singolo *marker*. Mentre, le immagini JPEG memorizzate in modalità progressive, di solito, contengono più scansioni e più marcatori dello stesso tipo. Questo marker specifica qual è la porzione di dati in esso contenuta ed è immediatamente seguito dai dati codificati.
APP*n*	0xFF, 0xE*n*	*Variabile*	Application-specific	Per esempio, un file JPEG contenente gli EXIF utilizza il *marker* APP1 per memorizzare i metadati, dando luogo ad una struttura molto simile a quella dei file TIFF.
COM	0xFF, 0xFE	*Variabile*	Comment	Contiene commenti di testo.
EOI	0xFF, 0xD9	-	End Of Image	

Estraendo la sequenza con tutti i *marker* d'interesse, è possibile tracciare un profilo sommario della struttura del file JPEG che è stato creato da un determinato tipo di dispositivo o software. Spesso, i JPEG generati con modelli di macchina fotografica diversi generano strutture di *marker* diverse, mentre lo stesso modello, anche se con impostazioni differenti, genera un JPEG con una struttura simile. È sempre possibile però avere dei falsi positivi, ossia di sequenze di byte corrispondenti che sono identiche a quelle dei marker.

6.3 **Analisi globale dell'immagine**

A volte l'immagine analizzata contiene dei difetti non immediatamente visibili, ma semplici tecniche di *image enhancement*, come il miglioramento del contrasto, [45] permettono di amplificare alcuni dettagli d'interesse ed evidenziare le tracce lasciate dalla manipolazione. Si tenga presente che non sarà sempre possibile discriminare in maniera certa e definita le zone manipolate nell'immagine, ma sarà possibile, se non altro, individuare delle aree sospette su cui concentrare l'analisi nei passi successivi. Molto spesso l'abilità di chi modifica l'immagine è tale da non lasciare degli indizi percepibili all'occhio umano, perciò è necessario fare ricorso a tecniche ad-hoc come quelle riportate di seguito.

Figura 1.
Didascalia immagine testo finto.

Le tecniche di analisi globale sono finalizzate a valutare la presenza di modifiche sui pixel dell'immagine, analizzando principalmente informazioni statistiche derivanti dall'analisi dei pixel e di alcune caratteristiche del formato. L'output di questi metodi è costituito da un grafico che rappresenta la distribuzione dei dati dell'immagine, analizzati con opportuni strumenti matematici. Comparandolo con quello di un'immagine acquisita con lo stesso dispositivo, si è in grado di determinare la presenza di eventuali anomalie statistiche, sebbene non sempre sia possibile localizzare la regione contenente tali irregolarità.

Queste tecniche richiedono generalmente una buona competenza da parte dell'analista per interpretare correttamente il significato dell'output, ma sono sicuramente più affidabili delle analisi basate sul formato. Infatti, esse descrivono il comportamento del dispositivo mediante degli opportuni parametri statistici, estratti dai dati dell'immagine nel dominio dei pixel o in quello DCT.

Le tecniche di analisi globale permettono di tracciare la "storia" dell'immagine riguardante le operazioni di base che possono essere state eseguite su di essa, quali salvataggio in JPEG, ridimensionamento o demosaicing. Esse sono, per certi versi, meno interessanti di quelle locali perché riescono solamente a dire se un'immagine è stata modificate senza sapere dove.

Lo svantaggio di tali tecniche è principalmente legato alla difficoltà intrinseca di automazione della procedura [11]. Supponiamo, ad esempio, di voler distinguere le immagini originali, provenienti direttamente da una fotocamera, da quelle manipolate, ottenute risalvando le originali in JPEG con Photoshop. In tal caso sarebbe necessario un classificatore che sulla base di una opportuna metrica sia in grado di distinguere tra immagini JPEG compresse una sola volta (classe A) da quelle che

sono state compresse due volte (classe B). Per poter fissare i relativi parametri, è necessario addestrare il classificatore utilizzando come input le caratteristiche statistiche che sono state estratte da un set abbastanza grande di immagini appartenenti ad entrambe le classi.
Il rischio che si corre è di avere molti falsi positivi in casi reali, poiché i risultati della classificazione sono fortemente dipendenti dal tipo, dalle dimensioni e dalla natura delle immagini che si sono utilizzate in fase di addestramento.

6.3.1 **Analisi dei coefficienti DCT**

L'analisi dei coefficienti DCT mira ad individuare le variazioni introdotte dall'algoritmo di compressione JPEG all'interno delle statistiche dei valori dei coefficienti. Il JPEG [16] è un algoritmo di compressione con perdita d'informazione: esso prevede, in fase di codifica, che i coefficienti di ciascun blocco DCT 8x8 dell'immagine siano quantizzati modo opportuno. Nel processo di quantizzazione il valore (decimale) di ciascun coefficiente DCT viene diviso per il corrispondente elemento della tabella di quantizzazione (inclusa nel codificatore) e il risultato arrotondato all'intero più vicino. Questa divisione introduce degli "errori" sistematici nei valori dei coefficienti che tendono a distribuirsi in modo caratteristico.
Di solito, i coefficienti DCT che si trovano nell'angolo in basso a destra del blocco (alta frequenza DCT) sono quantizzati a zero e possono essere trascurati. Perciò, l'analisi può essere circoscritta ai restanti coefficienti DCT localizzati nell'angolo in alto a sinistra del blocco (bassa frequenza DCT), escludendo il coefficiente in prima posizione (frequenza zero o in continua).
Una nota proprietà dei coefficienti DCT in bassa frequenza riguarda l'andamento dei loro istogrammi. In particolare, in [33] e [34] è stato osservato che gli istogrammi dei loro valori tendono ad avere una distribuzione che è caratteristica del livello di compressione dell'immagine analizzata. Nel caso di un'immagine che non è mai stata compressa (ad esempio una RAW convertita in BMP), l'istogramma presenta un picco centrale e un andamento decrescente sulle code, mentre, per un'immagine compressa più volte, assume la stessa forma ma contiene dei valori mancanti o delle forti discontinuità in posizioni periodiche. L'esistenza di questo tipo di artefatti è un "marchio" che rivela la presenza della compressione (o, più precisamente, della quantizzazione). Le tecniche basate su questo tipo di analisi, quindi, possono essere utilizzate per individuare la "storia" della compressione di un'immagine [34].
Come visto in precedenza, la maggior parte dei produttori di macchine fotografiche e di software di *editing* utilizzano tabelle di quantizzazione proprietarie per salvare l'immagine in formato JPEG. Inoltre, il contenuto di tali tabelle cambia a seconda delle impostazioni decise degli stessi produttori. Una foto manipolata, perciò, sarà con ogni probabilità, il risultato di almeno due processi di compressione distinti e sarà caratterizzata da un istogramma dei coefficienti DCT tipico delle immagini compresse più volte [53].

Affinché questo tipo di analisi risulti applicabile, è necessario che gli artefatti dovuti alla quantizzazione (singola o doppia) siano rilevabili. Nel caso di compressione multipla è necessario che le tabelle di quantizzazione impiegate siano distinte o che i fattori di qualità siano differenti. Più è piccola la differenza tra il fattori di qualità (o il rapporto dei passi di quantizzazione) utilizzati nelle compressioni successive, meno visibile risulta essere l'effetto della doppia quantizzazione. Ad esempio, comprimendo con fattore di qualità 100 (massima qualità) una qualsiasi immagine JPEG non si osserverà alcun effetto nell'andamento dell'istogramma DCT. Nonostante la presenza di artefatti caratteristici, è sempre meglio effettuare delle analisi di tipo comparativo confrontando le distribuzioni che si ottengono per l'immagine esaminata con quelle delle altre immagini, che si suppone siano state acquisite con lo stesso dispositivo.
I file da analizzare sono generalmente in formato JPEG, perciò è possibile estrarre, per tutti i canali YCbCr (Luminanza e Crominanza) disponibili, sia i coefficienti DCT che la tabella di quantizzazione dallo stream del file. Se l'immagine in esame, invece, è memorizzata in un formato non compresso, allora è necessario applicare la DCT a ciascun blocco 8x8 della stessa prima di effettuare quest'analisi. Inoltre, si tenga presente che le componenti relative alla crominanza dell'immagine (CbCr) sono molto spesso sottocampionate di un fattore 2 e i rispettivi coefficienti DCT vengono quantizzati con dei passi di quantizzazione più grandi rispetto alla luminanza. In tal caso, l'istogramma dei coefficienti DCT contiene poca informazione, tale da rendere difficile il processo di rilevazione delle periodicità introdotte della quantizzazione. Per questo motivo, la maggioranza delle volte vengono analizzati soltanto i coefficienti DCT (in bassa frequenza) che sono stati estratti dalla luminanza dell'immagine.

6.3.2 **Analisi della correlazione dei pixel**

La creazione di immagini contraffate in modo convincente richiede l'uso frequente di trasformazioni geometriche, quali ridimensionamento, rotazione, riflessione, che implicano di solito il ricampionamento dell'immagine o di una porzione di essa su una nuova griglia di campioni. L'esecuzione di tali trasformazioni implica l'uso di opportuni algoritmi di interpolazione per calcolare i valori dei pixel nell'immagine trasformata dai loro vicini.
L'effetto dell'interpolazione è quello di introdurre delle dipendenze lineari (o meno) tra gruppi di campioni vicini. Analogamente alla doppia quantizzazione, le trasformazioni geometriche introducono degli artefatti periodici nella correlazione dei pixel dell'immagine che sono caratteristici del tipo di algoritmo d'interpolazione utilizzato e che dipendono dall'entità del ricampionamento.
Uno dei metodi per misurare la correlazione è basato sul calcolo della covarianza dei valori dei pixel che si trovano all'interno di un certo intorno, sia orizzontalmente che verticalmente. Il risultato di quest'analisi è un grafico che presenta dei picchi molto pronunciati per le immagini che sono state ricampionate.
Queste tecniche sono particolarmente efficaci nel caso in cui si vuole

capire se le immagini analizzate sono state o meno acquisite alla risoluzione nativa del sensore di un determinato dispositivo. Le fotografie, ad esempio, presentano un picco molto pronunciato al centro dello spettro a causa dell'interpolazione dei valori provenienti dal CFA, mentre le immagini che sono state generate completamente al computer non hanno alcun picco centrale.
Si tenga presente che i risultati possono essere influenzati dalla presenza di altre correlazioni presenti nell'immagine come accade, ad esempio, per la compressione JPEG; in questo caso i blocking artifact producono dei picchi aggiuntivi in posizioni fisse. Allo stesso modo, la presenza di regioni contenenti degli edge molto forti o delle strutture significative può dar luogo a delle distribuzioni molto simili a quelle delle immagini interpolate.
Come nel caso della tecnica basata sui coefficienti DCT, ha più senso effettuare delle analisi di tipo comparativo piuttosto che assoluto, quindi è sempre meglio confrontare l'output dell'immagine esaminata con quello derivante dalle immagini di riferimento che si suppone siano state catturate dallo stesso dispositivo.

6.3.3 **Analisi di intensità e colori**

Tali tecniche sono molto utili per esaminare immagini che sono state modificate con delle operazioni di regolazione della luminosità al fine di correggerne alcuni difetti di acquisizione. Nel caso in cui l'immagine analizzata provenga direttamente da un determinato dispositivo è molto probabile che l'istogramma dei suoi valori segua un andamento regolare e senza variazioni improvvise. Mentre, nel caso in cui sia stata elaborata in modo tale da regolare l'intensità dei pixel, è possibile che l'istogramma contenga degli artefatti che variano a seconda della manipolazione di luminosità eseguita [35].
L'applicazione di operazioni come l'espansione del contrasto, l'equalizzazione d'istogramma e la LUT, modificano la gamma dinamica dei livelli di luminosità dell'immagine. Ad esempio, se si utilizza il filtro "Curves" di Photoshop per effettuare un'espansione del contrasto dell'immagine, saranno introdotti nell'istogramma dei picchi e delle valli che si ripetono periodicamente. Il filtro "Histogram Equalization", invece, effettua una ridistribuzione dei livelli di luminosità sull'intero intervallo dei possibili valori dell'immagine, rendendo l'istogramma approssimativamente piatto.
È possibile analizzare l'immagine anche mediante delle tecniche che valutano l'istogramma dei colori dell'immagine piuttosto che quello dell'intensità luminosa. L'analisi con questo tipo di tecniche viene eseguita di solito negli spazi di colore HSV e Lab [36]. Dal momento che tutti i valori HSV o Lab possono essere rappresentati da valori RGB e che la presenza di valori estremi è piuttosto improbabile in un'immagine naturale, un istogramma di colori con una distribuzione molto estesa o che contiene dei pattern caratteristici può essere indizio di una manipolazione eccessiva del colore nella foto.
A differenza delle tecniche di analisi globali descritte in precedenza, que-

ste non possono essere utilizzate per confrontare immagini provenienti dallo stesso dispositivo. Infatti, immagini della stessa scena possono essere caratterizzate da condizioni di illuminazione e di esposizione differenti, quindi da istogrammi di luminosità e di colore diversi, senza per questo motivo dover destar sospetti. L'analisi consente solo di diagnosticare i difetti dell'immagine o il tipo di trasformazione che è stata effettuata.

6.4 Identificazione del dispositivo

Se ci si trova a dover accertare la "paternità" di un'immagine digitale, l'identificazione del dispositivo avviene su tre livelli differenti.

1) Definizione del **tipo di dispositivo**, ossia se trattasi di un'immagine:
- proveniente da una fotocamera digitale;
- scannerizzata;
- creata interamente al computer
  (ad esempio con un software di *rendering*).

2) Definizione del **modello del dispositivo**, ossia identificare il nome del produttore e del modello particolare di macchina fotografica (o, alternativamente, scanner). Le tecniche di questo tipo si riferiscono alle analisi descritte nei paragrafi precedenti che includono implicitamente anche una valutazione sul tipo di dispositivo.

3) Identificazione dell'**esemplare specifico**. Sotto alcune ipotesi è possibile verificare che una certa immagine è stata scattata da uno specifico dispositivo in possesso di un determinato soggetto, similmente a ciò che si fa con le armi da fuoco. Non a caso, tecniche di questo tipo sono chiamate ***camera ballistic***.
Le tecniche finalizzate al riconoscimento del dispositivo partono dal presupposto che ogni esemplare di macchina fotografica prodotto, anche se dello stesso modello, è soggetto ad alcune imperfezioni e variazioni, introdotte durante la fase di fabbricazione, che sono uniche e specifiche. Queste specificano univocamente un dispositivo e possono essere considerate come "un'impronta digitale" dello stesso nelle foto. Tra le varie tecniche presenti in letteratura, quella che viene universalmente riconosciuta ed utilizzata nelle applicazioni pratiche è quella che sfrutta il PRNU globale, illustrato nel sottoparagrafo successivo.
Diversi studi sono stati fatti anche sull'analisi dei pixel "difettosi" del sensore della macchina fotografica (ossia quelli che rimangono sempre ad un valore fisso). Tuttavia, con il miglioramento delle tecniche di fabbricazione e con l'impiego sempre più rilevante di algoritmi di *post-processing* all'interno delle macchine fotografiche, tali pixel sono sempre meno presenti e poco visibili, quindi difficili da individuare e analizzare.

6.4.1 Analisi globale del PRNU

Per stabilire se un'immagine proviene da un determinato dispositivo, è necessario creare un CRP (*Camera Reference Pattern*), cioè un PRNU

di riferimento. A tal fine è necessario avere diverse decine di immagini di riferimento create dal dispositivo in esame.
Successivamente, il PRNU dell'immagine analizzata viene confrontato con il CRP. Tanto più alta è la correlazione fra i due, tanto più è probabile che l'immagine provenga dal dispositivo in esame. Mediante soglie opportune, calcolate caso per caso, si può suddividere l'intervallo dei possibili valori di correlazione in sotto-intervalli e classificare il valore ottenuto in categorie distinte (ad esempio Low, Medium, High). Si è osservato che l'affidabilità del metodo tende a decrescere con la risoluzione dell'immagine, poiché il CRP diventa meno significativo da un punto di vista statistico.
Nell'analisi del PRNU bisogna applicare particolari accorgimenti nel caso in cui le immagini siano state sottoposte, in fase di creazione o di post-processing, ad operazioni geometriche quali ridimensionamento, ritaglio, zoom digitale, rotazione o riflessione.

6.5 Analisi locale dell'immagine

L'analisi locale dell'immagine permette di evidenziare localmente eventuali artefatti nelle caratteristiche dei pixel, che possono essere dovuti alla presenza di un particolare tipo di manipolazione. L'output è generalmente un'immagine, ottenuta applicando un particolare filtraggio. Nella maggior parte dei casi, l'analista deve avere una certa competenza nell'interpretare correttamente le immagini risultanti e identificare le zone sospette. Talvolta è possibile automatizzare il metodo con delle soglie, al fine di estrarre una maschera binaria delle zone sospette. In ogni caso è sempre necessaria una valutazione critica del risultato da parte dell'esperto. Ad esempio, le regioni sature dell'immagine possono dare spesso dei risultati errati (tipicamente falsi positivi). In tal caso, è compito dell'analista comprendere che l'identificazione di aree sospette in presenza di saturazione spesso non è affidabile.
L'efficienza delle tecniche di analisi locale dipende fortemente dal tipo di *processing* che viene applicato alle immagini dopo la manipolazione. Ad esempio, se successivamente alla modifica, le immagini sono state compresse o ridimensionate in modo eccessivo, la maggior parte delle tracce visibili con questi algoritmi vengono per lo più rimosse.

6.5.1 **ELA**

L'ELA (*Error Level Analysis*), talvolta chiamato JPEG Ghost [37], è un metodo che permette di evidenziare zone dell'immagine che sono state compresse in maniera diversa. L'idea di base della tecnica in questione è piuttosto semplice: bisogna ricomprimere l'immagine analizzata in formato JPEG (con fattore di qualità variabile) e successivamente calcolare la differenza con l'immagine risultante. In questo modo le regioni che sono state soggette a modifiche dovrebbero risaltare dal resto dell'immagine perché caratterizzate da un "rumore di compressione" differente. Ciò non è sempre vero, ma nella sua semplicità è uno strumento che può dare buoni risultati.

L'ELA solitamente funziona bene nel caso in cui ci si trovi di fronte ad una strategia di *splicing* o *copy-paste*, che consiste nell'inserire una parte di un'immagine in un'altra.

6.5.2 **Mappa DCT**

Un'altra tecnica molto semplice, ma al tempo stesso molto efficace, è la visualizzazione dei coefficienti DCT di un'immagine JPEG [38]. Durante la fase di decodifica di un file JPEG, i coefficienti DCT di ciascun blocco 8x8 dell'immagine vengono moltiplicati per i corrispondenti elementi della tabella di quantizzazione e convertiti nei valori dei pixel applicando la trasformata DCT inversa. Nella mappa DCT vengono visualizzati i valori dei coefficienti non decodificati, con la possibilità di scalarli per un dato fattore moltiplicativo. Nel caso di immagini non JPEG, sarà possibile visualizzare solo i coefficienti decodificati che sono estratti applicando all'immagine la DCT a blocchi.
La mappa DCT dà buoni risultati soprattutto nel caso di applicazione di filtri di riempimento o di duplicazione di regioni all'interno della stessa immagine finalizzati a nascondere parti dell'immagine, come il "*Content Aware Fill*" di Adobe Photoshop.

6.5.3 **Mappa di probabilità**

La mappa di probabilità permette di visualizzare la correlazione locale fra i vari pixel dell'immagine [39]. Tale correlazione è dovuta agli algoritmi di interpolazione impiegati nelle operazioni di trasformazione geometrica dell'immagine o di una parte di essa, ma può esser legata anche all'algoritmo di demosaicing utilizzato dalla macchina fotografica per riempire i buchi lasciati dal CFA. Gli algoritmi d'interpolazione modificano le relazioni spaziali tra i pixel, per cui è sufficiente calcolare il grado di correlazione dei pixel vicini per capire se sono state applicate o meno delle operazioni di ricampionamento. Il metodo più semplice per far ciò è calcolare la differenza pesata tra i valori del pixel che si trovano all'interno di ciascun blocco 3x3 dell'immagine [39]. Differenze (errori di predizione) molto alte indicheranno una correlazione molto bassa e daranno luogo a dei valori molto piccoli della mappa, e viceversa.
La mappa di probabilità è particolarmente efficace nel caso in cui siano unite due immagini o regioni generate da macchine fotografiche/software differenti, cioè caratterizzate da artefatti d'interpolazione diversi.

6.5.4 **Mappa del rumore**

La mappa di rumore permette di visualizzare le inconsistenze del rumore che sono presenti in diverse parti dell'immagine. Uno dei metodi maggiormente usati consiste nel mappare la varianza del rumore nell'intorno di ogni pixel. Tale varianza può essere calcolata in diversi modi: quello che dà i risultati migliori è la stima della Kurtosis dei coefficienti DCT [40].

6.5.5 **Analisi locale del PRNU**

Come indicato in [41] è possibile confrontare localmente (blocco a bloc-

co) le diverse aree dell'immagine alla ricerca di zone in cui correlazione tra PRNU e il CRP di riferimento sia particolarmente bassa. Il vantaggio di questo tipo di analisi è che riesce a dare un risultato abbastanza affidabile in maniera rapida ed automatica. Affinché funzioni correttamente, sono necessarie un certo numero di immagini generate dalla macchina fotografica di riferimento che non siano state in alcun modo alterate. Più avanti vedremo una applicazione al calcolo del PRNU che permette di verificare se una fotografia proviene da un determinato dispositivo.

6.5.6 **Analisi dei cloni**

Un caso particolare di manipolazione è la duplicazione di regioni specifiche dell'immagine all'interno della stessa. La clonazione può essere utilizzata per aggiungere contenuto (ad esempio copiando un soggetto più volte sullo sfondo) o per rimuovere delle parti indesiderate (ad esempio copiando lo sfondo sopra un soggetto che si vuole nascondere).
Le tecniche di riconoscimento dei cloni sono principalmente di due tipologie, basate sui blocchi e sui *keypoint*. Le tecniche basate su **blocchi** sono concettualmente molto semplici: mirano a trovare gruppi di pixel identici (o molto simili) su varie parti dell'immagine [42]. Esse presentano però due problemi:

1) Sono caratterizzate da una complessità computazionale molto alta, che cresce esponenzialmente con la risoluzione delle immagini e del tipo di trasformazione geometrica considerata. Ad esempio, le immagini scattate con le macchine fotografiche moderne (che sono nell'ordine dei 10-20 Megapixel) possono richiedere un'elaborazione nell'ordine delle decine di minuti. L'onere computazionale può essere limitato con opportuni accorgimenti algoritmici, ma questi non sono sufficienti a ridurre in modo significativo i tempi di calcolo.
2) Funzionano solamente su gruppi di pixel quasi uguali: se il clone è stato ruotato o ridimensionato al di fuori del range considerato diventano poco affidabili. Anche una semplice compressione JPEG va ad introdurre delle modifiche tali per cui il metodo tende a classificare erroneamente.

In generale i metodi basati sui blocchi possono produrre falsi positivi su aree uniformi come porzioni di cielo o di muro.
Le tecniche basate sui **keypoint**, invece, identificano i punti ad alto contenuto informativo all'interno di un'immagine [36]. Se esistono dei gruppi di punti che possono essere in corrispondenza tra loro, allora c'è un'alta probabilità di trovarsi di fronte ad un clone. Questo tipo di tecniche funzionano correttamente anche nel caso in cui le zone clonate sono state ruotate o ridimensionate, mentre falliscono nel caso in cui venga duplicata una parte dello sfondo per coprire un soggetto (non esistono punti con particolare dettaglio).
I metodi basati sui keypoint possono produrre dei falsi positivi se ci sono degli elementi simili che si ripetono nella scena, anche se questi ultimi non sono il frutto di una clonazione digitale. I tempi di calcolo sono sempre di un certo rilievo, ma molto inferiori alle analisi basate sui blocchi.

6.6 Analisi dettagliata della scena

Le tecniche d'analisi della scena hanno il fine di esaminare le caratteristiche complessive della scena, piuttosto che interpretare le statistiche ricavate da alcune caratteristiche dei pixel. A differenza degli altri, questo approccio può essere applicato anche nel caso di immagini analogiche trasformate successivamente in digitale (ad esempio immagini scannerizzate).
L'idea di base di tale analisi è che la maggior parte delle manipolazioni contengono qualche tipo di errore che non è visibile a occhio nudo, ma può essere evidenziato da un'analisi opportuna. Infatti, è praticamente impossibile cercare di falsificare un'immagine facendo in modo che: il modello della scena rispetti tutti i modelli fisici d'illuminazione della stessa e, contemporaneamente, non presenti alcuna irregolarità dal punto di vista della prospettiva e delle ombre generate dagli oggetti in essa presenti; a meno che l'immagine non sia stata realizzata completamente in computer grafica.
Il limite principale delle analisi della scena risiede nel fatto che possono essere difficilmente automatizzate: ogni immagine deve essere esaminata con metodi specifici (non sempre applicabili) e necessitato di un'elevata competenza da parte dell'analista. Generalmente, esse sono più efficaci nell'analisi di immagini in cui è stata aggiunta dell'informazione piuttosto che rimossa.

6.6.1 **Analisi dell'illuminazione**

In questa categoria sono incluse tutte le tecniche che sono utilizzate per esaminare l'illuminazione della scena. Esse sono molto complesse da realizzare a causa della complessità del mondo reale che non sempre permette di applicare i modelli fisico-matematici (fonte di luce singola, oggetti geometrici di base). Di solito ci si limita a riprodurre la scena analizzata con un software di rendering ed a verificare che l'illuminazione risulti coerente nelle varie regioni che la compongono.
Una tecnica molto semplice è l'analisi del gradiente di luminosità [19], che permette di visualizzare meglio alcune inconsistenze nell'immagine, creando una mappa in cui il valore di ciascun pixel è legato alla direzione e all'intensità della luce.

6.6.2 **Analisi della geometria**

Quando si inserisce un oggetto estraneo in una scena, è spesso molto difficile essere precisi nel rispettare la prospettiva del resto dell'immagine o/e nel creare delle ombre perfettamente realistiche. Alcuni metodi presenti in letteratura [20], [43] permettono di eseguire un'analisi del punto principale dell'immagine (la proiezione del centro ottico della fotocamera sul piano immagine) e delle ombre per ricercare delle inconsistenze che segnalano la presenza di zone sospette.
Infine, possono essere utilizzate delle tecniche di fotogrammetria per verificare che all'interno dell'immagine ci sono elementi con dimensioni irrealistiche o diverse da quelle attese.

6.7 Analisi conclusive

L'ultima fase, per certi versi la più complessa, è quella di mettere assieme i risultati ottenuti con le varie analisi e di trarre delle conclusioni sull'autenticità dell'immagine. In generale, non sarà mai possibile dimostrare che un'immagine è autentica, ma solamente che non è stato possibile trovare elementi che confutino questa tesi. Sarà, invece, possibile dimostrare, spesso con un certo margine di sicurezza, che l'immagine non è autentica se è stata trovata almeno una traccia, non giustificabile altrimenti, di una manipolazione.

Per ogni categoria di analisi, potrà quindi essere possibile trarre delle conclusioni del tipo:
- Coerente con un'immagine originale (V)
- Incoerente con un'immagine originale (X)
- Non applicabile
- Inconclusiva

Tabella 2. Al termine di ogni analisi dovrà essere compilata una tabella che riporti le valutazioni per ogni gruppo di accertamenti.

	ESITO DELL'ANALISI	NOTE
Analisi del formato		
Analisi globale		
Analisi della sorgente		
Analisi locale		
Analisi della scena		
Conclusioni		

7. UN CASO DI STUDIO

A completamento della teoria e delle linee guida esposti nel capitolo precedente, esponiamo ora un caso di studio che permette di apprezzare visivamente i risultati che si ottengono con tale metodologia applicati ad uno scenario investigativo reale. Premettiamo che non in tutte le situazioni disponiamo di immagini con cui abbiamo la possibilità di usare tutti i metodi elencati precedentemente. Anche e soprattutto in questa fase entra in gioco l'abilità e l'esperienza dell'analista, il quale dovrà di volta in volta capire le "armi" più adatte per approcciarsi all'esame.

7.1 Analisi generale

Supponiamo che ci venga consegnato il file "IMG_20131016_183918.jpg", denominato di seguito come "evidence" e uno smartphone LG Nexus 4 che si suppone sia stato utilizzato per creare l'immagine. I quesiti cui rispondere sono i seguenti:

- Il file dell'immagine è autentico?

- L'immagine è autentica o sono state applicate delle manipolazioni di contenuto? Se si, dove?
- L'immagine è stata scattata da uno smartphone Nexus 4?
- L'immagine è stata scattata precisamente dall'esemplare di Nexus 4 in nostro possesso?

Se successivamente si vogliono eseguire delle analisi di tipo comparativo è necessario procurare alcune immagini di riferimento generate da un esemplare dello stesso modello, per cui dovremo utilizzare il dispositivo in nostro possesso per ottenere delle foto di prova.

7.1.1 **Analisi visiva dell'immagine**

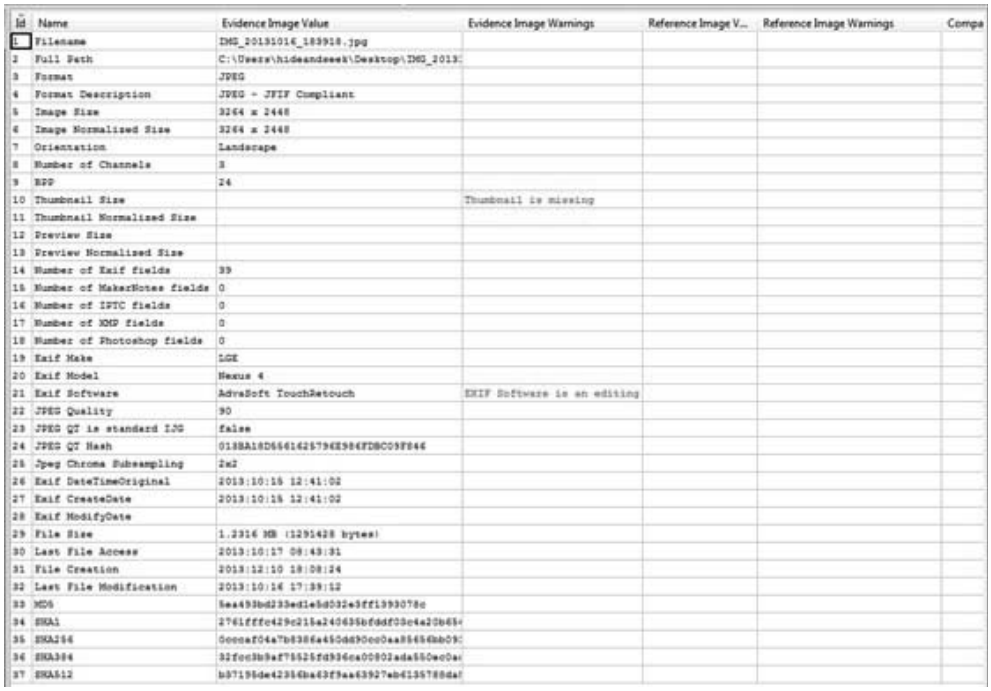
L'immagine oggetto di analisi è riportata in figura 14. L'analisi visuale non evidenzia inconsistenze di alcun tipo.

Figura 14. Immagine oggetto degli accertamenti. Ad una prima analisi visuale non vi sono particolari elementi degni di nota.

7.1.2 **Analisi generale del file**

Nella figura 15 è illustrato il risultato dell'analisi generale del formato dell'immagine. Si notino i seguenti elementi sospetti:

1) la thumbnail dell'immagine non è presente (scritta in rosso "Thumbnail is missing" nel campo 10);
2) il campo 21 (Software dei metadati EXIF) contiene "AdvaSoft Touch Retouch", sicuramente un nome non molto promettente per l'analisi dell'autenticità;
3) le tabelle di quantizzazione non sono compatibili con quelle conosciute (esito "false" nel campo 23) per il dispositivo in questione. Tuttavia, è possibile che il database di tabelle di quantizzazione per il determinato dispositivo sia incompleto.



Id	Name	Evidence Image Value	Evidence Image Warnings	Reference Image V...	Reference Image Warnings	Compa
1	Filename	IMG_20131016_183918.jpg				
2	Full Path	C:\Users\hideandseek\Desktop\IMG_2013				
3	Format	JPEG				
4	Format Description	JPEG - JFIF Compliant				
5	Image Size	3264 x 2448				
6	Image Normalized Size	3264 x 2448				
7	Orientation	Landscape				
8	Number of Channels	3				
9	BPP	24				
10	Thumbnail Size		Thumbnail is missing			
11	Thumbnail Normalized Size					
12	Preview Size					
13	Preview Normalized Size					
14	Number of Exif fields	39				
15	Number of MakerNotes fields	0				
16	Number of IPTC fields	0				
17	Number of XMP fields	0				
18	Number of Photoshop fields	0				
19	Exif Make	LGE				
20	Exif Model	Nexus 4				
21	Exif Software	AdvaSoft TouchRetouch	EXIF Software is an editing			
22	JPEG Quality	90				
23	JPEG QT is standard IJG	false				
24	JPEG QT Hash	013BA18D6561625794E984FDBC09F846				
25	Jpeg Chroma Subsampling	2x2				
26	Exif DateTimeOriginal	2013:10:15 12:41:02				
27	Exif CreateDate	2013:10:15 12:41:02				
28	Exif ModifyDate					
29	File Size	1.2316 MB (1291428 bytes)				
30	Last File Access	2013:10:17 08:43:31				
31	File Creation	2013:12:10 18:08:24				
32	Last File Modification	2013:10:16 17:39:12				
33	MD5	8ea439bd233ed1e5d032e3ff1393078c				
34	SHA1	2761fffc429c215a240635bfddf03c4a20b65				
35	SHA256	6cccaf04a7b8386e465dd90cc0aa85654bb09				
36	SHA384	32fcc3b9af71525fd936ca00802ada550ec0a				
37	SHA512	b37195de42316ba63f9aa63927eb4135788da				

Figura 15. L'analisi di formato dell'immagine (qui uno stralcio) evidenzia la mancanza della miniatura e l'utilizzo di un software di *editing*.

Questa prima analisi fa già dubitare dell'autenticità del file. Per approfondire la questione è possibile eseguire un'analisi di tipo comparativo, acquisendo alcune immagini di prova con lo smartphone in esame. Da questo tipo di esame notiamo le seguenti differenze (che confermano i dubbi evidenziati precedentemente) evidenziate in figura 16:

1) nell'immagine di riferimento è presente la thumbnail (campi 10 ed 11 - quinta colonna);
2) il numero di metadati EXIF nell'immagine di riferimento e quella analizzata sono diversi (campo 14 colonne 3 e 5);
3) nell'immagine di riferimento non è presente l'indicazione dell'uso di software per l'editing degli EXIF (campo 21 colonne 5 e 6)
4) la tabella di quantizzazione JPEG è diversa (campo 22 colonne 3 e 5).

A volte è tecnicamente impossibile ricreare tutte le condizioni di compatibilità a causa dell'elevato numero di impostazioni presenti sui dispositivi moderni. In ogni caso è importante acquisire molte immagini di prova.
In particolare, usando l'applicazione di default dello smartphone per scattare fotografie, si riscontra che:

1) non è possibile creare immagini senza thumbnail;
2) nelle immagini create è presente sempre una sola tabella di quantizzazione, corrispondente a quella della foto di riferimento (JPEG Quality =95);

3) il numero di dati EXIF possono variare, perché, ad esempio, la localizzazione GPS è abilitata o meno.

Id	Name	Evidence Image Value	Evidence Image Warnings	Reference Image Value	Reference Image Warnings	Comparison
1	Filename	IMG_20131016_183918.jpg		IMG_20131016_183922.jpg		Different
2	Full Path	C:\Users\hideandseek\De		C:\Users\hideandseek\De		Different
3	Format	JPEG		JPEG		
4	Format Description	JPEG - JFIF Compliant		JPEG - JFIF Compliant		
5	Image Size	3264 x 2448		3264 x 2448		
6	Image Normalized Size	3264 x 2448		3264 x 2448		
7	Orientation	Landscape		Landscape		
8	Number of Channels	3		3		
9	BPP	24		24		
10	Thumbnail Size		Thumbnail is missing	512 x 384		Different
11	Thumbnail Normalized Size			512 x 384		Different
12	Preview Size					
13	Preview Normalized Size					
14	Number of Exif fields	39		37		Different
15	Number of MakerNotes fields	0		0		
16	Number of IPTC fields	0		0		
17	Number of XMP fields	0		0		
18	Number of Photoshop fields	0		0		
19	Exif Make	LGE		LGE		
20	Exif Model	Nexus 4		Nexus 4		
21	Exif Software	AdvaSoft TouchRetouch	EXIF Software is an editing			Different
22	JPEG Quality	90		95		Different
23	JPEG QT is standard IJG	false		false		
24	JPEG QT Hash	0139A18D68616257962E96F		01E764F8ECB6C14A61FF83F		Different
25	Jpeg Chroma Subsampling	2x2		2x2		
26	Exif DateTimeOriginal	2013:10:16 12:41:02		2013:10:16 12:41:02		
27	Exif CreateDate	2013:10:16 12:41:02		2013:10:16 12:41:02		
28	Exif ModifyDate					
29	File Size	1.2316 MB (1291428 byte		1.6720 MB (1753189 byte		Different
30	Last File Access	2013:10:17 09:43:31		2013:10:17 09:43:31		
31	File Creation	2013:12:10 18:08:24		2013:12:10 18:08:24		
32	Last File Modification	2013:10:16 17:39:12		2013:10:16 11:41:03		Different
33	MD5	5ea493bd233ed1a5d032e3f		c6e316ef51a03384ecfc1f9		Different
34	SHA1	2761fffc429c215a240635b		2a3c8999d0a6066391cee4b		Different
35	SHA256	0cccaf04a7b8384a450dd90		7b1b56606ac2ff8a0714796		Different
36	SHA384	32fcc3b8af76525fd936ca0		df30c4330841efde75c4ba3		Different
37	SHA512	b37195de42364ba63f9aa63		5c9d119cc3004d3c2cb355a		Different

7.2 Analisi del file

Analizzando in dettaglio i dati EXIF dell'immagine (figura 17) si nota che è più volte riportato il campo Software con la dicitura "AdvaSoft TouchRetouch" assieme ad altre caratteristiche dell'immagine. Notiamo inoltre che nell'immagine sono presenti i dati relativi alle coordinate GPS, con cui è possibile localizzare il luogo dello scatto utilizzando un qualsiasi servizio di mappatura on line. Questa informazione può essere a volte molto interessante per la validazione dell'autenticità del contenuto. Nella figura 18 è visualizzato il risultato dell'immissione delle coordinate GPS (campi 43 e 44) in Google Maps.

Figura 16.
L'analisi comparativa dei dati di formato evidenzia alcune diversità tra l'immagine esaminare e quella di riferimento (scattata successivamente con lo stesso apparato): in quest'ultima è presente la *thumbnail*, vi sono meno campi testuali e non risulta alcun riferimento a software per l'*editing*.

Figura 17. L'analisi dei dati EXIF inclusi nel file da esaminare. Nella terza colonna si notano i riferimenti al modello del telefono ed al software di editing.

Id	Name		Evidence Image Value	Reference Im
1	[EXIF]	Make	LGE	
2	[EXIF]	Model	Nexus 4	
3	[EXIF]	Orientation	Horizontal (normal)	
4	[EXIF]	XResolution	72	
5	[EXIF]	YResolution	72	
6	[EXIF]	ResolutionUnit	inches	
7	[EXIF]	Software	AdvaSoft TouchRetouch	
8	[EXIF]	YCbCrPositioning	Centered	
9	[EXIF]	Software	AdvaSoft TouchRetouch	
10	[EXIF]	ExposureTime	1/30	
11	[EXIF]	FNumber	2.7	
12	[EXIF]	ISO	100	
13	[EXIF]	ExifVersion	0220	
14	[EXIF]	DateTimeOriginal	2013:10:15 12:41:02	
15	[EXIF]	CreateDate	2013:10:15 12:41:02	
16	[EXIF]	ComponentsConfiguration	Y, Cb, Cr, -	
17	[EXIF]	FocalLength	4.6 mm	
18	[EXIF]	FlashpixVersion	0100	
19	[EXIF]	ColorSpace	sRGB	
20	[EXIF]	ExifImageWidth	3264	
21	[EXIF]	ExifImageHeight	2448	
22	[EXIF]	InteropIndex	R98 - DCF basic file (	
23	[EXIF]	InteropVersion	0100	
24	[EXIF]	GPSLatitudeRef	North	
25	[EXIF]	GPSLatitude	45:39:26.74	
26	[EXIF]	GPSLongitudeRef	East	
27	[EXIF]	GPSLongitude	13:49:46.98	
28	[EXIF]	GPSAltitudeRef	Above Sea Level	
29	[EXIF]	GPSAltitude	363.6 m	
30	[EXIF]	GPSTimeStamp	10:41:03	
31	[EXIF]	GPSImgDirectionRef	Magnetic North	
32	[EXIF]	GPSImgDirection	78	
33	[EXIF]	GPSProcessingMethod	ASCII	
34	[EXIF]	GPSDateStamp	2013:10:15	
35	[EXIF]	Compression	JPEG (old-style)	
36	[EXIF]	XResolution	72	
37	[EXIF]	YResolution	72	
38	[EXIF]	ResolutionUnit	inches	
39	[EXIF]	Software	AdvaSoft TouchRetouch	
40	[Composite]	Aperture	2.7	
41	[Composite]	GPSAltitude	363.5 m Above Sea Leve	
42	[Composite]	GPSDateTime	2013:10:15 10:41:03Z	
43	[Composite]	GPSLatitude	45:39:26.74 N	
44	[Composite]	GPSLongitude	13:49:46.98 E	
45	[Composite]	GPSPosition	45:39:26.74 N, 13:49:4	

Figura 18.
Esito dell'interrogazione tramite Google Maps effettuata inserendo le coordinate GPS presenti nel campo GPSPosition nei dati EXIF.

7.2.1 **Analisi di thumbnail e preview**

Come visto nella analisi iniziale sul formato, il file è privo di thumbnail e preview (figura 16), mentre quello di riferimento ha la thumbnail ma non la preview (figura 19, quinta colonna). Mancando la thumbnail, non è ovviamente possibile fare un analisi della sua compatibilità con l'immagine principale.

10	Thumbnail Size		Thumbnail is missing	512 x 384		Different
11	Thumbnail Normalized Size			512 x 384		Different
12	Preview Size					
13	Preview Normalized Size					

Figura 19.
Nell'immagine di riferimento è presente la thumbnail, a differenza dell'immagine in esame, mentre per quanto riguarda la preview, anche in questo caso è mancante.

7.2.2 **Analisi del formato JPEG**

L'analisi del file JPEG identifica la tabella di quantizzazione e le caratteristiche di sottocampionamento, come illustrato nella figura 20. Sebbene la tabella di quantizzazione utilizzata non sia di tipo standard, risulta impiegata in più di un centinaio di modelli di fotocamera (per motivi di spazio tale lista non viene riportata) e in un software di photo editing (ACDSee [56]). Essa ha, quindi, carattere scarsamente identificativo.

Figura 20. Alcuni dati EXIF riferiti alla compressione JPEG dell'immagine. L'analisi comparativa dei parametri della compressione JPEG evidenzia sostanziali diversità tra l'immagine da esaminare e quella di riferimento: il fattore di qualità, le tabelle di compressione, e tutti i dati relativi alla miniatura, che nell'immagine sotto esame sono differenti o totalmente assenti.

Id	Name	Evidence Image Value	Reference Image Value	Comparison
5	Image Quality	90	95	Different
6	Standard Table	false	false	
7	Color Space	YCbCr	YCbCr	
8	Chroma Subsampling	2x2	2x2	
9	QT Hash	[illegible]	[illegible]	Different
10	QT 1 (Luma)	3 2 2 3 5 8 10 12 2 2 3 4 5 12 12 11 3 3 3 5 8 11 14 11 3 3 4 6 10 17 16 12 4 4 7 11 14 22 21 15 5 7 11 13 16 21 23 18 10 13 16 17 21 24 24 20 14 18 19 20 22 20 21 20	2 1 1 2 2 4 5 6 1 1 1 2 3 6 6 6 1 1 2 2 4 6 7 6 1 2 2 3 5 9 8 6 2 2 4 6 7 11 10 8 2 4 6 6 8 10 11 9 5 6 8 9 10 12 12 10 7 9 10 10 11 10 10 10	Different
11	QT 2 (Chroma)	3 4 5 9 20 20 20 20 4 4 5 13 20 20 20 20 5 5 11 20 20 20 20 20 9 13 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	2 2 2 5 10 10 10 10 2 2 3 7 10 10 10 10 2 3 6 10 10 10 10 10 5 7 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10	Different
12	QT 3 (Chroma)			
13	Thumbnail Image Quality		75	Different
14	Thumbnail Standard Table		false	Different
15	Thumbnail Color Space		YCbCr	Different
16	Thumbnail Chroma Subsampling		2x2	Different
17	Thumbnail QT Hash		[illegible]	Different
18	Thumbnail QT 1 (Luma)		8 6 5 8 12 20 26 31 6 6 7 10 13 29 30 28 7 7 8 12 20 29 35 28 7 9 11 15 26 44 40 31 9 11 19 28 34 55 52 39 12 18 28 32 41 52 57 46 25 32 39 44 52 61 60 51 36 46 48 49 56 50 52 50	Different
19	Thumbnail QT 2 (Chroma)		9 9 12 24 50 50 50 50 9 11 13 33 50 50 50 50 12 13 28 50 50 50 50 50 24 33 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50 50	Different
20	Thumbnail QT 3 (Chroma)			

Confrontando la tabella di quantizzazione in esame con quella dell'immagine di riferimento, si ha un'ulteriore controprova che la stessa non è compatibile con lo smartphone Nexus 4.

7.2.3 Analisi binaria del file

La struttura del file JPEG dell'immagine analizzata è confrontata con quella dell'immagine di riferimento. Come si vede in figura 21 la sequenza dei marker è notevolmente diversa.

Figura 21. L'analisi comparativa della sequenza dei marker evidenzia molte diversità tra l'immagine da esaminare e quella di riferimento.

Evidence Image Value	Reference Image Value
00000000: FF, D8 - SOI: Start of Image	00000000: FF, D8 - SOI: Start of Image
00000002: FF, E1 - APP1: EXIF	00000002: FF, E1 - APP1: EXIF
	000002E9: FF, D8 - SOI: Start of Image
00000344: FF, DB - DQT: Define Quantization Table(s)	000002EB: FF, DB - DQT: Define Quantization Table(s)
	00000371: FF, C0 - SOFO: Start of Frame (Baseline DCT)
	00000384: FF, C4 - DHT: Define Huffman Table(s)
	00000528: FF, DA - SOS: Start Of Scan
	00004909: FF, D9 - EOI: End Of Image
00000389: FF, DB - DQT: Define Quantization Table(s)	0000490B: FF, DB - DQT: Define Quantization Table(s)
000003CE: FF, C0 - SOFO: Start of Frame (Baseline DCT)	00004991: FF, C0 - SOFO: Start of Frame (Baseline DCT)
000003E1: FF, C4 - DHT: Define Huffman Table(s)	000049A4: FF, C4 - DHT: Define Huffman Table(s)
00000402: FF, C4 - DHT: Define Huffman Table(s)	
000004B9: FF, C4 - DHT: Define Huffman Table(s)	
000004DA: FF, C4 - DHT: Define Huffman Table(s)	
00000591: FF, DA - SOS: Start Of Scan	00004B48: FF, DA - SOS: Start Of Scan
0013B48E: FF, D9 - EOI: End Of Image	001AC063: FF, D9 - EOI: End Of Image

Analizzando lo stream con un visualizzatore esadecimale si può notare (figura 22 colonna di destra) la presenza delle stringhe relative al nome del dispositivo (Nexus 4) ed al software (AdvaSoft TouchRetouch).

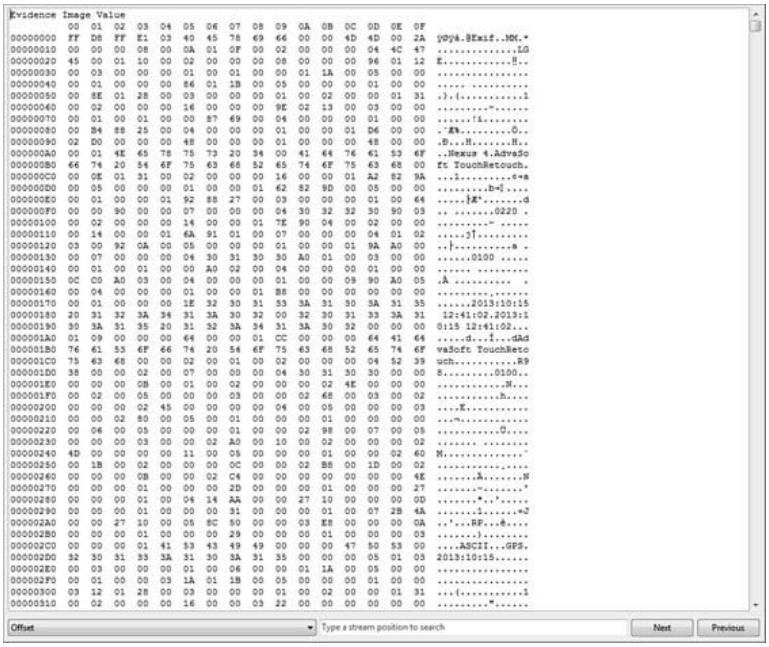


Figura 22.
L'analisi del file effettuata con un lettore di formato esadecimale. Nella colonna più a destra si notano i riferimenti al modello del telefono ed al software di *editing* dei metadati EXIF.

7.3 Analisi globale dell'immagine

L'analisi dell'istogramma dei coefficienti DCT dell'immagine in esame (figura 23, immagine di sinistra - riga in alto) mostra la presenza di "buchi" molto marcati nella distribuzione dei valori. Questo è il tipico effetto della doppia quantizzazione dei coefficienti DCT e indica che l'immagine è stata molto probabilmente compressa due volte [54]. Si noti, invece, che l'istogramma corrispondente all'immagine di riferimento (figura 23, immagine di sinistra – riga in basso) non presenta alcun artefatto, quindi è riconducibile ad un'immagine quantizzata una sola volta (durante l'acquisizione della stessa). L'effetto della doppia quantizzazione è visibile chiaramente anche trasformando l'istogramma nel dominio di Fourier (figura 23, immagine di destra) essa introduce dei picchi aggiuntivi oltre a quello centrale.

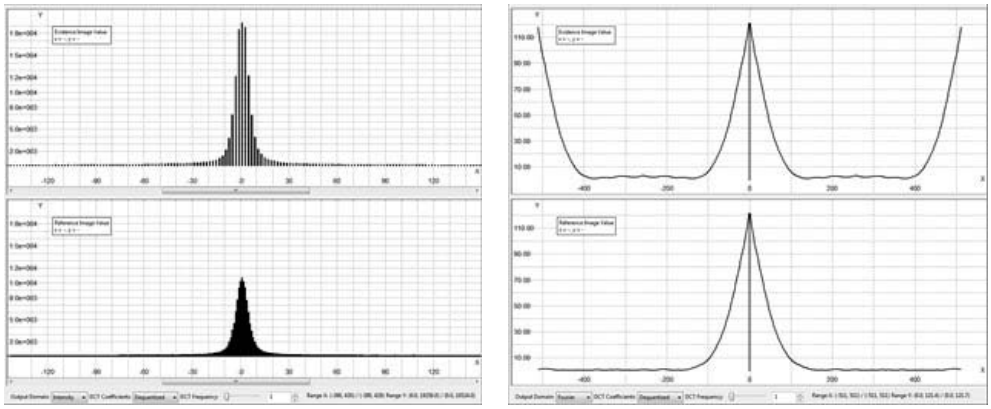


Figura 23.
La doppia quantizzazione lascia un'impronta caratteristica nell'istogramma dei coefficienti DCT dell'immagine: a sinistra vediamo tale effetto sopra, mentre sotto è evidenziato lo stesso istogramma dopo un'unica compressione. A destra lo stesso confronto nel campo delle frequenze: anche in questo caso si notano delle diversità.

7.3.1 Analisi della correlazione dei pixel

Il confronto delle periodicità nei pixel fra l'immagine analizzata e quella di riferimento (figura 24) indica una buona compatibilità. Infatti, picchi sono in posizioni abbastanza simili, sebbene alcuni di essi (es. il picco centrale) siano più accentuati solo nell'immagine di riferimento. I picchi mancanti potrebbero essere dovuti alla seconda compressione identificata nel filtro precedente.

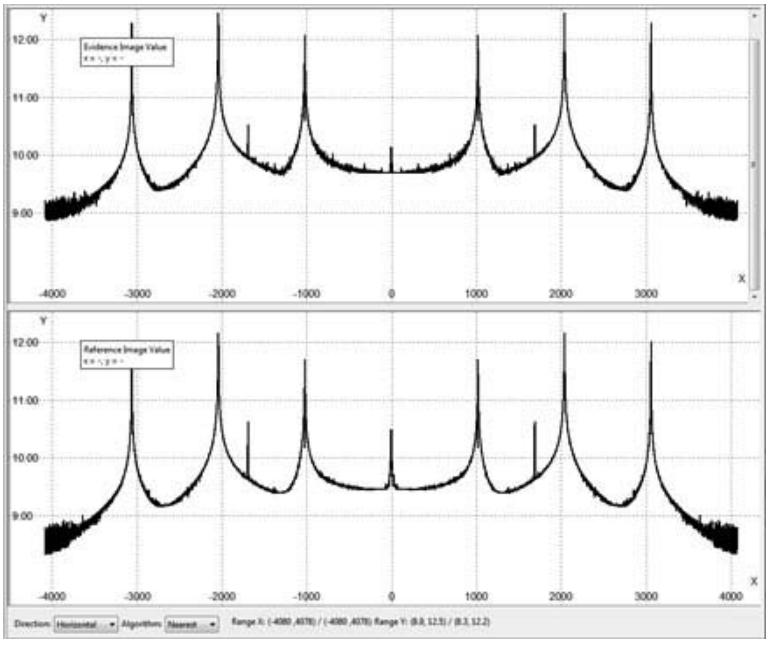


Figura 24.
L'analisi dei risultati della correlazione tra i pixels delle due immagini non permette di rilevare eccessive differenze, se si esclude il picco centrale più alto ed alcuni picchi mancanti nel grafico relativo all'immagine di riferimento (sotto).

7.3.2 **Analisi di intensità e colori**

L'analisi degli istogrammi di luminosità e dei colori nello spazio Lab (figura 25), non evidenzia nulla di particolare. L'istogramma dei valori, infatti, non presenta regolarità o periodicità sospette. L'analisi dello spazio colore vede una distribuzione su valori intermedi e non saturati, in quanto tutti i colori presenti nell'immagine risiedono all'interno dell'area bianca (Gamut RGB).

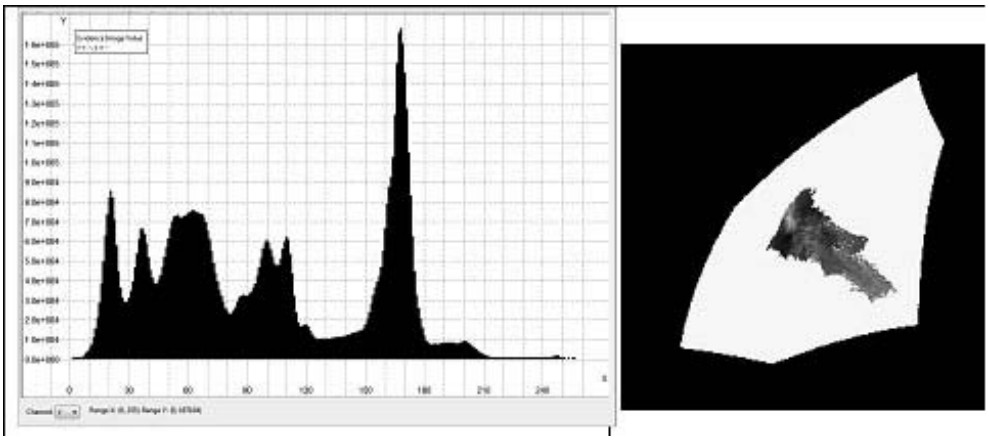


Figura 25.
L'analisi degli istogrammi di luminosità e dei colori nello spazio Lab non fornisce riscontri di positività: tutti i colori presenti nell'immagine risiedono all'interno dell'area bianca.

7.4 Identificazione del dispositivo

Nel caso in esame si è calcolato il CRP del dispositivo in nostro possesso acquisendo una serie di immagini neutre (sfocate e contenenti regioni omogenee). Tramite la valutazione della correlazione su immagini di test provenienti dallo stesso dispositivo e da altri modelli, è stata calcolata una soglia (0,00136). La correlazione del PRNU con il CRP del dispositivo è risultata 0.09888, quasi due ordini di grandezza superiore alla soglia (figura 26) questo ci permette di affermare che molto probabilmente l'immagine è stata acquisita dal dispositivo in nostro possesso.

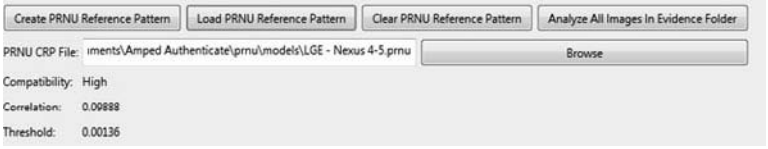


Figura 26.
Il confronto tra la soglia predeterminata ed il valore relativo al dispositivo in esame è di due ordini di grandezza superiore.

7.5 Analisi Locale

7.5.1 **ELA**

Tramite l'analisi ELA con qualità 94 ed una moltiplicazione per 200 dei valori ottenuti, risulta evidente una macchia al centro della scrivania (figura 27). Non essendoci nessun dettaglio degno di nota in quella regione

dell'immagine, ci sono buone probabilità che il filtro sia riuscito ad identificare una zona che è stata compressa diversamente dal resto a causa di una manipolazione dei pixel successiva alla generazione.

Figura 27. Risultato dell'analisi ELA. Con un particolare settaggio di valori e qualità, si evidenzia una zona i cui pixels hanno una "storia di compressione" differente

7.5.2 **Mappa DCT**

La visualizzazione della mappa DCT (figura 28) fornisce un risultato molto simile a quello dell'analisi ELA, evidenziando un andamento dei coefficienti DCT dell'immagine al centro della scrivania diverso dalle parti circostanti.

Figura 28. Mappa DCT. I coefficienti evidenziano un diverso andamento nella zona in cui è stata effettuata la manomissione.

7.5.3 **Mappa di probabilità**

La mappa di probabilità dell'immagine (figura 29) evidenzia la correlazione fra i pixel dell'immagine. In questo caso la traccia è legata al fatto che l'area manipolata presenta delle correlazioni fra pixel diverse dal resto dell'immagine.

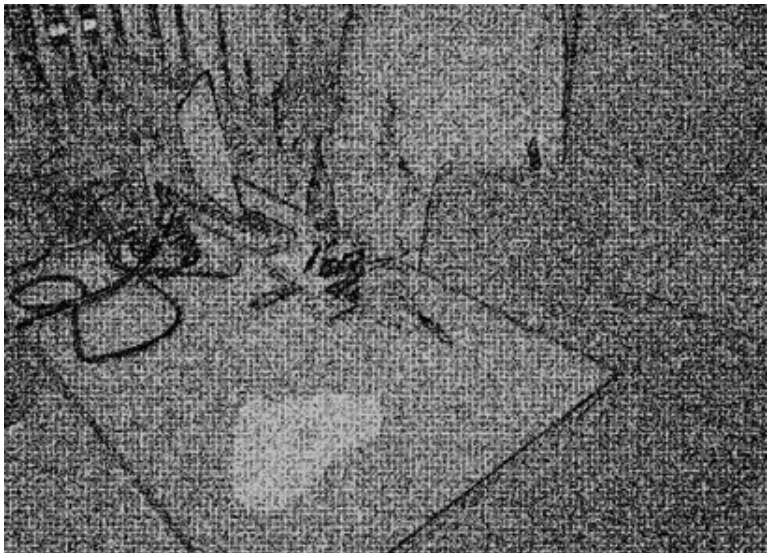
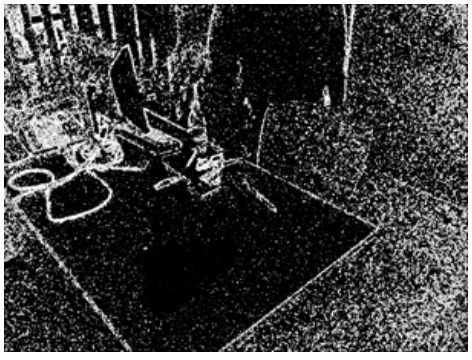


Figura 29.
Mappa di probabilità dell'immagine. L'area manipolata presenta delle correlazioni fra pixel diverse dal resto dell'immagine.

7.5.4 **Mappa del rumore**

Anche nell'analisi delle statistiche di rumore si nota piuttosto chiaramente la zona manipolata (figura 30). L'immagine di sinistra mostra l'analisi del rumore fatta con la Kurtosis, mentre quella di destra la semplice visualizzazione del PRNU dell'immagine.



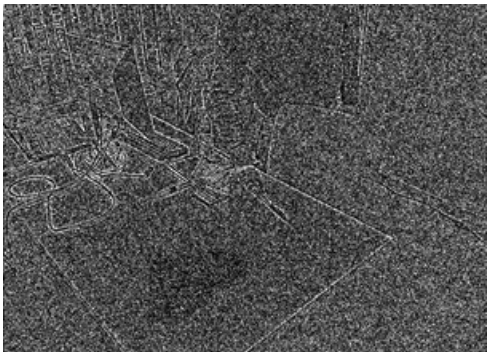
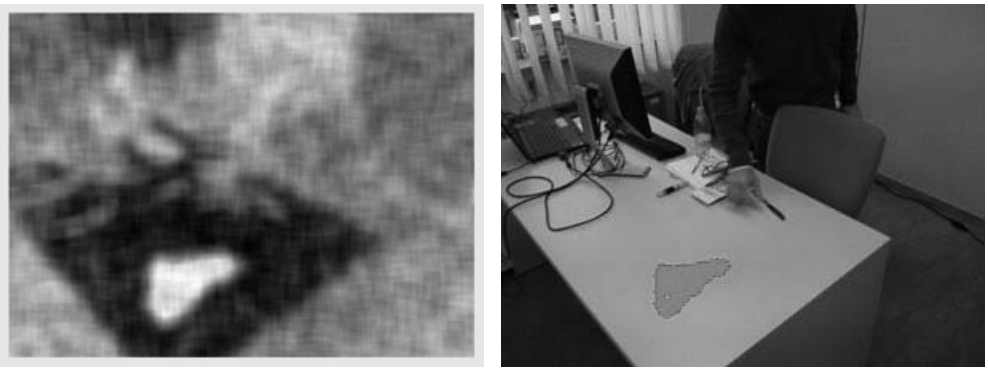


Figura 30.
La mappa del rumore mediante Kurtosis (sinistra) evidenzia la zona sospetta. La visualizzazione del semplice PRNU dell'immagine (destra) mostra una risposta meno leggibile.

7.5.5 **Analisi locale del PRNU**

La correlazione locale del PRNU con quella del CRP della macchina fotografica conferma le nostre analisi precedenti. Nella figura 31 (immagine di sinistra) si vede la mappa di correlazione a blocchi (zone più chiare indicano quelle regioni che sono meno compatibili con il CRP e quindi più sospette). L'immagine di destra mostra il risultato dell'applicazione della mappa, con una soglia scelta opportunamente. In questo caso il risultato è molto chiaro, ma la scelta di soglie non corrette rischia di fornire, alle volte, dei risultati inaffidabili; in tal caso è sempre consigliabile riferirsi alla mappa di correlazione.

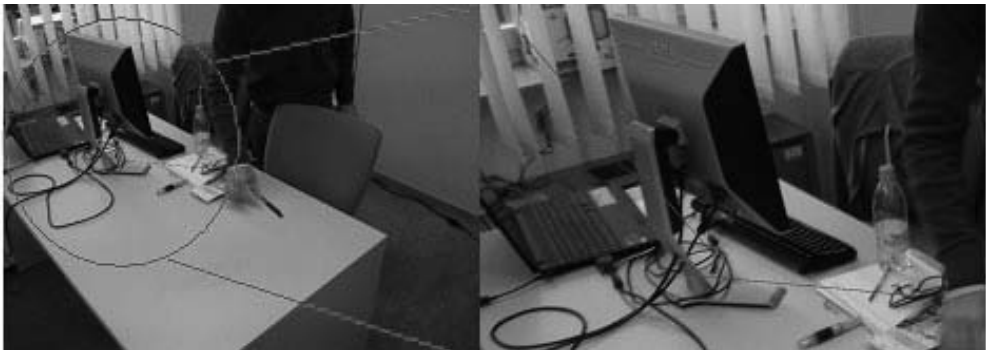
Figura 31. Mappa di correlazione a blocchi nell'analisi locale del PRNU: le zone più chiare (a sinistra) e l'area colorata di rosso (a destra) indicano le regioni più sospette.



7.5.6 **Analisi dei cloni**

L'analisi dei cloni non evidenzia zone duplicate all'interno dell'immagine. Gli algoritmi con keypoint identificano due coppie di punti simili (connessi dalle linee rosse), ma è facile verificare con l'analisi visuale (figura 32) che si tratta di falsi positivi.

Figura 32. Esito della ricerca dei cloni. In questo caso i punti segnalati dall'algoritmo sono falsi positivi.



7.6 Analisi dettagliata della scena

L'analisi dettagliata della scena per la rilevazione di inconsistenze nell'illuminazione, nelle ombre o nella prospettiva, non è sempre fatti-

bile in maniera semplice, né automatizzabile tramite software. In questo caso, tuttavia, non è stata rilevata alcuna irregolarità degna di nota.

7.7 Analisi conclusive

Dagli esiti delle analisi svolte possiamo trarre le conclusioni riassunte nella Tabella 3, in cui vengono elencati per permettere una visualizzazione diretta. Nella figura 33 possiamo confrontare l'immagine analizzata (a sinistra) con quella originale (a destra). Come evidenziato nei metadati (Figure. 15, 16 e 22), l'immagine analizzata è stata creata applicando il software "AdvaSoft TouchRetouch" su uno smartphone Android Nexus 4. Nell'immagine originale era presente una pistola (giocattolo), che è stata rimossa con tale applicazione.

Tabella 3.
Tabella riassuntiva in merito al caso di studio esposto.

	ESITO DELL'ANALISI	NOTE
Analisi del formato	X	File non originale
Analisi globale	X	File probabilmente ricompresso
Analisi della sorgente	V	Compatibile con il dispositivo sospetto
Analisi locale	X	Molteplici segni di manipolazione
Analisi della scena	V	Nulla di sospetto
Conclusioni	X	L'immagine è stata originariamente acquisita dal dispositivo sospetto, ma con ogni probabilità è stata soggetta a manipolazione. Il file analizzato non è autentico, né lo è il suo contenuto.

Figura 33.
Confronto tra l'immagine consegnata per l'analisi (a sinistra) e l'immagine originale (a destra).

Il caso utilizzato come esempio, sebbene assolutamente realistico, riporta una analisi in cui le tracce di manipolazione sono palesi in molti filtri. La ragione di ciò risiede nel fatto che è stato utilizzato uno strumento di "riempimento" per rimuovere un oggetto da una zona uniforme abbastanza grande. È bene precisare che spesso i risultati della manipolazione sono visibili solo in uno o due filtri a livello locale, ed ancora, come precisato all'inizio di questo capitolo, diventa determinante nei casi più complessi l'abilità dell'analista esperto.

8. ANALISI DI UN'IMMAGINE ANALOGICA

8.1 Presenza del negativo

Nonostante le foto analogiche siano sempre più rare, per questioni di completezza appare opportuno terminare la nostra esposizione riportando, anche se brevemente, alcuni approcci nel caso in cui si debba esaminare questo tipo di documento. Tralasceremo la fase dell'analisi visiva del contenuto dell'immagine, che è comune a quanto verrà riportato in seguito per il caso digitale, concentrandoci sugli accertamenti da effettuare materialmente sul documento.
Il motivo per il quale il negativo delle immagini analogiche è considerato (anche se non del tutto correttamente, come vedremo in seguito) affidabile, mentre le immagini digitali non godono della stessa fiducia, discende dalle differenze nella tecnica di formazione dell'immagine tra i due tipi di apparati. Nelle fotocamera analogiche la pellicola viene impressionata dalla luce proveniente dal sistema di lenti, dopodiché essa costituisce una sorta di "matrice" dell'immagine (il c.d. *negativo*), da cui si possono estrarre quante copie si desidera, tutte identiche all'originale. Nelle odierne fotocamere, come abbiamo visto, l'immagine semplicemente "transita" sulla matrice di pixel del sensore prima di essere salvata nella memoria, e quando scattiamo l'immagine successiva la nuova informazione ha cancellato per sempre la precedente.
Anche i negativi possono essere alterati, come di seguito indicato:

- Agendo fisicamente sulla pellicola, asportandone alcune parti oppure aggiungendone altre e successivamente sviluppando il negativo modificato;
- Duplicando il negativo con apposita strumentazione, applicando opportune maschere per nascondere od inserire i particolari voluti.

Entrambe queste modifiche sono rilevabili: nel primo caso è sufficiente esaminare al microscopio il negativo modificato per notare i ritocchi, nel secondo si sfruttano le diverse caratteristiche (grana, spessore) del negativo-copia, che per motivi tecnici non risultano essere mai identici a quelli dei rullini delle fotocamere. Inoltre, è bene sottolinearlo, questo tipo di modifiche (specie la seconda tecnica) non è alla portata dell'utente generico, ma richiedono conoscenze specifiche, abilità, e strumentazione adatta, tra l'altro sempre più difficile da reperire.
In aggiunta a quanto sopra, è necessario verificare che:

- la dimensione dell'immagine sul negativo sia più estesa rispetto alla stampa. Per questioni tecniche vi è una piccola differenza di dimensioni tra le stampe e la pellicola;
- eventuali altri scatti prima e dopo il fotogramma siano nella giusta sequenza. In caso positivo è possibile valutarne il contenuto per verificare la presenza di eventuali incongruenze nel contenuto informativo;

Riassumendo: una volta in possesso dei negativi di un'immagine, accertato che questi non siano stati modificati (o duplicati), la validità di un'immagine è considerata certa.

8.2 Mancanza del Negativo

A volte non siamo così fortunati da entrare in possesso della pellicola da cui è stata sviluppata l'immagine, e ci viene consegnata unicamente l'immagine stampata. Tra gli accorgimenti da mettere in atto per il nostro scopo, oltre alla già citata analisi visiva del contenuto informativo, vi sono:

- Esaminare visivamente il livello di invecchiamento del supporto (vi possono essere segni di usura o di invecchiamento);
- Controllare la coerenza tra la marca del supporto cartaceo o la data di stampa (impresse sul retro) e le notizie che conosciamo in merito alla fotografia in esame;

Per una collezione di ulteriori ed ancora più specifici metodi di analisi delle immagini analogiche, si rimanda a [44].

9. CONCLUSIONI

Sebbene molte delle tecniche esposte siano ormai collaudate e forniscano risultati attendibili, è impossibile provare scientificamente l'autenticità di una immagine. Il massimo che possiamo dire, è che l'immagine è "coerente" con l'ipotesi di autenticità, in quanto non possiamo mai escludere la possibilità che colui che ha manipolato l'immagine sia stato capace di nascondere le tracce a tutte le metodologie di analisi in nostro possesso. Per dimostrare la non-autenticità, basta avere una sola prova certa della presenza di un'alterazione, mentre la mancanza di segnalazioni in tal senso non costituisce di per sé una prova di originalità. Per effettuare modifiche ad una immagine in modo da rendere più difficile il rilievo delle relative tracce, un attaccante esperto potrebbe ricorrere a qualche azione di "disturbo" (Antiforensics). Si potrebbe ad esempio applicare, dopo la manipolazione, una sequenza di operazioni di editing "innocue" dal punto di vista del contenuto ma tali da alterare la traccia delle manipolazioni più evolute. Altri metodi prevedono l'inserimento nell'immagine di una sorta di "rumore artificiale" che cancella i segni della prima compressione [52].
Per quanto sopra esposto, il concetto di *originalità assoluta* di una immagine è un'astrazione che non ha cittadinanza nel contesto forense. In tale ambito ha senso invece parlare di *originalità accertabile*.

Dovendo quindi esprimere un giudizio in merito a quest'ultima, il metodo migliore di procedere, come visto nel caso di studio, consiste nel raggruppare i risultati (Tabella 3, paragrafo 6.7) e relazionarli esprimendo poi un giudizio in relazione alla presenza o meno di segnali di incoerenza con un'immagine originale (X). Per quanto riguarda la scala da utilizzare, prendendo spunto dal metodo di classificazione nel confronto tra volti introdotto dalla Polizia Scientifica Italiana nel 1997, potremo avere tre tipi di responso:

- *Immagine non coerente con l'ipotesi di autenticità*: nella tabella che raccoglie gli esiti delle analisi è presente almeno un risultato inequivocabilmente riconducibile alla presenza di artefatti introdotti da una o più operazione di modifica del contenuto informativo dell'immagine;
- *Immagine dall'autenticità incerta*: nella tabella che raccoglie gli esiti delle analisi è presente almeno un risultato che potrebbe ricondurre alla presenza di artefatti introdotti da una o più operazione di modifica del contenuto informativo dell'immagine. Tuttavia non è possibile dare un giudizio di autenticità, né di non autenticità, in quanto:
  - la presenza di artefatti all'interno dell'immagine rilevata dalle analisi, non è certa;
  - si ha certezza di modifiche al file che contiene l'immagine (ad esempio nei metadati Exif), ma non si hanno riscontri in merito a modifiche al contenuto informativo;
- *Immagine coerente con l'ipotesi di autenticità*: Tutto il contenuto del file risulta inalterato.

A parere degli autori, le considerazioni e la serie di accertamenti illustrati nei paragrafi precedenti, uniti alla metodologia espositiva espressa dalla scala di giudizio sopra esposta, permetterà alla parte interessata di corredare le proprie conclusioni da una solida base scientifica che esprime lo stato dell'arte nel campo dell'analisi forense di immagini.

REFERENZE:

[1] S. Battiato, F. Galvan: "*La validità probatoria delle immagini e dei video*", in Sicurezza e Giustizia n. II/MMXIII, pp. 30-31.

[2] https://www.swgit.org/ (2013).

[3] http://en.wikipedia.org/wiki/Google_Street_View (2013).

[4] S. Battiato, F. Galvan: "*Ricostruzione di informazioni 3d a partire da immagini bidimensionali*" - Sicurezza e Giustizia n. IV/MMXIII.

[5] V. Denti: "*Scientificità della prova e libera valutazione del giudice*", in Riv. dir. proc., (1972), p. 414.

[6] http://www.processig8.org/Udienze%2025/Ud.%20143/143_motivazioni-03_25.html (2013).

[7] *Crime investigation: physical evidence and the police laboratory*. Interscience Publishers, Inc.: New York, (1953).

[8] http://richardjevans.blogspot.it/2009/07/blog-post.html (2013).

[9] http://www.fourandsix.com/photo-tampering-history/ (2013).

[10] http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2005/index.htm/ (2013).

[11] S. Battiato, G. Messina e R. Rizzo: "*Image Forensics. Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive*" Chapter in IISFA Memberbook (2009).

[12] S. Battiato, M. Moltisanti: "*Tecniche di steganografia su immagini digitali*" Chapter in IISFA Memberbook (2012).

[13] J.A. Redi et al: "*Digital image forensics: a booklet for beginners*" Multimed Tools Appl (2011) 51:133 – 162.

[14] A. Piva: "*An overview on image forensics" ISRN Signal Processing*, (2013).

[15] R. Ramanath, W.E. Snyder, Y. Yoo and M.S Drew: "*Color image processing pipeline*", Volume 22, (2005).

[16] CCITT Recommendation T.81, ISO/IEC 10918-1:1994, "*Information technology - Digital compression and coding of continuous-tone still images: Requirements and guidelines*", (1992).

[17] J. Lukàš, J. Fridrich and M. Goljan: "*Digital camera identification from sensor pattern noise,*" IEEE Transaction on Information Forensics and Security, vo1. 1, pp.205-214, (2006).

[18] Mo Chen, J. Fridrich and M. Goljan: "*Digital Imaging Sensor Identification (Further Study)*", Proceedings. of SPIE Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents, pp. 0P-0Q, (2007).

[19] N. Krawetz: "*A picture's worth: Digital image analysis and forensics*", www.hackerfactor.com, (2007).

[20] A. Criminisi: "*Single-view metrology: Algorithms and applications*", Pattern Recognition. Lecture Notes in Computer Science Vol. 2449, 224-239. Springer Berlin Heidelberg, (2002).

[21] L. Wu, Y. Wang: "*Detecting Image Forgeries using Geometric Cues*" capitolo in Computer Vision for Multimedia Applications: Methods and Solutions (2011).

[23] CIPA DC-008, "*Exchangeable image file format for digital still cameras: EXIF Version 2.3*", (2012).

[24] JPEGsnoop by Calvin Hass http://www.impulseadventure.com/photo/jpeg-snoop.html (2013).

[25] http://www.photoshopdisasters.com (2013).

[26] E. Kee, M.K. Johnson and H. Farid: "*Digital image authentication from JPEG headers*", IEEE Transactions on Information Forensics and Security, vol. 6, pp. 1066-1075, (2011).

[27] P. Alvarez: "*Using extended file information (EXIF) file headers in digital evidence analysis*", International Journal of Digital Evidence, vol. 2, (2004).

[28] EXIFTool by Phil Harvey, http://www.sno.phy.queensu.ca/~phil/EXIFtool/ (2013).

[29] PhotMe by Jens Duttke http://www.photome.de/ (2013).

[30] http://www.photoshop.com/ (2013).

[31] http://www.getpaint.net/ (2013).

[32] http://www.irfanview.com/ (2013).

[33] Z. Lin, J. He, X. Tang and Chi K. Tang: "*Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis*", Journal Pattern Recognition, Vol. 42, pp. 2492-2501, (2009).

[34] Alin C. Popescu and H. Farid: "*Statistical tools for digital forensics*", Lecture Notes in Computer Science, vol. 3200, pp 128-147, (2005).

[35] Mahdian, S. Saic: "*Blind authentication using periodic properties of interpolation*", IEEE Transactions on vol.3, n. 3, pp. 529-538, (2008).

[36] X. Pan, S. Lyu: "*Region Duplication Detection Using Image Feature Matching*", IEEE Transactions on Information Forensics and Security, vol. 5, pp. 857-867, (2010).

[37] H. Farid: "*Exposing digital forgeries from JPEG ghosts*", Information Forensics and Security, vol. 4, pp. 154-160, (2009).

[38] C. Grigoras, J.M. Smith: "*Digital imaging: enhancement and authentication*", Encyclopedia of Forensic Sciences, Second Edition, pp. 303-314. (2013).

[39] M. Kirchner, T. Gloe: "*On Resampling Detection in Re-compressed*

Images". IEEE Workshop on Information Forensics and Security, pp. 21-25, (2009).

[40] X. Pan, X. Zhang and S. Lyu: "*Exposing Image Splicing with Inconsistent Local Noise Variances*", IEEE International Conference on Computational Photography, pp. 1-10, (2012).

[41] J. Lukas, J.Fridrich and M. Goljan: "*Detecting digital image forgeries using sensor pattern noise*", eProceedings of SPIE Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents, pp. 0Y11- 0Y11, (2006).

[42] W. Luo, J. Huang and G. Qiu: "*Robust Detection of Region-Duplication Forgery in Digital Image*", 18th International Conference on Pattern Recognition, vol. 4, pp. 744-749, (2006).

[43] H. Farid, M.J. Bravo: "*Image forensic analyses that elude the human visual system*". In SPIE Symposium on Electronic Imaging, San Jose, CA, (2010).

[44] D.A.Brugioni: "*Photo Fakery: The History and Techniques of Photographic Deception and Manipulation*", Ed. Brassey's, (1999).

[45] R. Gonzalez, R. Woods: "*Digital Image Processing (3rd ed.)*", Prentice Hall, pp. 165–168, (2008).

[46] S. Battiato, A.R. Bruna, G. Messina and G. Puglisi, *Image Processing for Embedded Devices*, Eds., ISSN: 1879-7458 - Applied Digital Imaging ebook series, ISBN: 978-1-60805-170-0, Bentham Science Publisher, (2010).

[47] Choi K-S, Lam E-Y and Wong KKY, *Source camera identification using footprints from lens aberration*, Proc. SPIE (2006).

[48] M. K. Johnson, H. Farid: "*Exposing digital forgeries through chromatic aberration*", Proceedings of the 8th workshop on Multimedia & Security, S. Voloshynovskiy, J. Dittmann, and J. J. Fridrich, Eds., pp. 48 andltland, (2006).

[49] http://theory.uchicago.edu/~ejm/pix/20d/tests/noise/#patternnoise (2013).

[50] A. C. Popescu, H. Farid: "*Exposing digital forgeries in color Filter array interpolated images*", IEEE Transactions on Signal Processing, vol. 53, n. 10, pp. 3948–3959, (2005).

[51] J. Kornblum: "*Using JPEG quantization tables to identify imagery processed by software*", Digital Investigation, vol. 5, pp. S21–S25, (2008).

[52] C. Stamm, S.K. Tjoa,W. S. Lin and K. J. R. Liu: *"Anti-forensics of Digital image compression" in Proc. IEEE Int. trans. Information forensics and security*, Vol. 6, N.3, pp. 1694–1697, (2011).

[53] F. Galvan, G. Puglisi, A. R. Bruna, and S. Battiato: *"First quantization coefficient extraction from double compressed jpeg images", in International Conference on Image Analysis and Processing (ICIAP)*, ser. Lecture Notes in Computer Science, vol. 8156, pp. 783–792, (2013).

[54] G. Puglisi, A. R. Bruna, F. Galvan, and S. Battiato: *"First JPEG quantization matrix estimation based on histogram analysis"*, in International Conference on Image Processing (ICIP), (2013).

[55] B. Carrier & E. H. Spafford: *"Getting Physical with the Digital Investigation Process"*, International Journal of Digital Evidence, Vol. 2, No. 2, (2003) [56] AES27:1996, Recommended Practice for Forensic Purposes – Managing Recorded Audio Materials Intended for Examination, Audio Engineering Society, (1996).

[56] http://www.acdsee.com/ (2013).