CAPITOLO PRIMO

"SOCIAL" IMAGE FORENSICS: STATUS E PROSPETTIVE

Sebastiano Battiato, Oliver Giudice, Antonino Paratore

Sommario: 1. Introduzione – 2. Le Immagini JPEG: Definizioni e caratteristiche –3. Un Dataset di immagini da Social Network –4. Analisi delle tracce lasciate dai Social Networks –5. Social Image Forensics: Image Ballistics – 6. Conclusioni.

1. INTRODUZIONE

L'Image Forensics, nell'ambito della più vasta area del Multimedia Forensics [1][2], si occupa di analizzare le immagini digitali al fine di esibire elementi di prova in ambito forense per ciò che riguarda l'autenticità e integrità dei dati e l'identificazione della sorgente di acquisizione [3]. Ci si riferisce ad esempio a casi di contraffazioni di immagini (Forgery Detection) [4] o alla ricostruzione della cosiddetta "storia" di un'immagine fin dalla sua acquisizione (Image Ballistics).

L'Image Ballistics, il cui termine deriva dalla ben nota balistica forense[1], fu definita per la prima volta da Farid [5]. Obiettivo di tale disciplina è l'estrazione e l'interpretazione delle caratteristiche intrinseche presenti nelle immagini, per poter ricostruire avvenimenti di interesse giuridico o probatorio, in cui hanno un ruolo predominante i dispositivi di acquisizione di immagini digitali e i software di elaborazione di immagini.

Il problema dell'identificazione del dispositivo di acquisizione (Camera Source Identification) è stato nel tempo affrontato attraverso numerosi approcci tra cui, fra i più efficaci, menzioniamo il PRNU [6][7] (**Photo Response Non-Uniformity**) ovvero l'estrazione di un segnale di rumore invisibile presente sulle immagini digitali, dovuto principalmente a piccole imperfezioni, di natura elettronica, presenti nel sensore che le acquisisce. Il PRNU rappresenta una sorta di impronta lasciata dal sensore sull'immagine e quindi legata in maniera univoca al dispositivo che ha acquisito l'immagine stessa.

La questione si complica quando le immagini subiscono alterazioni di vario genere a seguito di processamenti da parte di applicativi software.

E' stato ormai dimostrato come la Camera Source Identification basata su PRNU, non risulta essere sufficientemente valida su immagini elaborate anche con semplici editing (quali rescaling, cropping, ecc.) attraverso software di pubblico dominio quali ad esempio Photoshop o GIMP. Inoltre, le operazioni di ricodifica che vengono operate a valle, da uno qualunque di tali software, alterano pesantemente i valori del PRNU compromettendone l'efficacia[8].

[1] Balistica forense: branca della scienza forense che tenta di ricostruire avvenimenti relativi a delitti in cui sono state utilizzate delle armi da fuoco.

Oggi, i Social Network consentono ai loro utenti di caricare e condividere un'enorme quantità di immagini: basti pensare che quotidianamente, si stima che su Facebook vengano caricate più di 300 milioni di immagini. Si definisce "Social Image Forensics" lo studio delle caratteristiche intrinseche delle immagini, pubblicate su un Social Network, al fine di identificare una sorta di "fingerprint" che tiri fuori delle evidenze, chiare e documentabili, tali da ricostruirne la "storia digitale" dell'immagine fin dall'acquisizione.
Lo studio delle tematiche della "Social Image Forensics" è molto utile sia a scopo forense che investigativo: conoscere l'origine di una determinata immagine può infatti essere determinante in molti contesti. A tal fine però risulta fondamentale comprendere nel dettaglio le peculiarità che il processo di upload e di condivisione di tali informazioni genera sui Social Network.
In questo articolo verrà illustrato un possibile protocollo per l'Image Ballistics basato su caratteristiche intrinseche riscontrabili sulle immagini dopo i processi di upload/download delle stesse sulle piattaforme Social di uso più comune. Nei prossimi paragrafi verranno descritti i dettagli tecnici di tali caratteristiche mentre a seguire alcuni casi di studio ne illustreranno le potenzialità.

2. LE IMMAGINI JPEG: DEFINIZIONI E CARATTERISTICHE

In questo paragrafo verranno presentati brevemente i fondamenti delle *immagini* in formato JPEG: il formato più comune e maggiormente utilizzato all'interno dei Social Network e non solo.
In ambito forense lo studio delle anomalie di codifica, presenti in immagini manipolate, ha dato origine ad un filone di ricerca promettente soprattutto nel caso della individuazione di manipolazioni locali (es. cloning, splicing, ecc.) seguite in genere da ricodifiche nel dominio DCT (Discrete Cosine Transform)[9][10].

2.1 La compressione JPEG

La compressione delle immagini digitali affronta il problema della riduzione del numero di bit necessari alla rappresentazione delle stesse. Da un punto di vista matematico, si attua una trasformazione in grado di realizzare un mapping tra la matrice di pixel ed un insieme di dati non correlati. Per le immagini digitali è possibile individuare due differenti tipi di compressione: lossless e lossy. La compressione lossless comprime tutte le informazioni di un'immagine, in modo tale che la stessa, una volta decompressa, sia identica a quella originale, senza alcuna perdita di informazioni e di conseguenza senza riduzione della qualità. La compressione di tipo lossy, invece, scarta opportunamente alcune delle informazioni poco visibili all'occhio umano (es. alte frequenze) comprimendo le rimanenti informazioni. L'immagine compressa ottenuta, risulta essere in genere, rispetto al livello/fattore di qualità, una buona approssimazione dell'immagine originale.
JPEG è l'acronimo di "Joint Photographic Experts Group", un gruppo di lavoro che ha definito l'omonimo standard internazionale di compressione per le immagini [11].

La conversione di uno stream di byte in formato JPEG avviene attraverso le seguenti fasi: Trasformazione, Quantizzazione e Codifica come mostrato in Figura 1.

(inserire qui fig1.)

Figura 1 – Fasi della compressione di un immagine in formato JPEG

Attraverso la prima fase si ottiene una rappresentazione del segnale che ne facilità la compressione. Le operazioni coinvolte sono: conversione di spazio di colori, sotto-campionamento, suddivisione in blocchi e DCT. Successivamente, attraverso il processo di quantizzazione, vengono eliminate le informazioni trascurabili, ovvero quelle informazioni che non sono essenziali per la ricostruzione dell'immagine originale. Per fare ciò si divide ogni componente della matrice dei coefficienti delle frequenze per una costante fissata, e si arrotonda il valore così ottenuto. Il risultato di questa operazione è una matrice contenente un numero elevato di valori nulli in corrispondenza delle alte frequenze ed una serie di valori interi vicini allo zero. La matrice così elaborata può essere codificata con un elevato fattore di compressione. Questo passo dell'algoritmo JPEG è quello che maggiormente degrada la qualità dell'immagine, poiché ne elimina definitivamente alcune componenti.

Lo standard JPEG non specifica i valori da utilizzare nelle tabelle (matrice 8x8 contenenti i valori di cui sopra) in quanto queste dovrebbero essere generate per ogni immagine ed il processo risulterebbe oneroso. Le tabelle sono spesso quindi dipendenti dai dispositivi utilizzati o dai software di elaborazione di immagini [12].

2.2 Struttura di un file JPEG

Lo standard JPEG definisce anche il formato del file la sua estensione e ovviamente la sua struttura che definisce le modalità con cui vengono memorizzate le varie parti di un'immagine.

La parte iniziale del file è costituita dai cosiddetti *marker* [13]. Tali *marker* vengono utilizzati per segnalare la tipologia di dati inserita nel file ed hanno una lunghezza di 2 Byte. I *marker* possono essere di due tipi: Stand-alone che non contengono dati oltre i due byte del marker stesso e quelli che non rientrano in questa categoria che sono immediatamente seguiti da un valore di due Byte che segnala il numero di Byte di dati che il *marker* contiene.

I dati compressi sono l'unica parte che nel file non sono inseriti tra specifici *marker* e sono sempre seguiti immediatamente dal marker "Start of Scan" (SOS). I diversi tipi di *marker* che è possibile trovare in un file JPEG sono elencati in Tabella 1 mentre un esempio di struttura file JPEG, con esclusione dei dati compressi, viene riportato in Tabella 2.

MARKER	DESCRIZIONE
SOI (Start Of Image)	Indica l'inizio del file JPEG.
AP_0 – APP_{15}	Tengono traccia dell'applicazione utilizzata per elaborare l'immagini in fase di compressione.
COM	Delimita, se presenti, la stringa per i commenti (es. copyright).
DHT (Define Huffman Table)	Definisce le tabelle di Huffman utilizzate.
DRI (Define Restart Interval)	Identifica il punto da dove riprendere la decodifica nel caso in cui il decodificatore interrompe la scansione.
DQT (Define Quantization Table)	Definisce le tabelle di quantizzazione usate nell'immagine
EOI (End Of Image)	Delimita la fine del file JPEG.
RST_n	Vengono utilizzati per delimitare blocchi di dati indipendenti dalla codifca di compressione.
SOF_n: (Start Of Frame)	Stabilisce l'inizio di un frame.
SOS: (Start of Scan)	Delimita l'inizio dei dati compressi.

Tabella 1- Marker presenti in un file JPEG

Start of Image
JFIF APP0 marker: version 1.01, density 1x1 0
Miscellaneous marker 0xed, length 130
Define Quantization Table 0 precision 0
11 8 7 11 17 28 36 43
8 8 10 13 18 41 42 39
10 9 11 17 28 40 48 39
10 12 15 20 36 61 56 43
13 15 26 39 48 76 72 54
17 25 39 45 57 73 79 64
34 45 55 61 72 85 84 71
50 64 67 69 78 70 72 69
Define Quantization Table 1 precision 0
12 13 17 33 69 69 69 69
13 15 18 46 69 69 69 69
17 18 39 69 69 69 69 69
33 46 69 69 69 69 69 69
69 69 69 69 69 69 69 69
69 69 69 69 69 69 69 69
69 69 69 69 69 69 69 69
69 69 69 69 69 69 69 69
Start Of Frame 0xc2: width=540, height=720, components=3
Component 1: 2hx2v q=0
Component 2: 1hx1v q=1
Component 3: 1hx1v q=1
Define Huffman Table 0x00
0 2 3 1 1 1 1 0
0 0 0 0 0 0 0 0
Define Huffman Table 0x01
1 1 1 1 1 1 1 0
0 0 0 0 0 0 0 0
Start Of Scan: 3 components
Component 1: dc=0 ac=0
Component 2: dc=1 ac=0
Component 3: dc=1 ac=0

Ss=0, Se=0, Ah=0, Al=0 **Define Huffman Table** 0x10 0 2 2 2 1 2 3 6 5 4 2 2 3 1 1 0 **Start Of Scan**: 1 components Component 1: dc=0 ac=0 Ss=1, Se=7, Ah=0, Al=1 **Define Huffman Table** 0x11 0 2 1 3 4 2 3 0 3 1 0 0 0 0 0 0 **Start Of Scan:** 1 components Component 2: dc=0 ac=1 Ss=1, Se=63, Ah=0, Al=0 **Define Huffman Table** 0x11 0 2 2 1 2 7 0 2 2 2 3 0 0 0 0 0 **Start Of Scan:** 1 components Component 3: dc=0 ac=1 Ss=1, Se=63, Ah=0, Al=0 **End Of Image**

Tabella 2- Esempio struttura di un file JPEG

2.3 I metadati di un file JPEG

La stragrande maggioranza delle macchine fotografiche moderne, incapsula dei meta-dati nel file JPEG, composto da un'intestazione (header) ed un corpo principale contenente l'immagine.

(inserire fig2)

Figura 2 – Suddivisione dei dati all'interno di un file JPEG

L'intestazione di un file immagine contiene numerosi dati sull'immagine stessa (meta-dati) in un formato chiamato formato EXIF [14].

Le specifiche EXIF definiscono sia dei campi comuni alla maggior parte dei produttori, che campi personalizzati e difficilmente decodificabili. Un dispositivo moderno può salvare all'interno dei metadati diverse informazioni [1], quali ad esempio: dati contenenti informazioni dettagliate associate alle foto digitali, produttore e modello di fotocamera, informazioni legate alla data e all'ora di generazione e di salvataggio del file, informazioni sulle caratteristiche dell'immagine (risoluzione in pixel, dpi, profondità del colore, ecc.), impostazioni di scatto (tempo di scatto, apertura, flash, focale, ecc.), Coordinate GPS, seriale del dispositivo ed altre ancora.

Le analisi sugli EXIF consentono di stabilire se un'immagine è stata generata o meno da un particolare modello di fotocamera che si tratti di una reflex, di una compatta, di un telefono cellulare o di un tablet. L'Image Ballistics basato sugli EXIF risulta però essere un approccio fragile che non garantisce l'autenticità di un'immagine in quanto tali meta-dati appaiono in chiaro, in forma testuale risultando facilmente alterabili.

A tal proposito esistono diversi applicativi, anche open source, in grado di estrapolare tali informazioni, a titolo esemplificativo citiamo in questa sede i seguenti: Jpegsnoop[2], Authenticate[3], Exif dataViewer[4], ExifToolGUI[5].

[2] **http://www.impulseadventure.com/**
[3] **http://www.impulseadventure.com/**
[4] **http://www.exifdataviewer.com/**
[5] **http://exiftoolgui.software.informer.com/**

3. UN DATASET DI IMMAGINI DA SOCIAL NETWORK

Le procedure di condivisione di dati ed in particolare di immagini digitali sulle piattaforme Social, introducono vari e diversi processi di editing già durante il processo di upload. Queste vere e proprie alterazioni sono principalmente attuate al fine di ridurre lo spazio fisico di archiviazione o ancora lo spreco di banda necessario per il trasferimento o per la fruizione da parte degli utenti finali. Tutto ciò fa decadere del tutto la cosiddetta integrità del file e rende ancora più complessa la fase di ricostruzione della storia dell'immagine, fino a distruggere del tutto ogni informazione sull'acquisizione originaria.

Risulta altresì chiaro come tali alterazioni dipendano da una molteplicità di fattori legati sia alla specifica piattaforma Social, su cui si realizza il caricamento dell'immagine, che alle caratteristiche delle immagini in termini di contenuto e di risoluzione; si è quindi deciso di comprendere meglio il fenomeno, collezionando un dataset di immagini aventi particolari caratteristiche come di seguito specificato.

In prima istanza sono stati utilizzati i seguenti dispositivi: Canon Eos 650D, Qumox SJ4000, Sony Powershot A2300, Samsung Note 3 Neo, HTC Desire 526g, Huawei G Play mini, iPhone 5 and iPad mini 2 e sono state acquisite 2720 immagini rappresentanti scenari diversi, avendo cura di gestire sia la massima (High Quality) che la minima (Low Quality) risoluzione consentita da ogni dispositivo.

In Tabella 3 vengono descritti in dettaglio i dispositivi utilizzati e le rispettive risoluzioni utilizzate durante l'acquisizione.

Model	Low Quality	High Quality
("inserire qui fig3") **Canon Eos 650D**	720x480	5184x3456
(inserire qui fig4) **Qumox SJ4000**	640x480	4032x3024
(inserire qui fig5) **Sony Powershot A2300**	640x480	4608x3456
(inserire qui fig6) **Samsung Note 3 Neo**	640x480	3264x2448
(inserire qui fig7) **HTC Desire 526g**	640x480	3264x2448
(inserire qui fig8) **Huawei G Play mini**	640x480	4208x3120
(inserire qui fig9) **iPhone 5**	640x480	2448x3254
(inserire qui fig10) **iPad mini 2**	640x480	800x600

Tabella 3- Dispositivi utilizzati

Una volta creato il dataset, sono state identificate 5 categorie di piattaforme Social su cui è possibile condividere immagini e per ognuna sono stati scelti i 2 Social Network più popolari. In Tabella 4 vengono riportati i Social Network presi in considerazione in questo lavoro.

Categoria	Social
Social Network Classici	(inserire qui fig11) (inserire qui fig12)
Piattaforme di Micro-Blogging	(inserire qui fig13) (inserire qui fig14)
Piattaforme di condivisione di foto artistiche	(inserire qui fig15) (inserire qui fig16)
Piattaforme di condivisione immagini generiche	(inserire qui fig17) (inserire qui fig18)
Piattaforme di messaggistica mobile	(inserire qui fig19) (inserire qui fig20)

Tabella 4- Categorie di piattaforme Social e rispettivi Social Network utilizzati

Definite le piattaforme Social, oggetto di studio, sono state caricate su di esse le immagini collezionate precedentemente. Per l'operazione di upload si è creato un apposito account di test su ognuna delle piattaforme e si è utilizzata la modalità di default di upload fornita dai Social selezionati. La conseguente operazione di download, è stata realizzata attraverso la ricerca dell'URL dell'immagine all'interno del sorgente HTML.
Il processo di upload e successivo download è stato eseguito attraverso 4 differenti browser web (Safari, Google Chrome, Mozilla Firefox and Opera).

4. ANALISI DELLE TRACCE LASCIATE DAI SOCIAL NETWORK

Le immagini ottenute dalle operazioni descritte nel paragrafo precedente, sono state collezionate allo scopo di analizzare le differenze tra il dato originale e quello ottenuto dopo il processo di upload e download da uno dei Social Network considerati.
L'analisi ha individuato delle tipiche tracce riguardanti ogni Social Network. Tali tracce sono state principalmente evidenziate nelle alterazioni del formato JPEG di un'immagine quali:

-nome file,
-dimensione immagine,
-EXIF,
-struttura file,
-informazioni relative alla compressione.

Le alterazioni che le immagini subiscono non sono dipendenti dal browser ma solo dalla piattaforma Social. Pertanto, non è stata fatta alcuna distinzione sul browser utilizzato. I dettagli delle alterazioni osservate per ogni piattaforma verranno riportati nei prossimi paragrafi.

4.1 Alterazione del nome del file

La valutazione effettuata, si è basata sulle alterazioni che ogni piattaforma effettua sul nome del file.
Tutte le piattaforme Social rinominano il file di input ad eccezione di *Google+*, che mantiene il nome del file immagine originale.
Nella tabella 5 vengono riportati i nuovi nomi dei file generati da ogni piattaforma per la corrispondente immagine avente come nome originale "IMG_2641.jpg".
Il nuovo nome, contiene al suo interno alcune informazioni utili tra cui l'ID dell'immagine ovvero un identificativo univoco che consente di costruire un URL che punta a "dove" l'immagine è memorizzata sulla piattaforma stessa (Image Lookup).
In particolare, per *Facebook*, *Flickr*, *Tumblr* e *Instagram* è possibile usare tale ID insieme alle API pubbliche (ad esempio Graph[6] per *Facebook*) per costruire il corrispondente URL [15] e risalire cosi all'immagine e all'account corrispondente.
Per quanto riguarda *Imgur*, è possibile risalire all'immagine avente nome "01- 8dmatWj.jpg" semplicemente navigando all'indirizzo *http://imgur.com/8dmatWj* , mentre *Twitter* consente di risalire all'immagine avente nome "*Cdp0a0qWoAAtKfd.jpg*" navigando all'indirizzo *https://pbs.twimg.com/media/Cdp0a0qWoAAtKfd.jpg* .
Le restanti piattaforme non codificano l'ID immagine all'interno dei nomi che vengono assegnati.
Altre informazioni utili presenti nel nome del file sono: la data di ricezione (*WhatsApp*) e la risoluzione dell'immagine (*Facebook*, *Flickr*, *Tumblr* e *Instagram*). A queste ultime informazioni si può risalire attraverso la presenza di particolari suffissi presenti all'interno del nome file (es. _n per *Facebok*).

Social	Image Lookup	Esempio
Facebook	**Si**	11008414_**746657488782610**_8508378989307666639_n.jpg
Google+	**no**	IMG_2641.jpg
Flickr	**Si**	26742193671_**8a63f10c85**_h.jpg
Tumblr	**Si**	tumblr_**o3q9ghRCRh1vnf44lo9**_1280.jpg
Imgur	**Si**	04 - **Dw0KXG2**.jpg
Twitter	**Si**	**CdqCPQ-WAAAzrHI.jpg**
whatsApp	**No**	IMG-20160314-WA0038.jpg
Tinypic	**No**	1zqdirm.jpg
Instagram	**Si**	1689555_**169215806798447**_744040439_n.jpg
Telegram	**no**	422114602_5593965449613038107.jpg

Tabella 5- tabella riepilogativa dell'alterazione dei nomi

Il nome file può da solo risolvere il problema di identificare la piattaforma da cui proviene un'immagine ma tale evidenza risulta essere molto debole; il nome di un file infatti, può essere facilmente modificato da un utente anche nel preciso istante in cui decide di scaricare un'immagine da un Social Network.

[6] **https://developers.facebook.com/docs/graph-api**

4.2 Alterazione della dimensione dell'immagine

Un'ulteriore importante traccia, che rappresenta un'evidenza lasciata da un Social Network sull'immagine, è il ridimensionamento. Analizzando i diversi Social, si è osservato come il ridimensionamento sia applicato solo se una condizione sull'immagine originale viene soddisfatta. In particolare, se il lato più grande (in pixel) dell'immagine da processare è maggiore di una determinata soglia, l'immagine viene ridimensionata, lo stesso valore di soglia diventa la dimensione del lato più lungo dell'immagine ridimensionata mentre il lato più corto viene scalato proporzionalmente.
In Tabella 6 vengono riportate le condizioni e i valori di soglia osservati per ogni piattaforma.

Social	Soglia
Facebook	960,2048
Google+	2048
Flickr	dipende dall'opzione di caricamento
Tumblr	1280
Imgur	Nessuno
Twitter	1024
whatsApp	1600
Tinypic	1600
Instagram	1080
Telegram	2560

Tabella 6- Soglie per il ridimensionamento delle immagini

Si è constatato come, a differenza degli altri Social, *Tumblr* è l'unica piattaforma che non effettua mai un ridimensionamento delle immagini caricate. Per quanto riguarda *Facebook* la condizione viene soddisfatta a meno di una soglia fissata dall'utente in fase di upload; in particolare, la soglia risulta essere pari a 960 se l'immagine viene caricata con l'opzione LQ (Low Quality) e di 2048 se invece viene scelta l'opzione HQ (High Quality). Infine per *Flickr* la condizione viene soddisfatta a meno di una soglia stabilita dall'utente in fase di caricamento.
Poiché le soglie sono pressoché diverse per ogni piattaforma, la dimensione osservata su un'immagine potrebbe essere una traccia dell'operazione di ridimensionamento effettuata dalla piattaforma corrispondente. Ad esempio, visto quanto detto finora, se un'immagine presenta, nel suo lato più lungo, una dimensione di 1280 pixel, è probabile che tale immagine sia stata processata e ridimensionata da *Tumblr*.

4.3 Alterazione della struttura del file JPEG

Come già accennato nel Paragrafo 2, lo standard JPEG impone una struttura ben definita ai file. La presenza o meno di alcuni campi della struttura potrebbe fornire un buon indizio sull'originalità dell'immagine. Gli studi effettuati hanno permesso di identificare le modifiche che i Social apportano a tale struttura. Naturalmente l'eliminazione di queste informazioni, anche se sono tutte di pochi Byte, viene effettuata al fine di risparmiare spazio di archiviazione da parte dei Social.

Gran parte dei Social oggetto di studio alterano la struttura del file in maniera differente. Tali variazioni hanno come conseguenza la riduzione del numero di *marker* presenti. Tale valore, calcolabile attraverso i campi descritti in Tabella 2, risulta essere un'evidenza lasciata su un'immagine e corrispondente alla piattaforma.

A tal uopo, sono state riscontrate delle strutture tipiche per *Facebook*, che presenta 26 *marker*; *Instagram*, che presenta 20 *marker* e *Twitter* che ne presenta 25. Tutte le altre piattaforme considerate utilizzano la stessa struttura e lo stesso numero di *marker* pari a 10.

4.4 Alterazione degli EXIF

La migliore evidenza, per quanto riguarda le informazioni sul dispositivo che ha acquisito un determinata immagine, si trova nei dati EXIF. Come già trattato nel Paragrafo 2.3, tra gli EXIF vengono memorizzate informazioni come: il modello della camera che ha acquisito l'immagine, la data e l'ora di acquisizione e anche le coordinate GPS corrispondenti. A tal proposito citiamo un reale caso di studio risolto proprio grazie a queste informazioni:

IL CASO HUAWEI

Un recente caso, che ha suscitato grande clamore mediatico, è stato quello che ha visto coinvolta la nota casa produttrice di cellulari: "Huawei".

La Huawei aveva basato la campagna pubblicitaria del suo nuovo prodotto puntando sulle altissime prestazioni della fotocamera integrata nello stesso. A tal fine aveva pubblicato su numerosi Social Network (tra cui Google+) un esempio di immagine di altissima qualità e definizione acquisita tramite il suo nuovo prodotto. Google+ mantiene tutti gli EXIF relativi al dispositivo di acquisizione, pertanto, scaricando tale immagine e analizzandone gli EXIF è stato facile appurare che il dispositivo che aveva acquisito l'immagine corrispondeva a una fotocamera "CANON EOS 5D Mark III" e non al nuovo modello di cellulare

"HUAWEI", come dichiarato.
L'immagine, infatti, era stata acquisita da una fotocamera di ultima generazione e di prestazioni qualitative elevate, ovviamente non paragonabili a quelle di una fotocamera presente in un dispositivo cellulare.

(inserire qui fig21)

Per gli scopi del nostro studio, le informazioni presenti negli EXIF sono state divise in due categorie: "dati sulla camera" con riferimento a quelle che consentono di effettuare il Camera Source Identification e "altri dati" per tutte le altre.

In Tabella 7 vengono riportate le osservazioni relative alle alterazioni degli EXIF ed è possibile osservare come ogni piattaforma cancella, mantiene o modifica la categoria di informazioni corrispondente. Come si può facilmente notare, la maggior parte delle piattaforme elimina tutte le informazioni presenti negli EXIF, specialmente quelle relative al modello di camera utilizzato per l'acquisizione, rendendo il Camera Source Identification basato su EXIF praticamente impossibile.

Social	**Modifica Exif**	
	Dati Camera	**Altri Dati**
Facebook	Elimina	Elimina
Google+	Mantiene	Mantiene/modifica
Flickr	Elimina	Mantiene/modifica
Tumblr	Mantiene	Mantiene/modifica
Imgur	Elimina	Elimina
Twitter	Elimina	Elimina
whatsApp	Elimina	Elimina
Tinypic	Mantiene	Mantiene/modifica
Instagram	Elimina	Elimina
Telegram	Elimina	Elimina

Tabella 7- Tabella riassuntiva del trattamento degli EXIF

4.5 Alterazione della compressione JPEG

Le operazioni di compressione che le piattaforme Social eseguono sulle immagini, alterano le immagini stesse (ed in particolare le componenti ad alta frequenza) al punto da rendere i metodi di Camera Source Identification basati sul PRNU, tranne alcune eccezioni, poco efficienti.

Anche in questo caso sono state confrontate coppie di immagini originali e processate al fine di individuare, per ciascuna piattaforma Social, le tracce individuabili nella ricompressione.

Sulla base di ciò, è possibile dividere le piattaforme considerate in due categorie: piattaforme che effettuano sempre una ricompressione (che dalle nostre osservazioni risultano essere: *Facebook*, *Twitter*, *Telegram*, *WhatsApp* e *Instagram*) e quelle piattaforme che eseguono una ricompressione solo sulla base di una condizione (che dalle nostre osservazioni risultano essere: *Google+*, *Tumblr*, *Tinypic*, *Imgur* e *Flickr*).

In Tabella 8 viene riportata la condizione che l'immagine caricata deve soddisfare per essere sottoposta a ricompressione.

Quando la piattaforma Social esegue la ricompressione, utilizza una tabella di quantizzazione avente coefficienti tipici della piattaforma stessa.

Social	Condizione di Ricompressione
Facebook	Sempre
Google+	M > 2048
Flickr	Dipende dall'opzione di caricamento
Tumblr	M > 1280
Imgur	La dimensione dell'immagine(MB)> 5,45 MB
Twitter	Sempre
whatsApp	Sempre
Tinypic	M > 1600
Instagram	Sempre
Telegram	Sempre

Tabella 8 – Condizioni di ricompressione dove M è il valore in pixel della dimensione massima dell'immagine in input

5. SOCIAL IMAGE FORENSICS: IMAGE BALLISTICS

Nei precedenti Paragrafi, sono stati elencati in dettaglio, per ognuno degli elementi di un'immagine in formato JPEG, le alterazioni subite durante il caricamento su un Social Network. Tali alterazioni costituiscono una vera e propria traccia, lasciata sull'immagine, del passaggio sulla piattaforma Social stessa. Purtroppo tali alterazioni, prese in considerazione singolarmente, possono non essere sufficienti per ricostruire l'origine di un'immagine. E' necessario quindi seguire un protocollo specifico per considerare l'insieme delle alterazioni al fine di giungere a conclusioni utili a identificare la piattaforma d'origine con un certo grado di compatibilità.
Nei seguenti Paragrafi verrà presentata una procedura utile per investigare su un'immagine alla ricerca della sua origine. A seguire verrà riportato a titolo esemplificativo un caso di studio.

5. 1 L'investigazione su un'immagine

Data un'immagine in formato JPEG, ci si pone il quesito di risalire all'origine dell'immagine.
In prima istanza è utile analizzare il nome del file immagine stesso. Tale nome, come visto nel Paragrafo 4.1, potrebbe essere identificativo del Social Network da cui l'immagine è stata scaricata. Una volta effettuata l'analisi sul nome, si può procedere ad analizzare gli EXIF, che se presenti possono identificare il modello della camera utilizzato.
Infine, estraendo i dati relativi alla dimensione dell'immagine, al numero di *marker* nella struttura del file JPEG e alle tabelle di quantizzazione, si può effettuare un confronto di queste con le alterazioni note che vengono effettuate dalle piattaforme e inferire di conseguenza la "storia" dell'immagine.
Una volta ricostruita la provenienza dell'immagine, qualora si disponesse anche dell'immagine originale, si potrebbe dimostrare la validità di tali evidenze, eseguendo un esperimento in cui, facendo ripercorrere all'immagine originale la storia ricostruita, si ottiene una nuova immagine perfettamente identica a quella oggetto dell'indagine in prima istanza.
Ulteriore considerazione va fatta riguardo alle alterazioni che possono variare nel tempo, essendo i Social Network degli applicativi software che evolvono continuamente, ciò richiede una continua sperimentazione da parte dell'esperto forense per avere certezza di quali siano le alterazioni per ogni Social in un dato momento. Inoltre tale processo potrebbe essere in parte automatizzato attraverso una procedura in grado di effettuare tali analisi in cascata.
E' bene notare come alcune tra le piattaforme considerate, effettuano alterazioni solo a meno di una condizione. Pertanto, un'immagine, potrebbe portare con sé evidenze parziali delle alterazioni di più Social Network permettendo di ricostruire un'ipotesi rispetto alla sua vera e propria storia.
Questo è quanto avviene nel caso di studio riportato nel paragrafo successivo.

5. 2 Caso di studio

In questo paragrafo, verrà presentato un possibile scenario che dimostra l'utilità delle informazioni provenienti dalle analisi, presentate nei paragrafi precedenti e che realizzano la Image Ballistics, su immagini processate da Social Network.

Il caso in questione è un caso di furto di informazioni coperte da segreto industriale e di estorsione. L'attore principale della storia è il sig. R, titolare della società XXX, che in data 1 Luglio riceve la seguente e-mail da un indirizzo anonimo:

> *Siamo in possesso di immagini contenenti i suoi segreti industriali, le consigliamo di visitare il forum che si trova al seguente indirizzo (https://www.forumallurlspecificato.it/) dove ne troverà pubblicate alcune. Se non verserà entro 3 giorni a partire da oggi, la somma di 10 Bitcoin all'indirizzo "33soi2mLAT73GGot66QaaNakPyswEaAbmb", tutte le immagini in nostro possesso verranno pubblicate sui più popolari Social Network a partire da Google+.*

Il sig. R, visitando l'indirizzo indicato nell'e-mail minatoria e appurando l'effettiva consistenza della minaccia decideva di non sottostare al ricatto.

In data 4 luglio il sig. R riceveva una nuova e-mail avente il seguente contenuto:

> *Poiché non ha ottemperato alla nostra richiesta la informiamo che stiamo procedendo alla divulgazione delle immagini su Google+. Ha ulteriori 3 giorni di tempo per versare 20 Bitcoin all'indirizzo "33soi2mLAT73GGot66QaaNakPyswEaAbmb" altrimenti procederemo nella divulgazione delle immagini, questa volta pubblicandole su Facebook.*

Il sig. R, intimorito dalle conseguenze che si sarebbero verificate per l'azienda a seguito della divulgazione delle immagini sui Social Network frequentati da milioni di persone, decide di sporgere regolare denuncia.

Al colloquio con gli investigatori, il sig. R comunicava che le uniche persone ad avere accesso ai dati oggetto del ricatto sono i signori: BBB, CCC, DDD e EEE. Nonostante tale informazione, per potere sporgere denuncia contro di essi, sarebbe stato necessario ottenere prove inconfutabili della loro colpevolezza. Le 2 e-mail ricevute dal sig. R, in tal senso, non contenevano tali evidenze. Pertanto, l'unica fonte di informazioni risultavano essere le immagini già pubblicate dai ricattatori.

Veniva quindi interpellato un esperto di Image Forensics che conosce bene le tecniche di Image Ballistics. Tramite tali tecniche l'esperto sarebbe stato in grado di ricostruire la storia delle immagini incriminate, estrapolando dati utili ai fini probatori.

L'operazione di analisi forense inizia quindi tramite il download delle immagini incriminate. L'esperto procede accedendo all'indirizzo del forum, comunicato nella prima e-mail, senza trovare purtroppo nessuna

pagina web essendo questa stata rimossa dai ricattatori. Egli procede quindi a scaricare le immagini pubblicate su Google+ collezionando il reperto n. 1.

L'analisi delle caratteristiche delle immagini del reperto n. 1 conferma la loro provenienza da Google+ essendo sia la dimensione dell'immagine che le tabelle di quantizzazione utilizzate compatibili con quelle conosciute per il Social. Le immagini non contengono però gli EXIF data. L'assenza di EXIF non permette di dare un giudizio sull'originalità delle immagini. L'esperto, infatti, sa bene che Google+ non cancella gli EXIF e nemmeno rinomina i file immagine caricati. Pertanto analizza i nomi dei file del reperto n. 1 trovando, per una di esse, una corrispondenza con il pattern di nomi tipico della piattaforma di condivisione di immagini Imgur (piattaforma comunemente utilizzata come hosting per le immagini pubblicate su forum e siti web).

Una volta recuperata quest'informazione, l'esperto, dato che all'interno del nome di un file di Imgur è presente l'Image ID che consente di effettuare l'image lookup, risale al corrispondente indirizzo su Imgur. Dall'indirizzo recuperato, l'esperto scarica l'immagine che effettivamente presenta gli stessi contenuti della corrispondente immagine del reperto n.1. Questa nuova immagine viene etichettata come reperto n. 2.

Il reperto n. 2 presenta caratteristiche diverse rispetto alla corrispondente immagine del reperto n. 1. Infatti ha una dimensione diversa (2560x1707) e delle tabelle di quantizzazione diverse. Solo il nome file coincide.

L'esperto, rileva un alto grado di compatibilità tra le caratteristiche estratte dal reperto n. 2 e la piattaforma di messaggistica mobile Telegram.

Partendo dall'evidenza che le immagini hanno subito un processamento tramite Telegram, unito alle informazioni fornite dal sig. R, si ottiene quindi dall' A.G. la possibilità di sequestrare i dispositivi cellulari dei signori BBB, CCC, DDD ed EEE, alla ricerca di una corrispondenza inequivocabile tra le informazioni ottenute dall'esperto e le immagini contenute nei dispositivi sequestrati. Dalle analisi sui dispositivi, risultava che nel cellulare di proprietà del sig. DDD erano presenti alcune immagini aventi medesimi contenuti dei reperti n.1 e n. 2. Inoltre, vista l'evidenza di processamento delle immagini pubblicate su Imgur, tramite Telegram, si è proceduto ad analizzare più in dettaglio il cellulare del sig. DDD, al fine di estrarre tutte le conversazioni effettuate con l'app di Telegram. Tale ricerca ha dato il seguente riscontro: in data 29 giugno il sig. DDD inviava tramite Telegram le immagini incriminate ad un numero di telefono corrispondente a un tale sig. AAA. Nessuna informazione è stata trovata per incriminare i signori BBB, CCC ed EEE che risultavano quindi estranei ai fatti.

Le immagini ritrovate all'interno del cellulare del sig. DDD, aventi lo stesso contenuto delle immagini dei reperti 1 e 2 e utilizzate per inoltrare il ricatto, presentavano ancora tutti gli EXIF e quindi nessuna caratteristica di alterazione da processamento da piattaforma Social.

A vista degli inquirenti queste immagini risultavano quindi essere le immagini originali scattate dal sig. DDD tramite la fotocamera del cellulare. A conferma di questo, gli EXIF riportavano il modello del dispositivo che aveva acquisito l'immagine e coincidente con quello di proprietà del sig. DDD.

Al fine di dare un carattere probatorio e scientifico all'evidenza trovata, gli investigatori hanno eseguito, per ogni immagine originale trovata nel dispositivo del sig. DDD, lo stesso processamento che ha percorso il

reperto n. 1 per arrivare fino a Google+: sono state inviate tramite Telegram, quindi caricate su Imgur e infine condivise tramite l'apposito pulsante su Google+. Il confronto tra le immagini così ottenute e quelle del reperto n. 1 confermava una perfetta coincidenza tra tutti gli elementi JPEG.

Il ritrovamento delle immagini, delle corrispondenti conversazioni Telegram, e la ricostruzione inequivocabile della storia delle immagini, ha dimostrato in maniera scientifica e non ripudiabile la colpevolezza del sig. DDD nella diffusione di immagini contenenti segreto industriale e la complicità del sig. AAA nella diffusione e nella messa in opera del ricatto a scapito del sig. R.

6. CONCLUSIONI

Le tecniche di Image Forensics costituiscono un utile strumento di indagine a disposizione degli investigatori per poter estrarre ed inferire informazioni dalle immagini digitali. In questo articolo ci si è soffermati sugli aspetti legati al riconoscimento ed individuazione di caratteristiche peculiari che le immagini posseggono dopo aver subito alterazioni di vario tipo da parte dei Social Network. Sono stati presentati alcuni concetti di base, necessari per poter comprendere i dettagli tecnici su cui gli studi effettuati si sono basati. Infine è stato presentato un protocollo di analisi per la ricostruzione della storia di un'immagine digitale.

Sulla base delle analisi riportate, abbiamo sviluppato un approccio automatico e sperimentale di Image Ballistics che permette la classificazione dell'origine di un'immagine a partire dalle tracce lasciate dal processamento delle piattaforme Social. Tale approccio, pur essendo ancora in fase prototipale, risulta essere promettente e verrà a breve condiviso con la comunità scientifica internazionale.

Infine, crediamo sia possibile inferire la "storia" di un'immagine a partire da una originale attraverso analisi di processamenti differenti a quelli trattati quali: applicazione di filtri speciali o il cropping.

Per essere in grado di recuperare o di inferire delle evidenze di prova, sfruttando le tecniche presentate, sono necessarie competenze specifiche nel dominio della teoria dell'elaborazione delle immagini.

BIBLIOGRAFIA

[1] Piva, A. – An overview on image forensics. Proceedings of ISRN Signal Process., 2013, p. 496701.

[2] Stamm, M.C, Wu, M., Liu, K.J.R. – Information forensics: An overview of the first decade. IEEE Access, vol. 1, pp. 167–200, May 2013.

[3] S. Battiato, G. Messina, R. Rizzo – *Image Forensics - Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive* - Chapter in *IISFA Memberbook 2009 DIGITAL FORENSICS*– Eds. G. Costabile, A. Attanasio – Experta, Italy 2009

[4] S. Battiato, G.M. Farinella, G. Puglisi – *Image/Video Forensics: Casi di Studio* - Chapter in *IISFA Memberbook 2011 DIGITAL FORENSICS* - Eds. G. Costabile, A. Attanasio - Experta, Italy 2012

[5] Farid, H – Digital image ballistics from JPEG quantization, Tech. Rep. TR2006-583, Department of Computer Science, Darthouth College (2006).

[6] J. Luk´aˇs, J. Fridrich, and M. Goljan – "Digital camera identification from sensor pattern noise," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205–214, June 2006.

[7] 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)

[8] G. Cattaneo, U. F. Petrillo, M. Ianulardo, G. Roscigno – *Nuovi Metodi di Indagine basati su Immagini Digitali e Rumore Caratteristico del Sensore*- Chapter in IISFA Memberbook 2015: DIGITAL FORENSICS- Eds. G. Costabile, A. Attanasio, M. Ianulardo.

[9] Battiato, S., & Messina G. – *Digital forgery estimation into DCT domain: a critical analysis*. In Proceedings of the First ACM workshop on Multimedia in forensics (pp. 37-42). ACM.

[10] Galvan, Fausto, G. Puglisi, A. R. Bruna, S.Battiato. – "*First quantization matrix estimation from double compressed JPEG images*." IEEE Transactions on Information Forensics and Security 9.8 (2014): 1299-1310.

[11] G. K. Wallace – *The JPEG Picture Compression Standard*. IEEE Transactions on Consumer Electronics 38.1 (1992).

[12] Battiato, S., Mancuso, M., Bosco, A., & Guarnera, M. (2001, September) – *Psychovisual and statistical optimization of quantization tables for DCT compression engines*. In Image Analysis and Processing, 2001. Proceedings. 11th International Conference on (pp. 602-606). IEEE ISO 690.

[13] J. Miano – *Compressed image file formats : JPEG, PNG, GIF, XBM, BMP*. Addison Wesley, 1999 ISBN : 0201604434.

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

[15] M.Moltisanti, A. Paratore, S. Battiato, L. Saravo, *Image Manipulation on Facebook for Forensics Evidence*, Lecture Notes in Computer Science. Springer International Publishing, Proceedings of ICIAP 2015, Vol. 9280, pp.506-517.