LA VALIDITÀ PROBATORIA DELLE IMMAGINI E DEI VIDEO

di Sebastiano Battiato e Fausto Galvan

❶ *Introduzione*

Il numero di immagini in circolazione sul *web,* e non solo, è in costante aumento. Nel 2008 il numero di telecamere installate nel mondo ammontava a circa 11 milioni; per il 2013 ci si attende che il loro numero raggiunga i 30 milioni. 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, e su Facebook sono state inserite circa 300 milioni di fotografie digitali **[1]**. Questo scenario ha un inevitabile riscontro in ambito forense: è sempre più improbabile che un evento delittuoso possa consumarsi senza che la scena del crimine o parte di essa, oppure l'autore del fatto, non vengano ripresi da un sistema di videosorveglianza. La relativa facilità con cui al giorno d'oggi l'uso di *software* di fotoritocco o di *editing* video, anche di facile reperimento, permette di "comporre" una immagine o "montare" una scena alterandone i contenuti originari impone, come in parte accennato in **[2]**, che l'acquisizione ed il trattamento di immagini e video digitali sia regolato da "*best practice*" di riferimento.

❷ *Pellicola vs Sensore: due epoche a confronto*

Prima dell'avvento della fotografia digitale, molto raramente veniva messa in dubbio l'autenticità di una immagine presentata come fonte di prova in un procedimento giudiziario. Nel caso in cui fosse stato necessario corredare un fascicolo di indagine delle relative fotografie, era comunque prassi depositare anche la pellicola da cui queste provenivano, i cosiddetti negativi. In realtà anche questi ultimi potevano essere alterati, sia agendo fisicamente sulla pellicola asportando od aggiungendo alcune parti e poi sviluppando l'immagine dal negativo modificato (Fig.1), oppure duplicando il negativo con una apposita strumentazione dopo avere applicato opportune maschere atte a nascondere od inserire i particolari voluti. In entrambi i metodi però, le modifiche erano rilevabili da un occhio esperto: nel primo caso era sufficiente esaminare il negativo modificato per notare i ritocchi, nel secondo si sfruttavano le diverse caratteristiche (grana, spessore) del negativo-copia, che per motivi tecnici non erano mai uguali a quelli dei rullini delle fotocamere.

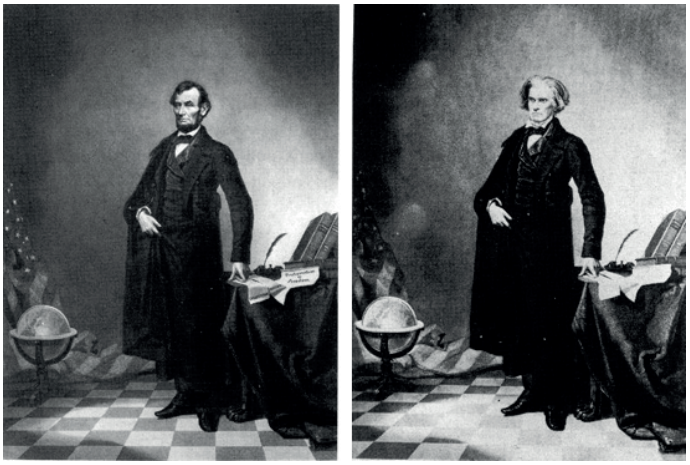

Figura 1: l'immagine di sinistra, nota come la prima contraffazione fotografica (1860 ca.), è ottenuta unendo la testa del presidente americano Abraham Lincoln al corpo del politico sudista John Calhoun (a destra) [3].

Rispetto al contesto analogico, in cui l'immagine "si forma stabilmente" sulla pellicola, nelle odierne fotocamere l'informazione sulla scena "transita" nel sensore (l'analogo funzionale della pellicola) prima di essere salvata nella memoria di massa decisa dall'utente **[2]**. Negli apparati digitali nulla vieta all'operatore di cancellare in tempo reale l'immagine appena scattata, se questa non lo soddisfa, dopo averla preliminarmente visionata sul display o addirittura agire sulla memoria di massa successivamente allo scatto per alterare o sostituire il contenuto originario. Per un confronto approfondito tra vecchi e nuovi metodi di "*forgery*" si veda **[4,5]**.

❸ *L'approccio scientifico nel definire l'autenticità di una immagine o di un video digitale*

Accertare l'integrità di una immagine o di un video rappresenta un compito notevolmente più difficile di un tempo: non vi sono segni su un negativo o spessori di pellicole da controllare, ma una quantità enorme di dati, che vanno interpretati valutandone anche il grado di attendibilità. Bisogna innanzitutto ricostruire la cosiddetta catena di custodia (*chain of custody*) al fine di garantire la non alterabilità dei dati come pre-requisito indispensabile alla accettazione di qualsiasi fonte di prova. Inoltre, è fondamentale l'analisi dei *metadati*: informazioni contenute nello *stream* del *file* in cui sono riportati, tra gli altri, la data di creazione, le impostazioni della macchina al momento di riprendere la scena, eventuali miniature delle immagini (*thumbnail*) ed in taluni casi le coordinate GPS della posizione della camera al momento dello scatto. I metadati (es. EXIF, XMP, ecc.), possono essere utilizzati per isolare evidenze investigative, per verificare eventuali inconsistenze con le informazioni visive nelle immagini (es, una scena notturna associata ad un'orario di ripresa diurno) e per evidenziare alcune manipolazioni, anche se un utente esperto potrebbe modificarli/alterarli mediante appositi *software*.

Infine, nel caso in cui si utilizzi apparati di fascia medio/alta, è possibile che questi forniscano la possibilità di imprimere sulle immagini i cosiddetti *watermark*: piccoli "timbri" digitali la cui presenza (o assenza) può essere utile per validare una immagine. È possibile infine sfruttare metodi di *Image/Video Forensics* che derivano direttamente dalla teoria dell'elaborazione della immagini. È il caso ad esempio della ricerca delle tracce lasciate dalla doppia quantizzazione, uno dei metodi "*format based*" descritti in dettaglio in **[9]**. Nel caso del formato compresso JPEG, che copre più del 90% delle immagini in circolazione, l'immagine prima di essere memorizzata subisce una compressione, in parte dovuta al processo di "quantizzazione" a cui è sottoposta.

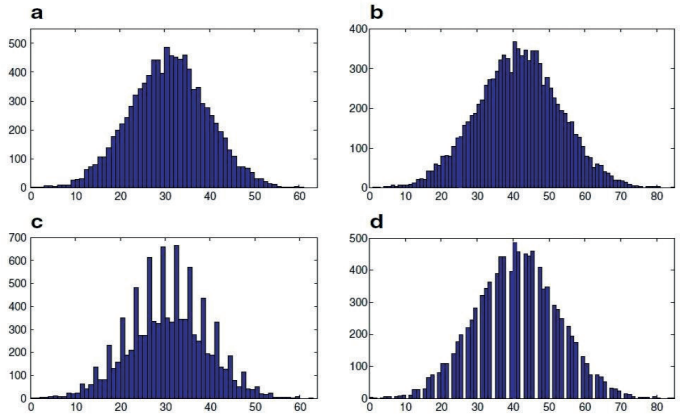

Figura 2: istogramma dei valori assunti da un coefficiente dell'immagine nel caso di singola quantizzazione, con q1 (il coefficiente della prima compressione) pari a 4 (a), e 3 (b), a confronto con gli andamenti dello stesso termine dopo che l'immagine è stata sottoposta a doppia quantizzazione con q1 = 3 e q2 = 4 (c), oppure con q1 = 4 e q2 = 3.

In occasione di una eventuale modifica, essa dovrà essere decompressa per poter essere visualizzata, e nuovamente compressa in occasione del definitivo salvataggio. Per ragioni legate alla non reversibilità (il formato JPEG è infatti detto "*lossy*", cioè "con perdita di informazione") della procedura, questo doppio salvataggio lascerà alcune "tracce caratteristiche", diverse da quelle che si evidenziano in caso di singola compressione. La figura 2 mostra queste differenze, ben visibili anche ad occhio nudo **[6,8]**. Sebbene un doppio salvataggio dell'immagine non implichi di per sé un'avvenuta manipolazione (si potrebbe visualizzare l'immagine, non inserire alcuna modifica e poi risalvarla) sicuramente dopo questo procedimento l'immagine non è più quella originale. L'utilizzabilità in termini legali di questo risultato è evidente.

❹ *L'utilizzo della Image/Video Forensics nei casi reali*

Tra i molti episodi in cui i metodi di *Image Forensics* sono state utilizzati come strumenti di indagine, appare sicuramente degno di nota il caso della "mozzarella blu": nel 2010 alcune mozzarelle in vendita presso la grande distribuzione, all'apertura della confezione presentavano una colorazione bluastra a chiazze, causata da alcune anomalie nel processo di produzione e dalla presenza di un batterio. Il sequestro del prodotto in tutti i punti vendita italiani ha dato al caso una risonanza mediatica oltremodo rilevante. Come conseguenza dell'episodio, si è assistito in rete al proliferare di immagini riproducenti mozzarelle colorate con le più svariate tonalità. Come ancora oggi è possibile verificare effettuando una ricerca sul *web* con le parole chiave "mozzarella blu", numerose immagini provengono da alterazioni artificiose delle componenti "cromatiche" della medesima foto, con il chiaro intento di enfatizzare il messaggio codificato nell'immagine.

Mediante l'ispezione di alcune caratteristiche di base delle immagini, ad esempio il loro istogramma, gli esperti di *Image Forensics* hanno potuto mettere in evidenza numerose manipolazioni e, tramite l'acquisizione "forense" dei dati nei siti in cui erano presenti le immagini, risalire anche alla presunta fonte di prova inquinata iniziale **[7]**. Bisogna quindi riflettere anche sull'interpretazione semantica del termine "alterazione": non si tratta solo di "togliere" o "aggiungere" particolari all'immagine (o al video), ma anche di modificarne i valori di luminosità o di colore, allo scopo di alterarne l'aspetto e quindi il messaggio associato alla fruizione della stessa. Citiamo a tal proposito un recente caso **[10]** riguardante le "alterazioni" che avrebbe subito l'immagine vincitrice del premio "World Photo Press 2012". In merito all'ammissibilità, ed in genere all'utilizzo in dibattimento di fonti di prova costituite da immagini e video, è sicuramente interessante quanto riportato a proposito dell' "ammissibilità e regole di valutazione per immagini" relative ai fatti del G8 svoltosi a Genova nel 2001 **[11]**. In primo luogo perchè si ricorda che "*l'art. 189 c.p.p. prevede espressamente prove non disciplinate dalla legge e la giurisprudenza costante del S.C. riconosce alle immagini fotografiche e filmate valenza di documento figurativo, del tipo testimoniale e diretto.*" Inoltre, si fa rilevare come "*la stessa giurisprudenza ammette, poi, in materia di prove filmiche l'utilizzo, anziché dell'originale, della copia del documento, quando emessa sia idonea ad assicurare l'accertamento dei fatti*". Infine, il collegio replica alle obiezioni sull'utilizzo di fonti di prova, costituite da filmati che a dire della difesa non sarebbero ammissibili in quanto "*formati dalla giustapposizione di materiale vario, selezionato e montato […]*" sottolineando come questo non basti a determinare la loro non utilizzabilità, "*fatte salve la possibilità per le altre parti di addurre elementi idonei a dimostrare eventuali difetti di genuinità e manipolazioni arbitrarie delle immagini stesse.*"

❺ *Conclusioni*

La tecnologia sviluppata negli ultimi decenni fornisce strumenti sempre più potenti sia a chi intende manipolare un'immagine, che a colui che necessita di provarne l'autenticità. Alcuni accorgimenti e metodologie operative, più o meno sofisticate, qualora messe in pratica correttamente possono evitare errori che pregiudicano l'accettabilità in giudizio di documenti visivi. Altre procedure, dedicate all'analisi dei reperti, fanno uso di concetti e risultati provenienti direttamente dal mondo della ricerca e necessitano di un uso accorto e di una interpretazione dei risultati effettuata da utenti esperti. Le esperienze "sul campo", dimostrano una volta di più che la strada da percorrere è quella di una standardizzazione delle procedure di analisi. ©

RIFERIMENTI

[1] http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/ (2013).
[2] S. Battiato, F. Galvan – "Introduzione alla Image/Video Forensics"- Sicurezza e Giustizia n. I /MMXIII - pp 42-43.
[3] http://www.cs.dartmouth.edu/farid/research/digitaltampering/ (2013)
[4] http://petapixel.com/2013/05/08/how-photographers-photoshopped-their-pictures-back-in-1946/ (2013)
[5] Cynthia Baron Adobe PhotoShop Forensics: *Sleuths, Truths, and Fauxtography* (2007) ISBN-13:978-1598634051
[6] J.A. Redi et al: *Digital image forensics: a booklet for beginners*. Multimed Tools Appl (2011) 51:133 – 162
[7] S. Battiato, G.M. Farinella, G. Puglisi - "*Image/Video Forensics: Casi di Studio*" Chapter in IISFA Memberbook (2011)
[8] S. Battiato, G. Messina: *Digital Forgery Estimation into DCT Domain - A Critical Analysis*. ACM Multimedia 2009 Workshop Multimedia in Forensics (2009)
[9] S. Battiato, G. Messina, R. Rizzo – "*Image Forensics. Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive*" Chapter in IISFA Memberbook (2009).
[10] http://daily.wired.it/news/cultura/2013/05/17/world-press-photo-34648.html (2013)
[11] http://www.processig8.org/Udienze%2025/Ud.%20143/143_motivazioni-03_25.html (2013).◊