

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/242495487>

Image Forensics Contraffazione Digitale e Identificazione della Camera i Acquisizione: Status e Prospettive d

ARTICLE

READS

26

3 AUTHORS, INCLUDING:



Sebastiano Battiato

University of Catania

267 PUBLICATIONS **1,842** CITATIONS

SEE PROFILE



Giuseppe Messina

STMicroelectronics

48 PUBLICATIONS **380** CITATIONS

SEE PROFILE

Image Forensics

Contraffazione Digitale e Identificazione della Camera di Acquisizione: Status e Prospettive

Sebastiano Battiato - Giuseppe Messina - Rosetta Rizzo

Università di Catania

Dipartimento di Matematica ed Informatica

Image Processing Laboratory

Viale Andrea Doria 6 - 95125 Catania, Italy

IPLAB - <http://iplab.dmi.unict.it>

email: {battiato,gmessina, rosetta.rizzo}@dmi.unict.it

Introduzione all'Image forensics

“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” (SWGIT – www.fbi.gov)

Per Image Forensics si intende tutto ciò che riguarda l'attività di analisi delle immagini (che siano esse digitali o meno) per la validazione in ambito forense.

La bibliografia nel campo dell'elaborazione dell'immagine per uso forense si può suddividere nelle seguenti principali categorie:

- **Image Forgery Identification:** Identificazione di manipolazione, ovvero inserimento o cancellazione di particolari, di un'immagine, mediante analisi dei dati.
- **Image Source Identification:** Individuazione del tipo di sorgente che ha generato l'immagine, sia dal punto di vista del modello (macchina fotografica Canon, Nikon, Hp, Olympus, ecc.) sia dal punto di vista dell'apparecchiatura (scanner, fotocamera).
- **Image Reconstruction:** Restauro di immagini deteriorate al fine di identificare, anche parzialmente, il contenuto originale.
- **Self Embedding:** Tecniche di inserimento ed estrazione di informazioni all'interno dell'immagine al fine di alterarne il contenuto (per esempio sostituendo il reale codice di una targa di una macchina con uno fittizio).
- **Video Analysis:** Analisi comportamentale, per esempio al fine di individuare comportamenti sospetti oppure abbandono, o furto di oggetti.
- **Ricostruzione 3D:** Estrazione delle informazioni tridimensionali contenute all'interno della scena per ricavare misure originali (per esempio l'altezza di un individuo, oppure la velocità di un mezzo).
- **Steganografia:** Individuazione di informazioni nascoste all'interno di un'immagine mediante watermarking o tecniche simili.

In questo documento ci si occuperà solamente dei primi due aspetti che hanno assunto particolare rilevanza anche nella comunità scientifica di riferimento, come dimostrato dal numero crescente di paper scientifici che riguardano proprio questi aspetti. Cercheremo di distinguere tra le tecniche puramente accademiche [1], al confine della ricerca, rispetto a ciò che invece è già disponibile e pronto per essere utilizzato in ambito forense [2] e [3].

Fondamenti di Elaborazione delle Immagini

Le immagini digitali possono essere rappresentate come un segnale discreto bidimensionale (e cioè rappresentabile mediante dei numeri finiti e con una certa precisione) in grado di replicare la sensazione percettiva legata alla visione di una scena reale con una certa fedeltà/qualità. La differenza quindi rispetto alle immagini analogiche sta nella rappresentazione intrinseca dell'informazione da visualizzare. In generale un'immagine digitale è ottenuta attraverso un campionamento spaziale che scarta necessariamente delle informazioni dal mondo continuo (e analogico). Questo processo ne determina la cosiddetta risoluzione spaziale che, per esempio, nelle fotocamere digitali viene misurata in MegaPixel. All'aumentare della risoluzione migliora l'accuratezza nella rappresentazione delle variazioni più piccole, ai dettagli, che in gergo tecnico vengono definite alte frequenze. La conversione nella rappresentazione digitale, rappresenta il segnale con un numero fissato di bit per campione. Questo numero rappresenta la precisione del campione. L'utilizzo di 8 bit per campione è solitamente sufficiente a dare l'illusione di un intervallo continuo di valori a scala di grigio, quando l'immagine viene visualizzata in un tipico display CRT (o LCD). Rappresentazioni con più bit si possono incontrare in applicazioni mediche, militari e scientifiche. Ogni campione in un'immagine monocromatica (o a colori) viene chiamato pixel o pel. Pixel è l'abbreviazione di "picture element".

La Figura 1 mostra tre diversi tipi di immagini digitali. Essi sono tutti esempi di immagini digitali "still" (ferme); il termine "still" è usato per distinguerle dalle sequenze di immagini in movimento. A 8 bit/campione, l'immagine di esempio, mostrata nella Figura 1 (a), ha sufficiente precisione da essere considerata un'immagine a scala di grigi o a tono continuo.



Figura 1 (a) immagine a scala di grigi, 8-bit/campione. (b) Immagine binaria, 1-bit/campione; (c) immagine a colori, 24-bit/campione.

La stessa immagine campionata con un solo bit per campione è mostrata in Figura 1 (b); si parla in questo caso di un'immagine binaria o bi-livello. I toni di grigio rappresentabili sono ovviamente solo due, bianco e nero. Con opportune tecniche di *digital halftoning* è possibile simulare l'effetto di toni continui in un'immagine binaria alternando, tra spazi chiusi, campioni bianchi e neri. Si pensi alle immagini stampate tipicamente sui quotidiani cartacei. L'immagine presentata in Figura 1 (c) mostra invece una versione a colori dello stesso viso di Lena [4] ottenuta utilizzando ben 24 bit per campione con delle convenzioni opportune. In particolare i 24 bit vengono ripartiti in 3 gruppi distinti di 8 bit, ciascuno dei quali tiene traccia della quantità di colore **Rosso** (*Red*), **Verde** (*Green*) e **Blu** (*Blue*) necessaria a riprodurre una data sensazione cromatica. In pratica ciascun pixel, in accordo con la teoria del tristimolo, agisce selettivamente su tre classi di recettori nell'occhio operando su certe frequenze dello spettro di luce visibile e producendo l'effetto dei colori. Con 24 bit si è in grado di codificare circa 16 milioni di colori che sono una quantità più che sufficiente a rappresentare fedelmente una qualsiasi scena reale. Ovviamente le immagini digitali, tipicamente non contengono un numero così alto di colori, ma questo "alfabeto" così ricco consente una scelta molto accurata. Proprio per questo motivo le immagini a 24 bit, sono anche dette immagini *True Colors*. Un'immagine a colori può quindi essere idealmente vista come la composizione di 3 immagini a colori così come mostrato in Figura 2.

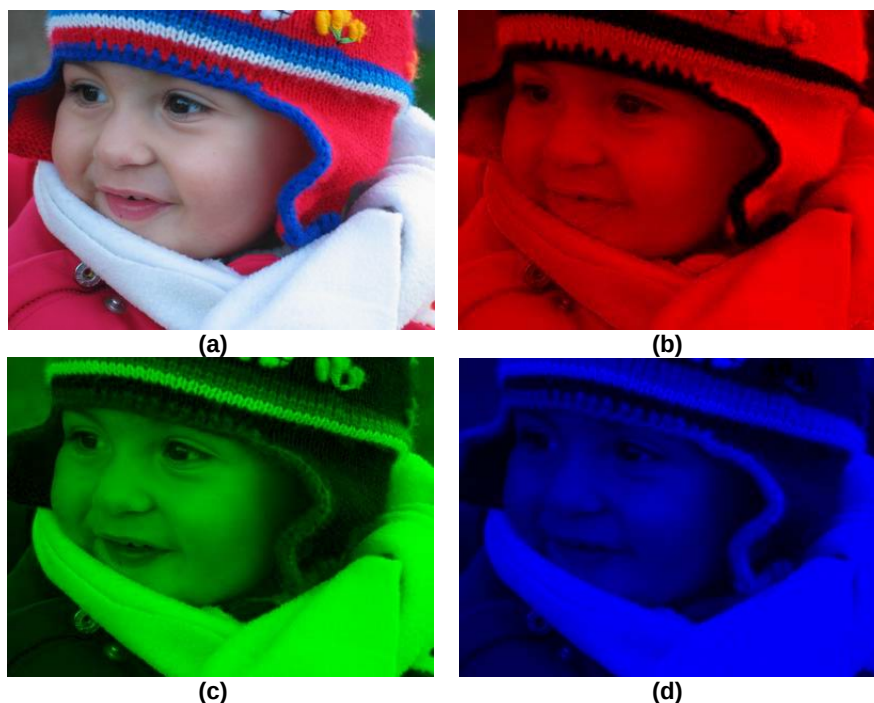


Figura 2 - Un esempio di immagine a colori e i relativi piani di colore del rosso, del verde e del blu.

Un immagine digitale può essere oggetto di diverse manipolazioni, che permettono di migliorarne la qualità o di restaurarne l'aspetto. Tra queste citiamo a titolo esemplificativo le tecniche di manipolazione dell'istogramma (miglioramento del contrasto, equalizzazione, ecc.) e le tecniche di filtraggio spaziale utili per esempio ad evidenziare i contorni o ad attenuare il rumore. Per maggiori dettagli si veda [5] e [6].

La compressione JPEG:

JPEG è l'acronimo di Joint Photographic Experts Group, un comitato ISO/CCITT che ha definito il primo standard internazionale di compressione per immagini a tono continuo, sia a livelli di grigio che a colori. E' un formato gratuito e open-source.

Attualmente JPEG è lo standard di compressione, delle immagini fotografiche, più utilizzato. Le estensioni più comuni per questo formato sono .jpeg, .jpg, .jfif, .JPG, .JPE, anche se il più comune su tutte le piattaforme è .jpg.

JPEG specifica solamente come un'immagine possa essere trasformata in uno stream di byte, ma non come questo debba essere incapsulato in supporti di memorizzazione. Un ulteriore standard chiamato JFIF (JPEG File Interchange Format), creato da Independent JPEG Group, specifica come produrre un file appropriato per la memorizzazione su computer di uno stream JPEG. Nell'uso comune, con il termine "file JPEG" generalmente si intende un file JFIF o alcune volte un file Exif JPEG.

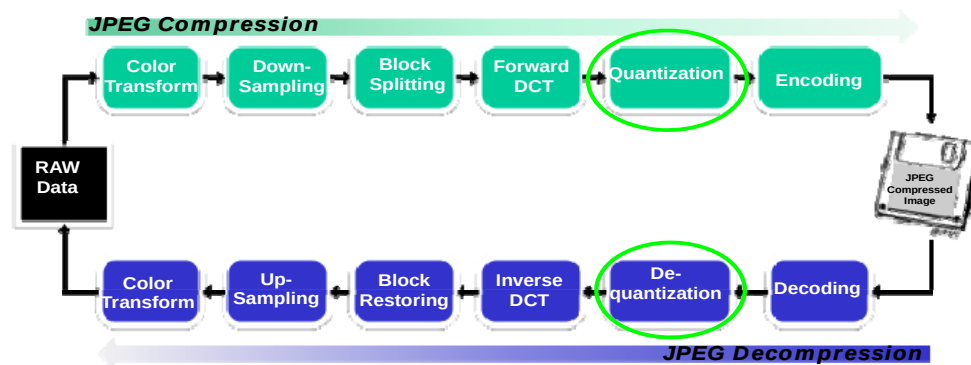


Figura 3– Compressione e decompressione mediante lo standard JPEG

La conversione di uno stream di byte in formato JPEG avviene nel seguente modo:

- L'immagine, composta da pixel **RGB**, è convertita nel formato **YCbCr**;
- I due canali di cromaticità, C_r e C_b , sono ridotti, di un fattore variabile tra $\frac{1}{2}$ e $\frac{1}{4}$, in altezza e larghezza;

- c) I tre canali Y, C_r e C_b sono suddivisi in blocchi di 8x8 punti;
- d) Ad ogni blocco è applicata la Trasformata Discreta del Coseno (DCT);
- e) I coefficienti DCT sono quantizzati (processo con perdita di dati) tramite delle tabelle pre-caricate;
- f) Infine si applica una codifica entropica (**compressione senza perdita di dati**), completando così la codifica JPEG.

Di seguito descriveremo nel dettaglio le varie parti della codifica.

Conversione del colore e riduzione di scala:

Il primo passo dell'algoritmo consiste nel convertire ogni pixel dal formato RGB (dati provenienti da immagini non compresse) al formato YC_bC_r. A tale scopo si usa la seguente formula di conversione:

$$\begin{aligned}
 Y &= 0.299 \cdot R + 0.587 \cdot G + 0.114 \cdot B \\
 C_b &= -0.169 \cdot R - 0.331 \cdot G + 0.500 \cdot B \\
 C_r &= 0.500 \cdot R - 0.419 \cdot G - 0.081 \cdot B
 \end{aligned}$$

La componente Y rappresenta la luminanza, le componenti C_b e C_r rappresentano invece le cromaticanze (cromaticanza blu e cromaticanza rossa rispettivamente).

Le cromaticanze sono in genere ridotte in scala poiché, per via della densità dei recettori della luminanza e della cromaticanza del colore nell'occhio, gli esseri umani sono in grado di rilevare molti più particolari nel canale della luminanza piuttosto che in quelli delle cromaticanze. Le cromaticanze possono essere dimezzate sia in termini di altezza e di larghezza dell'immagine (1/4 della dimensione originale), che semplicemente in termine di altezza dell'immagine (1/2 della dimensione originale).

Blocchi 8x8

Dopo aver convertito l'immagine, i tre canali sono suddivisi in blocchi di dimensioni 8x8 "pixel". Qualora la dimensione del canale non fosse multipla di 8 occorrerà aggiungere una certa quantità di dati fittizi all'ultima riga (e/o colonna) di blocchi. In genere si replicano i pixel di bordo dell'immagine al fine di evitare artefatti sgradevoli lungo i contorni.

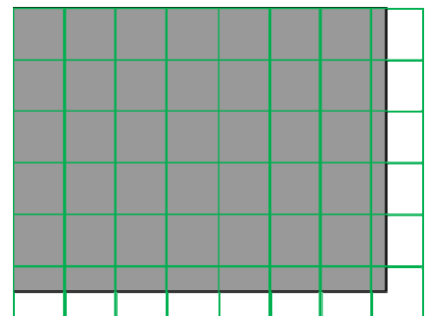


Figura 4 – Suddivisione in blocchi 8x8.

Trasformata Discreta del Coseno (Discrete Cosine Transform – DCT)

Da questo punto in poi ogni blocco è processato singolarmente. Questo procedimento rende l'algoritmo di compressione indipendente dalla dimensione delle immagini, inoltre l'elaborazione a blocchi permette di velocizzare notevolmente le operazioni necessarie alla compressione.

In questa fase i blocchi dei singoli canali (Y, Cb, Cr) sono convertiti nello spazio delle frequenze. La funzione di trasformazione utilizzata è una trasformata discreta del coseno, normalizzata, di tipo II (DCT).

Al fine di migliorare la comprensione di tale trasformazione consideriamo il seguente esempio di blocco di luminanza (il processo è analogo per le crominanze):

52	55	61	66	70	61	64	73
63	59	55	90	109	85	69	72
62	59	68	113	144	104	66	73
63	58	71	122	154	106	70	69
67	61	68	104	126	88	68	70
79	65	60	70	77	68	58	75
85	71	64	59	55	61	65	83
87	79	69	68	65	76	78	94

Poiché stiamo considerando un esempio basato su un blocco di luminanza, al fine di attuare la DCT occorre traslare i valori da $[0..255]$ a $[-128..127]$. Lo scopo è quello di centrare i valori intorno allo zero. Per fare ciò basta semplicemente sottrarre 128 ad ogni valore della matrice del blocco. Otterremo quindi la seguente matrice:

-76	-73	-67	-62	-58	-67	-64	-55
-65	-69	-73	-38	-19	-43	-59	-56
-66	-69	-60	-15	16	-24	-62	-55
-65	-70	-57	-6	26	-22	-58	-59
-61	-67	-60	-24	-2	-40	-60	-58
-49	-63	-68	-58	-51	-60	-70	-53
-43	-57	-64	-69	-73	-67	-63	-45
-41	-49	-59	-60	-63	-52	-50	-34

Il passo successivo consiste nel applicare la trasformata DCT al blocco 8x8. La trasformata è così definita:

$$G_{u,v} = \alpha(u)\alpha(v) \sum_{x=0}^7 \sum_{y=0}^7 g_{x,y} \cos\left[\frac{\pi}{8}\left(x + \frac{1}{2}\right)u\right] \cos\left[\frac{\pi}{8}\left(y + \frac{1}{2}\right)v\right]$$

dove

- u è la componente di frequenza orizzontale, per interi con $0 \leq u < 8$.
- v è la componente di frequenza verticale, per interi con $0 \leq v < 8$.

- la funzione di normalizzazione $\alpha(n) = \begin{cases} \sqrt{\frac{1}{8}}, & \text{se } n = 0 \\ \sqrt{\frac{2}{8}}, & \text{altrimenti} \end{cases}$
- $g_{x,y}$ è il valore del pixel in (x, y)
- $G_{u,v}$ è il valore del coefficiente della trasformata DCT in (u, v)

La trasformata DCT non fa altro che convertire il blocco in ingresso in funzione di una base di frequenze note. Nella figura sono rappresentate le componenti in frequenza usate dalla DCT. Il coefficiente in alto a sinistra è quello più significativo ed è detto coefficiente DC, i rimanenti 63 coefficienti sono detti AC e rappresentano le combinazioni di frequenze verticali e orizzontali (via via crescenti).

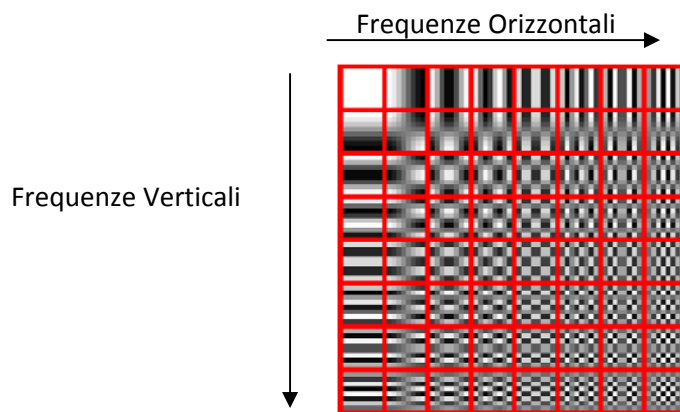


Figura 5 – Base delle frequenze DCT.

La trasformata DCT ha lo scopo di convertire il blocco in input in un nuovo blocco 8x8 dove ogni elemento della nuova matrice corrisponde alla "quantità" di componente di ogni data frequenza necessarie per descrivere il segnale originale.

Applicando la trasformata alla matrice 8x8 dell'esempio, arrotondando all'intero più vicino, otteniamo:

$$\begin{bmatrix} -415 & -30 & -61 & 27 & 56 & -20 & -2 & 0 \\ 4 & -22 & -61 & 10 & 13 & -7 & -9 & 5 \\ -47 & 7 & 77 & -25 & -29 & 10 & 5 & -6 \\ -49 & 12 & 34 & -15 & -10 & -6 & 2 & 2 \\ 12 & -7 & -13 & -4 & -2 & 2 & -3 & 3 \\ -8 & 3 & 2 & -6 & -2 & 1 & 4 & 2 \\ -1 & 0 & 0 & -2 & -1 & -3 & 4 & -1 \\ 0 & 0 & -1 & -4 & -1 & 0 & 1 & 2 \end{bmatrix}$$

Il vantaggio della trasformata DCT è la sua tendenza ad aggregare gran parte dei valori del segnale in un angolo (in alto a sinistra), come è visibile

anche nell'esempio. La quantizzazione, che segue immediatamente la trasformata, accentua ulteriormente questa tendenza. La conseguenza di ciò è un elevato grado di comprimibilità delle informazioni ricavate.

Campionamento mediante Tabelle di Quantizzazione

Come precedentemente accennato l'occhio umano è molto meno sensibile alle variazioni contenute nelle alte frequenze. Questa condizione permette di ridurre drasticamente la quantità di informazioni fornite dalle alte frequenze contenute nelle immagini. Per fare ciò occorre semplicemente dividere ogni componente della matrice dei coefficienti delle frequenze per una costante fissata, e quindi arrotondare 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 elimina definitivamente i valori reali.

Per proseguire l'esempio finora descritto consideriamo la tabella di quantizzazione definita dallo standard JPEG per i coefficienti DCT della luminanza:

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	12	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

I coefficienti quantizzati sono ottenuti mediante le seguente formula:

$$B_{j,k} = \text{round} \left(\frac{G_{j,k}}{Q_{j,k}} \right) \text{ per } j = 0, \dots, 7; k = 0, \dots, 7.$$

dove G è la matrice dei coefficienti non quantizzati; Q è la tabella di quantizzazione e B è la matrice di valori quantizzati.

Ritornando all'esempio otteniamo la seguente matrice di valori quantizzati:

$$\begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -4 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

In effetti se consideriamo -415 (il coefficiente DC) ed applichiamo la quantizzazione otteniamo:

$$\text{round}\left(\frac{-415}{16}\right) = \text{round}(-25.9375) = -26$$

si noti come i coefficienti nulli siano definitivamente persi.

Compressione dei Dati

L'ultimo passo della codifica JPEG è la compressione dei dati. La codifica entropica è una particolare forma di compressione lossless (senza perdita di dati). I coefficienti quantizzati vengono ordinati in modalità "zigzag", raggruppando, allo stesso livello, frequenze dello stesso tipo; quindi gli zeri finali sono rimossi e i rimanenti dati sono compressi mediante l'algoritmo di compressione Huffman.

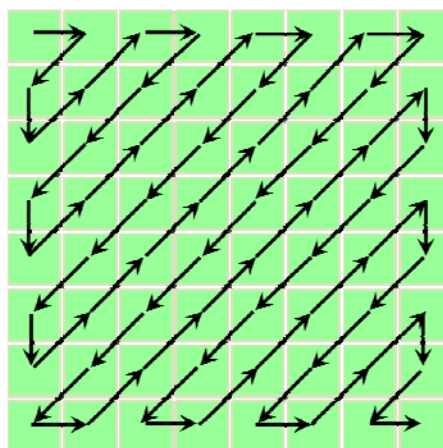


Figura 6 – Modalità a "zigzag"

Nell'esempio considerato, seguendo l'andamento a "zigzag" descritto nella figura, otteniamo la sequenza di dati:

-26							
-3	0						
-3	-2	-6					
2	-4	1	-4				
1	1	5	1	2			
-1	1	-1	2	0	0		
0	0	0	-1	-1	0	0	
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	
0	0	0	0	0	0		
0	0	0	0	0			
0	0	0	0				
0	0	0					
0	0						
0							
0							

Utilizzando il carattere speciale di fine blocco (EOB), per eliminare gli zeri finali, la sequenza diventa:

-26						
-3	0					
-3	-2	-6				
2	-4	1	-4			
1	1	5	1	2		
-1	1	-1	2	0	0	
0	0	0	-1	-1	EOB	

Una volta fissata la fine del blocco si utilizza l'algoritmo di Run Length Encoding (RLE). RLE cerca nei dati da comprimere una serie di elementi uguali, e la sostituisce con un solo elemento, quindi un carattere speciale e infine il numero di volte che esso va ripetuto.

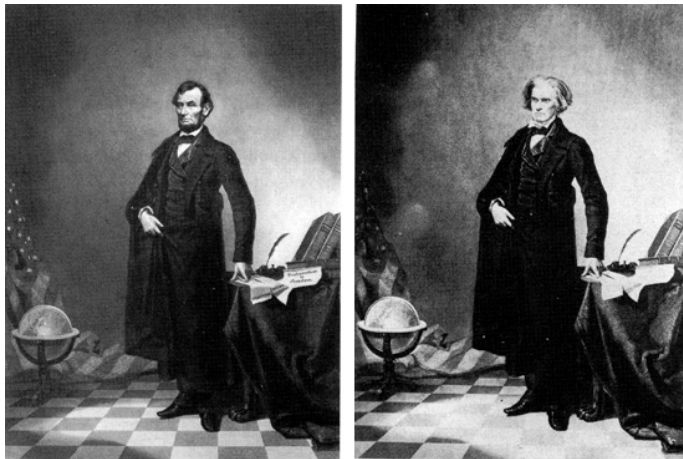
Finalmente la stringa risultante è analizzata mediante l'algoritmo di compressione Huffman e sfruttando l'entropia del sistema comprime finalmente i dati.

Decompressione dei Dati

Il processo di decompressione consiste semplicemente nel ripetere tutti i passi in ordine inverso. È chiaro che poiché la compressione è stata applicata con perdita di dati, l'immagine risultante sarà diversa dall'immagine originale. Ripetere il processo di compressione/decompressione due, o più, volte implica un deterioramento continuo dell'immagine. Infatti l'individuazione della doppia compressione è spesso utilizzata al fine di accertare l'alterazione di un'immagine (come vedremo più avanti).

Contraffazioni: casi famosi e non

La fotografia ha perso la sua innocenza sin dagli albori della sua nascita. In effetti già nel 1860, solo pochi decenni dopo che Niépce creò la prima fotografia, era il 1826, vennero individuate fotografie manipolate. Con l'avvento delle fotocamere digitali, videocamere e sofisticati software di editing fotografico, la manipolazione di immagini digitali sta diventando sempre più comune. Di seguito sono descritti alcuni dei più noti casi di manomissione [7].



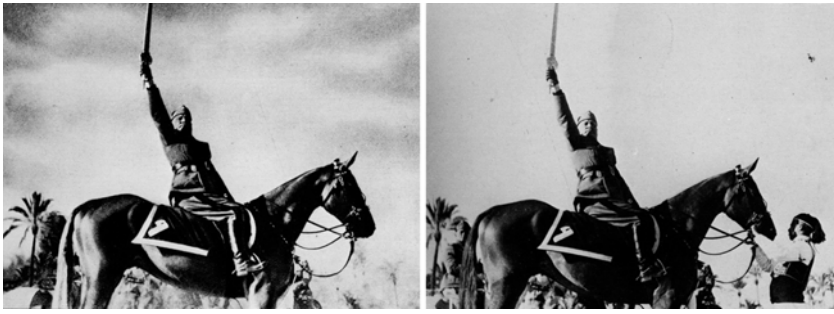
1860 circa: Questo ritratto del presidente americano Abraham Lincoln è una composizione della testa di Lincoln e del corpo del politico sudista John Calhoun. Occorre considerare che l'immagine è nota come la prima contraffazione fotografica, inoltre la Eastman Dry Plate Company (più tardi Eastman Kodak) è stata fondata nel 1881.

1930 circa: Stalin ricorreva abitualmente all'aerografo al fine di rimuovere i suoi nemici dalle fotografie. In questa fotografia un commissario venne rimosso dal documento originale.



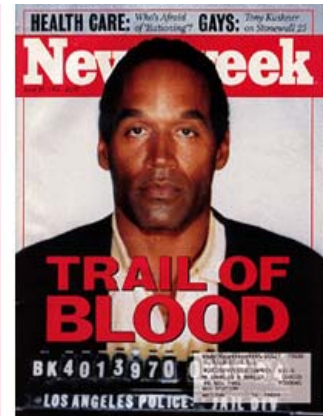
1937: Nella seguente fotografia Adolf Hitler fece rimuovere Joseph Goebbels (il secondo a destra).





1942: Benito Mussolini fece rimuovere dalla illustrazione originale il soldato che domava il suo cavallo, al fine di rendere più epica la scena che lo ritraeva.

Giugno 1994: Questa fotografia alterata di OJ Simpson venne pubblicata sulla copertina della rivista Time Magazine, subito dopo il suo arresto per omicidio. In effetti la fotografia risultò alterata rispetto all'immagine originale che comparve sulla copertina della rivista Newsweek. La rivista Time venne accusata di aver manipolato la fotografia al fine di rendere la figura di Simpson più scura e minacciosa.



Novembre 1997: Dopo l'uccisione di 58 turisti durante un attacco terroristico presso il tempio di Hatshepsut a Luxor (Egitto), il tabloid svizzero Blick alterò digitalmente una pozzanghera d'acqua trasformandola in una più lugubre scia di sangue.



Settembre 2000: Sperando di rendere più politically-correct le sue iscrizioni, l'università del Wisconsin falsificò la copertina della brochure inserendo uno studente nero in mezzo ad una folla di tifosi della squadra di football. La fotografia originale fu in realtà scattata nel 1993. Lo studente aggiunto, un certo Diallo Shabazz, fu invece fotografato nel 1994. I dirigenti dell'università si giustificavano dichiarando di aver speso l'intera estate alla ricerca di un'immagine che dimostrasse l'equità dell'accademia, ma senza successo.



Aprile 2003: Questa composizione di un soldato Inglese a Basra, che gesticola verso un civile iracheno indicandogli di restare coperto, è apparsa sulla copertina del Los Angeles Times, subito dopo l'invasione dell'Iraq. Brian Walski, un fotografo dello staff del Los Angeles Times e un veterano della notizia con trenta anni di esperienza alle spalle, è stato licenziato in tronco dal suo editore per aver fuso due dei suoi scatti al fine di migliorare la composizione.



Febbraio 2004: Durante la campagna per le primarie presidenziali emerse questo fotomontaggio composto dal senator John Kerry e dall'attrice Jane Fonda che sembravano condividere lo stesso palco ad una manifestazione anti-guerra. In realtà l'immagine del senatore Kerry fu scattata dal fotografo Ken Light mentre Kerry si stava preparando a pronunciare un discorso al "Register for Peace Rally" svoltosi a Mineola, New York, nel giugno del 1971; mentre Jane Fonda fu fotografata da Owen Franken mentre parlava ad una manifestazione politica a Miami Beach, Florida, nel agosto 1972.

Fonda Speaks To Vietnam Veterans At Anti-War Rally



Marzo 2004: Quest'immagine, tratta dal promo distribuito per la campagna elettorale di George W. Bush, illustrava una gremita platea di soldati come sfondo ad un bambino che sventolava la bandiera americana. Questa immagine è stata digitalmente truccata, mediante un grossolano copia ed incolla, rimuovendo Bush dal podio. Dopo aver ammesso la manomissione lo staff di Bush rieditò e rispedì alle stazioni televisive il promo con la foto originale.



Agosto 2006: Questa immagine di Adnan Hajj, un fotografo libanese, illustrava uno spesso strato di fumo nero che si ergeva dal centro della capitale libanese poco dopo un raid aereo israeliano. L'agenzia Reuters pubblicò, inizialmente, la fotografia sul proprio sito, per ritirarla appena risultò evidente che l'originale fosse stata contraffatta per mostrare un fumo più nero e denso. "Hajj nega di aver contraffatto deliberatamente l'immagine, dicendo che il suo intento era quello di rimuovere polvere dalla foto e che per via delle scarse condizioni di luminosità in cui si è trovato ad operare non si è accorto dell'errore", fu la dichiarazione del capo delle relazioni pubbliche della Reuters.



Agosto 2007: La rivista francese *Paris Match* manomise questa fotografia del presidente Nicolas Sarkozy rimuovendo dal suo fianco una lieve protuberanza. Il magazine dichiarò di aver solamente tentato di correggere la luminosità dell'immagine, concludendo che "La correzione è stata sicuramente amplificata dal processo di stampa".



Gennaio 2008: Il giornale taiwanese *Liberty Times* pubblica la seguente fotografia di una delegazione, guidata dal presidente della Franz Collection, al cospetto del Papa. Nello scatto originale Wang Shaw-lan, il direttore di una testata avversaria, la *United Daily News*, risultava presente. Il *Liberty Times* dichiarò che fu la Franz Collection a fornire lo scatto già contraffatto, mentre la Franz Collection replicò che la manomissione fu direttamente richiesta dalla testata giornalistica.



Luglio 2008: Questa immagine di un test missilistico iraniano apparve sulla copertina di diversi importanti giornali. L'immagine proveniva dal sito web della *Sepah News*, il braccio mediatico della Guardia Rivoluzionaria Iraniana. Dopo la pubblicazione di questa foto fu scoperto che il secondo missile a destra fu digitalmente aggiunto, mediante copia e incolla, al fine di nascondere il fallimento del lancio di un missile dalla fotografia originale.



Luglio 2008: Questa foto del Principe William venne pubblicata sul tabloid *The Sun*. L'uomo al timone dell'imbarcazione fu rimosso (eccetto che per un ginocchio). Il concorrente *The Metro* replicò immediatamente pubblicando lo scatto originale.



Settembre 2008: Dopo aver pubblicato le foto di due soldati caduti in Iraq, la Associated Press le ritirò, poiché fu scoperto che una delle due era stata contraffatta. In effetti venne sovrapposta la testa del soldato nero sul corpo del second soldato. Le due fotografie furono effettivamente rilasciate dalla U.S. Army presso Fort Stewart in Georgia.



Tecniche avanzate di Identificazione di Contraffazioni

Quanto visto finora rappresenta solo una piccola parte delle manomissioni di immagini digitali relativamente a casi famosi saliti alla ribalta in quanto banalmente e manualmente scoperti. Ai giorni nostri le immagini digitali possono essere molto più facilmente manomesse. Infatti, creare, manipolare e alterare immagini digitali, senza lasciare tracce, è piuttosto semplice se si utilizzano gli strumenti giusti.

Prima di proseguire con la descrizione di tecniche per l'individuazione di contraffazioni occorre chiarire il significato stesso di "manomissione di un'immagine".

La manomissione può essere intesa in differenti modi:

1. Alterazione dell'immagine per fini personali, per esempio sostituendo un cielo grigio con un cielo azzurro, oppure aggiungendo dei fiori, oppure ancora inserendo degli effetti artistici.
2. Alterazione dell'immagine a fine di lucro o per acquisire fama, come per esempio è stato fatto da qualche fotografo freelance per rendere più appetibile uno scatto.

Principalmente le contraffazioni possono essere classificate in tre categorie:

- a. Elaborazione dell'immagine mediante applicazioni di computer grafica.
- b. Alterazione del significato dell'immagine, senza modificarne il contenuto.
- c. Alterazione del contenuto dell'immagine, inserendo o nascondendo parti significative.

Nel vecchio mondo della fotografia analogica, un'immagine era, in genere, considerata una prova d'evidenza attendibile. Allo stato attuale non esistono tecniche automatiche "perfette" che permettono l'esatta individuazione di manomissioni delle immagini digitali. Per questo motivo le fotografie digitali non sono, in genere, attendibili ai fini di prove d'evidenza, se non con i dovuti accorgimenti "formali" e "procedurali". Obiettivo della ricerca scientifica in questo settore è quello di individuare tecniche automatiche o quantomeno semi-automatiche in grado di scovare opportunamente tali problemi.

Alcune tecniche di watermarking digitale sono state introdotte al fine di inserire una firma nell'immagine direttamente all'atto dello scatto della macchina fotografica. Il problema di questo tipo di approccio è legato alla difficoltà di inserire tale firma in modo univoco in tutti i dispositivi esistenti e mediante uno

standard noto a tutti. Esistono poi diversi approcci detti passivi che cercano di operare in assenza di una firma identificativa. Queste tecniche si basano sul concetto che, anche se le contraffazioni dovessero essere significativamente dissimulate, in ogni modo queste alterano il contenuto statistico dell'immagine stessa.

I metodi di Digital Forensics possono essere raggruppati come di seguito indicato:

1. Tecniche pixel-based: che individuano anomalie statistiche a livello di pixel.
2. Tecniche format-based: che fanno leva sulle correlazioni statistiche contenute nelle tecniche di compressioni lossy (con perdita di dati).
3. Tecniche camera-based: che sfruttano gli artefatti introdotti dalla lente, dal sensore o dalla pipeline della macchina fotografica.
4. Tecniche physically-based: che generano un modello specifico delle anomalie mediante un'interazione nello spazio 3D degli oggetti, delle fonti di luce e del sensore della fotocamera.
5. Tecniche geometric-based: che confrontano misure fisiche degli oggetti reali e delle loro posizioni rispetto alla fotocamera.

Di seguito saranno descritte alcune, tra quelle più note, delle tecniche sopracitate.

Pixel-based:

Di seguito sono descritte diverse metodologie che sfruttano le correlazioni a livello di pixel al fine di individuare eventuali contraffazioni.

Copia e Incolla (Cut & Paste)

La più elementare delle manomissioni, al fine di eliminare oggetti o persone all'interno di un'immagine, consiste nel clonare intere regioni della stessa immagine, mediante operazioni di copia e incolla. Quando questa operazione è effettuata con una certa meticolosità, può essere veramente arduo identificare visualmente la zona alterata. Inoltre potrebbe risultare proibitivo, da un punto di vista computazionale, individuare tali zone, poiché le aree clonate possono essere di qualsiasi dimensione e/o forma all'interno dell'immagine. A tale riguardo sono da segnalare due approcci significativi [8] e [9].

Gli autori di [8] applicano inizialmente una trasformata Discreta del Coseno (DCT) a blocchi, quindi effettuando un'analisi lessicografica, e ordinando i

blocchi DCT, individuano i blocchi duplicati (che risulteranno essere vicini nell'ordinamento applicato). In un approccio simile [9], effettuando un'analisi delle componenti principali (PCA) su blocchi di pixel, gli stessi autori ricorrono ad un'analoga analisi lessicografica, ordinando i gruppi di blocchi stimati mediante la PCA. Sia la DCT che la PCA sono utilizzate per semplificare i calcoli da effettuare per l'individuazione delle zone simili, e per rendere gli approcci più robusti alle variazioni introdotte da eventuali compressioni e/o inserimento di rumore.

Ricampionamento

Al fine di generare una contraffazione convincente, molto spesso si ricorre ad operazioni di ridimensionamento, rotazioni, oppure deformazioni di porzioni di immagini. Per esempio quando si crea un fotomontaggio con due persone, una delle due deve essere manipolata per raggiungere dimensioni compatibili con la risoluzione dell'altra. Questo procedimento richiede di ricampionare l'immagine di partenza in una nuova griglia di destinazione, generando in questo modo delle correlazioni periodiche nei dintorni dei pixel manomessi. La presenza di queste correlazioni, normalmente inesistenti, è utilizzata per individuare questo tipo di manomissione [10].

Fusione

Un altro metodo, di uso comune, per la manipolazione delle immagini è la fusione di due o più scatti. Quando è fatta a dovere, la zona di divisione tra le due immagini è difficilmente individuabile. Un esempio di fusione di immagini è dato dalla creazione di immagini in formato Panorama, ottenute mediante la fusione di diversi scatti di un paesaggio (di solito) al fine di ottenere una vista d'insieme più ampia. In [11] e [12] gli autori hanno dimostrato che la fusione altera le statistiche di ordine superiore della trasformata di Fourier, che possono evidentemente essere usate per l'individuazione di tali artefatti.

Statistica

Ci sono $256^{n \times n}$ possibile immagini a scale di grigio di dimensioni $n \times n$. Supponendo di fissare $n=10$, abbiamo 10^{240} possibili immagini (più del numero stimato di atomi presenti dell'universo). Analizzando nel dettaglio questo sterminato insieme di immagini è evidente che non saranno tutte immagini significative. Questa osservazione porta alla conclusione che esiste sicuramente qualche proprietà statistica che permette di razionalizzare le fotografie. Gli autori di [13], [14] e [15] sfruttano le regolarità statistiche delle scene naturali al fine di individuare eventuali manomissioni.

Format-based:

La prima regola fondamentale dell'indagine forense è ovviamente quella della conservazione dei dati originali. Per questo motivo la compressione lossy delle immagini JPEG può essere considerata il peggior nemico dell'analista forense. Il caso vuole che proprio questa caratteristica, di "perdita dei dati", sia utilizzata come ottimo strumento per l'individuazione delle manomissioni.

Quantizzazione JPEG

La maggior parte delle macchine fotografiche digitali memorizzano gli scatti in formato JPEG. Questo schema di compressione lossy permette di stabilire, in qualche modo, un grado di compressione dei dati. Di solito, sono i produttori di fotocamere a stabilire i differenti gradi di compressione selezionabili, in funzione a statistiche che bilanciano qualità e dimensioni finali dei files. Come descritto in [16] e [17], queste differenze, tra produttori, possono essere utilizzate per identificare la sorgente (Modello di fotocamera, produttore) di un'immagine.

Attraverso le tabelle di quantizzazione si modifica il fattore di compressione dell'immagine. Per livelli di compressione minimi, i valori delle tabelle di quantizzazione tendono ad 1 mentre crescono man mano che si tende a raggiungere fattori di compressione più elevati. La sorgente principale di variazione, rispetto alla codifica JPEG, dei vari produttori è quindi attribuita alla scelta delle tabelle di quantizzazione (quando queste differiscono dalle tabelle dello standard). Le tabelle di quantizzazione possono essere semplicemente estratte dai metadati delle immagini oppure stimate mediante analisi dell'immagine [18]. Occorre precisare che le tabelle di quantizzazione possono variare anche per singola fotocamera, in funzione di un fattore di qualità; inoltre non è inusuale riscontrare diversi produttori con simili tabelle di quantizzazione. In ogni modo questa semplice analisi può essere significativa in caso di balistica dell'immagine digitale, per un'eventuale conferma della sorgente dell'immagine.

Doppia Quantizzazione

Qualunque sia il tipo di manomissione, all'interno di un'immagine, questa sarà eseguita tramite un software di fotoritocco e l'immagine nuovamente salvata. Poiché la maggior parte delle immagini è compressa mediante codifica JPEG, è molto probabile che sia l'immagine originale, che quella contraffatta siano state salvate usando questo formato. In questo scenario l'immagine contraffatta sarà quindi compressa due volte. Per via della natura lossy dell'algoritmo JPEG,

la doppia compressione introduce artefatti specifici, altrimenti assenti nelle immagini in singola compressione. La presenza di questi artefatti, in alcuni casi, è utilizzata per dimostrare un'eventuale manomissione. Occorre, comunque, considerare che certe manomissioni non sono necessariamente commesse con intenti ingannevoli, ma ad ogni modo la doppia compressione implica la non autenticità di uno scatto digitale.

Blocking JPEG

Come descritto in precedenza, la base della codifica JPEG è il blocco di pixel 8x8. Per via della natura di questa decomposizione a blocchi, trasformati tramite DCT e quantizzati, la presenza di artefatti lungo i bordi non è inconsueta. Quando un'immagine viene manomessa questi artefatti, detti di blocking, possono essere scompigliati. In [19] gli autori caratterizzano il blocking utilizzando le differenze tra pixel contenuti dentro e sui bordi dei blocchi. Queste differenze tendono ad essere piccole nei singoli blocchi ed elevate tra blocchi adiacenti. Quando un'immagine è ritagliata e ricompressa, nuovi artefatti di blocking possono essere introdotti, e non necessariamente allineati agli originali.

Camera-based:

Le scanalature impresse dalle canne delle pistole sui proiettili collegano, con un certo grado di confidenza, una pallottola ad una ben determinata pistola. Sfruttando la stessa filosofia, sono state sviluppate molte tecniche di digital forensics che, basandosi su determinati artefatti introdotti dai vari stadi dell'elaborazione dell'immagine all'interno delle fotocamere, determinano un collegamento univoco tra fotocamera e immagine. Di seguito verranno descritte alcune delle tecniche atte ad individuare e modellare artefatti dovuti alla fotocamera.

Aberrazione Cromatica

In un sistema ideale, la luce entra nella fotocamera e, attraverso la lente, colpisce il sensore di acquisizione in un solo punto. I sistemi ottici reali, purtroppo, si scostano da questo modello ideale poiché riescono difficilmente a focalizzare la luce da tutte le possibili lunghezze d'onda. Nello specifico, le aberrazioni cromatiche laterali si manifestano in una traslazione dei colori laddove la luce, a differenti lunghezze d'onda, colpisce il sensore della macchina digitale. In [20], gli autori evidenziano il fatto che le aberrazioni laterali possono essere approssimate sfruttando espansioni e contrazioni di un

piano di colore in corrispondenza agli altri. Utilizzando questa tecnica è possibile rilevare zone di inconsistenza cromatica all'interno dell'immagine. Per esempio incollando un ritaglio da un'altra immagine, le eventuali aberrazioni presenti (oppure assenti) nelle parti incollate risulteranno in contrasto con il resto dell'immagine.

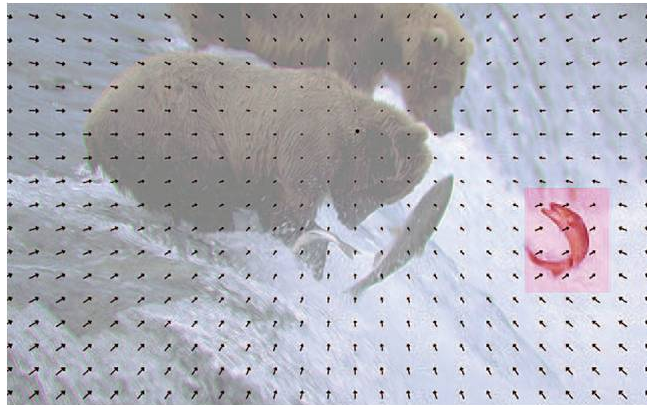


Figura 7 - Esempio di incongruenza nella mappa di difettosità cromatica (il pesce evidenziato in rosso è stato aggiunto in un secondo tempo)

CFA Color Filter Array

Com'è noto un'immagine è composta da tre canali di colore, campionati a partire da tre bande differenti dello spettro del colore: Rosso, Verde e Blu. La maggior parte delle macchine fotografiche è invece equipaggiata con un singolo sensore che cattura le immagini attraverso un Color Filter Array (un filtro a griglia dei colori). La pluralità dei filtri CFA è composta da una griglia che alterna i tre colori Rosso, Verde e Blu, posizionata direttamente sul sensore. Poiché, con questo sistema, è possibile catturare solo un canale per pixel, per ottenere un'immagine a colore occorre ricostruire le due componenti mancanti per ogni singolo pixel. Questo procedimento prende il nome di Color Interpolation ovvero Demosaicing [21].

Trascurando la metodologia utilizzata al fine di ricreare i tre piani di colore, l'interpolazione, in genere, introduce specifiche correlazioni statistiche tra sottoinsiemi di pixel, in ognuno dei tre canali. Poiché il filtro CFA è una griglia con una tessitura periodica, queste correlazioni avranno un andamento periodico. In definitiva sfruttando questa periodicità è possibile individuare un tipo di firma digitale associata all'interpolazione del colore.

In [22] gli autori descrivono una tecnica per individuare sia la forma della correlazione che i pixel coerenti con tale forma.

Risposta della Camera

Poiché molti dei sensori delle macchine fotografiche digitali hanno una risposta quasi lineare, dovrebbe esistere una qualche relazione lineare tra la quantità di luce misurata dai sensori e i valori finali assegnati ai pixel. La maggioranza, comunque, applica una risposta non lineare per punto, al fine di migliorare la qualità finale dell'immagine. Gli autori in [23] descrivono una tecnica per stimare questa traccia, definendo un funzione di risposta a partire da una singola immagine. Le differenze rilevate nella funzione di risposta stimata permettono di individuare eventuali manomissioni contenute all'interno delle immagini così analizzate.

Rumore del Sensore

Durante tutto il processo di acquisizione ed elaborazione, l'immagine può essere affetta da rumore o imperfezioni di diversa natura. Sia per via di fattori esterni, come temperatura ambiente, umidità, che per via di tipici difetti di fabbrica (fixed pattern noise, ecc). Il rumore nelle immagini digitali si evidenzia in prevalenza nelle aree uniformi, o in aree scure con poco dettaglio. Vedremo più avanti maggiori dettagli riguardo questo argomento, utilizzato soprattutto per l'identificazione della sorgente. Tra i vari lavori noti in letteratura vogliamo citare l'approccio proposto da [24]. In questo articolo, gli autori generano un modello additivo e moltiplicativo del rumore a partire dal processo di generazione dell'immagine effettuato dalla camera. I parametri del modello di rumore sono stimati direttamente a partire dalla fotocamera, oppure utilizzando una serie di immagini generate dalla fotocamera. Sfruttando questo modello è possibile evidenziare un'eventuale anomalia contenuta all'interno di un'immagine.

Physically Based

Consideriamo il caso di un fotomontaggio contenente due persone affiancate estratte, precedentemente, da due contesti diversi. Al fine di ottenere un buon risultato occorre fare coincidere anche la direzione della luce, ovvero dell'illuminante, dei due personaggi.

Di seguito sono descritte tre tecniche che permettono di stimare diverse proprietà delle condizioni di luce della scena e degli oggetti fotografati. La presenza di imperfezioni, o incoerenze, delle illuminanti possono quindi risultare utile al fine di evidenziare contraffazioni.

Direzione della Luce (2D)

Poiché la parte destra della faccia, in Figura 8, è visibilmente più illuminata di quella sinistra, è chiaramente deducibile che la sorgente della luce è individuabile a destra del soggetto. Questa osservazione si formalizza mediante semplici assunzioni: la quantità di luce incidente ad una superficie è

proporzionale alla normale sul piano e alla direzione della luce. Sfruttando tecniche 3D per la stima in funzione della normale al piano, la direzione della luce è quindi stimabile [25]. La difficoltà di individuare superficie 3D a partire da una singola immagine ha portato gli autori dell'articolo [26] a considerare unicamente normali alle superficie 2D degli oggetti contenuti nelle immagini. Conseguentemente è possibile individuare unicamente due delle tre componenti necessarie per individuare la sorgente di luce. Malgrado rimanga un certo grado di possibile ambiguità l'approssimazione risulta comunque utile in ambito forense.

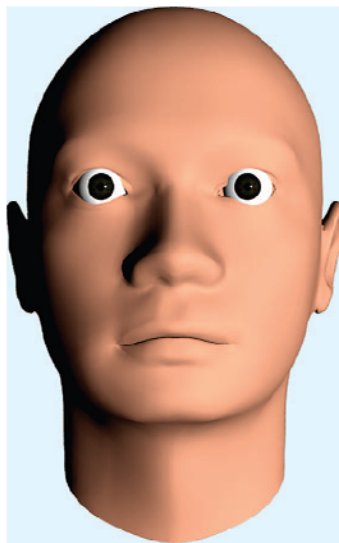


Figura 8 – Individuazione della sorgente di luce

Direzione della Luce (3D)

Nel paragrafo precedente si stimava la direzione della luce, in 2D, a partire da una sola immagine, in [27] gli autori descrivono come stimare la direzione della luce a partire dal *glint* (riflesso) presente sulla superficie dell'occhio. In tale caso la superficie 3D necessaria ad una corretta stima della sorgente è ricavata mediante simulazione del modello sferico dell'occhio umano.

Luce ambientale

Nei due punti precedenti, in effetti, è stato trascurato uno dei principali fattori di inquinamento della sorgente diretta di luce, ovvero la luce ambientale. In pratica le scene illuminate possono contenere differenti fonti di luce, aumentando in questo modo la complessità della stima delle varie posizioni. Gli autori di [28] descrivono un tecnica, basata su superficie Lambertiane, per stimare sistemi complessi di questo tipo.

Geometric Based

Punto principale

Nelle immagini reali il punto principale (la proiezione del centro della fotocamera sul piano dell'immagine) è vicino al centro dell'immagine. Quando si sposta un oggetto oppure una persona nell'immagine, il punto principale è spostato proporzionalmente. La differenza tra il punto principale stimato e quello effettivo può quindi essere utilizzato al fine di individuare una eventuale manomissione della fotografia. In [29] gli autori descrivono una tecnica per stimare il punto principale a partire da una coppia di occhi oppure mediante l'utilizzo di altre metriche geometriche planari.



Figura 9 – Estrazione della targa

Misure

In Figura 9 è visibile la fotografia di una macchina la cui targa è parzialmente illeggibile. Nel riquadro possiamo vedere come una trasformazione prospettica (accompagnata ad un ingrandimento) possa rendere visibili i caratteri alfanumerici altrimenti irriconoscibili. In [30] gli autori segnalano diversi tools che permettono l'utilizzo di trasformazioni geometriche proiettive nonché, in alcuni casi, di strumenti per la misurazione delle distanze reali a partire da fotografie.

Individuazione della Fotocamera mediante il Rumore

Con l'enorme diffusione di dispositivi in grado di acquisire ed elaborare immagini digitali, identificare in modo affidabile i sensori a partire da una immagine diventa sempre più una necessità. Questo è vero specialmente in ambito forense, per determinare l'origine di scatti presentati come prova in un'aula di tribunale. Metodi di identificazione, inoltre, potrebbero essere utili per dimostrare che alcune immagini sono state ottenute utilizzando una specifica fotocamera piuttosto che elaborate al PC tramite programmi ad hoc. Nei successivi paragrafi analizzeremo il problema dell'identificazione del sensore, tramite l'uso del rumore delle immagini che in un certo senso identifica univocamente la fonte di acquisizione .

Processo Di Generazione Dell'immagine Digitale

Diversamente da una macchina fotografica tradizionale, una fotocamera digitale utilizza, al posto della pellicola, un sensore costituito da milioni di elementi fotosensibili (*pixel*) in grado di catturare l'immagine e trasformarla in segnale elettrico di tipo analogico. Gli impulsi elettrici catturati dal sensore vengono quindi convertiti in digitale da un convertitore A/D nel chip di elaborazione e trasformati in un flusso di dati digitali atti ad essere immagazzinati in vari formati su supporti di memoria.

Prima che la luce della scena fotografata raggiunga il sensore, essa passa attraverso le lenti della fotocamera, un filtro di *antialiasing*, e poi attraverso il Color Filter Array (*CFA*). Il CFA è un mosaico di filtri colorati che consente ad ogni pixel di catturare informazioni riguardanti ciascuna delle tre componenti RGB (Red-Green-Blue) che compongono la luce della scena da acquisire: in questo modo ogni pixel può registrare le informazioni relative ad un solo specifico colore (Figura 10).

Per ricostruire il colore originale occorre calcolare le componenti primarie mancanti su ogni pixel usando algoritmi di interpolazione del colore (*demosaicing*). Il segnale risultante viene quindi ulteriormente elaborato tramite regolazione del bilanciamento del bianco, correzione gamma e vari altri metodi di correzione del colore.

Infine, l'immagine digitale è scritta sul dispositivo di memorizzazione della fotocamera nel formato selezionato dall'utente. Questo processo potrebbe richiedere una ulteriore elaborazione dell'immagine, come ad esempio la compressione JPEG.

Maggiori dettagli sul processo di acquisizione di un'immagine mediante un sensore digitale possono essere trovati in [21].

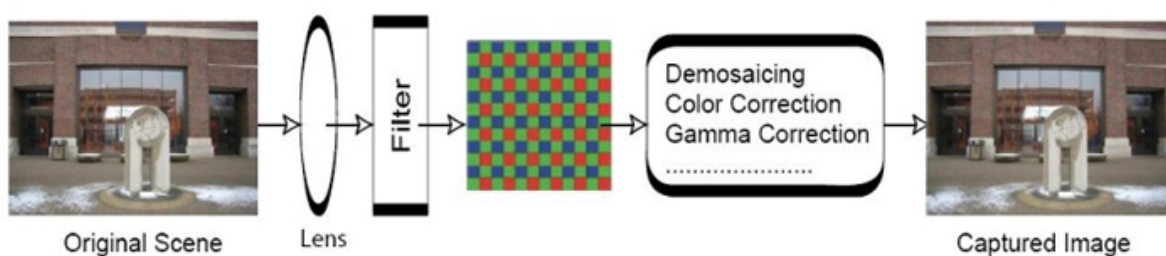


Figura 10 – Schema del processo di acquisizione di un'immagine.

Sorgenti Di Rumore

Durante tutto il processo di acquisizione ed elaborazione, l'immagine può essere affetta da rumore o imperfezioni di diversa natura.

Il rumore nelle immagini digitali si evidenzia in prevalenza come una certa granulosità o puntinatura monocromatica (luminance noise) e/o come puntini o macchioline colorate (chroma noise) evidenti soprattutto nelle aree uniformi come il cielo, o in aree scure con poco dettaglio. L'effetto è molto simile a quello delle immagini da pellicola ad alta sensibilità.

Il rumore che contamina le immagini digitali può essere di diverso tipo e avere varia natura. Analizziamo brevemente alcune delle principali fonti di rumore:

- Photon shot noise: è il rumore legato al principio di formazione dell'immagine, e si somma alle deformazioni ottiche e le aberrazioni cromatiche introdotte dalle lenti. Questo disturbo dipende dalla variabilità del numero di fotoni che raggiungono una certa zona del sensore per un dato tempo di esposizione, e provoca una incertezza nel valore dei pixel che segue una determinata statistica.
- Rumore termico: è il rumore generato dal surriscaldamento del sensore, che determina la formazione di cariche che si sommano a quelle generate dai fotoni, contribuendo all'aumento della granularità dell'immagine.
- Pattern noise: è un rumore spaziale che non varia in maniera significativa da immagine ad immagine, rimanendo pressoché costante su tutte le immagini acquisite con la stessa fotocamera. Il pattern noise si distingue in: defect pixel, fixed pattern noise (FPN) e photo-response non-uniformity (PRNU).
 - I pixel difettosi sono quelli che non registrano correttamente il livello di luce incidente. Possiamo distinguerli in "hot pixel", sempre bianchi, e "dead pixel", sempre neri. Questi difetti in genere sono compensati dalla fotocamera tramite appositi algoritmi di post-processing.

- Il fixed pattern noise (FPN) è un rumore additivo causato da correnti (*dark current*) che si spostano dal substrato del sensore verso i singoli pixel. Il *dark current* è funzione della dimensione del pixel, della densità di drogaggio del silicio, e da materiali estranei intrappolati nel sensore durante la fabbricazione. Questo tipo di rumore è intrinseco del sensore, pertanto risulta essere indipendente dall'intensità di luce incidente.
 - Il photo-response non-uniformity (PRNU) è determinato dalla differenza di sensibilità dei pixel dello stesso sensore, e dipende da differenze di dimensione, risposta spettrale, spessore del rivestimento, e altre imperfezioni create durante il processo di fabbricazione.
- Readout noise: è il rumore introdotto durante la lettura dei dati dal sensore. Questo è più visibile ad alte ISO, o quando l'immagine è eccessivamente illuminata.

Ulteriori fonti di rumore sono connesse con le operazioni di processing effettuate sul valore del pixel dopo l'acquisizione, come ad esempio le conversioni di colore, il demosaicing, e la compressione, la cui entità dipende molto dal modo in cui queste operazioni sono effettuate.

Identificazione della camera tramite pattern noise.

Quando il sensore acquisisce una scena, anche nelle migliori condizioni di illuminazione, l'immagine digitale mostrerà comunque piccole variazioni di intensità tra i singoli pixel, a causa delle numerose fonti di rumore che intervengono nel processo di formazione dell'immagine.

Come precedentemente accennato, il rumore è composto da una componente casuale che dipende dal photon shot noise, rumore termico, ecc., e una componente fissa, dovuta al pattern noise, che lascia una traccia pressoché identica su tutte le immagini acquisite con lo stesso sensore.

Il pattern noise si presta dunque ad essere usato per l'identificazione della fotocamera. In particolare, ogni fotocamera digitale possiede un sensore lievemente differente dalle altre dello stesso modello, per via di un "disturbo" univoco e riconoscibile, ciò permette di identificare il sensore a partire dalle immagini, sfruttando la stessa idea che ci consente di distinguere le tracce univoche lasciate dalle canne delle armi da fuoco sui proiettili.

Il disturbo generato nelle immagini è legato sia al sensore in sé, che alle minuzie nella costruzione e nell'assemblaggio di ogni dispositivo. Questo assicura una differenza tra singoli dispositivi sufficiente a rendere improbabile la presenza di due camere che generino il medesimo disturbo, proprio come avviene per le impronte digitali.

Procedura di identificazione.

Il *pattern noise* di una fotocamera può essere estrapolato sottraendo all'immagine originale una versione della stessa da cui è stato rimosso il rumore, con uno dei molti algoritmi presenti in letteratura.

Dalla media dei pattern noise di un certo numero di immagini catturate dalla stessa fotocamera è possibile estrarre il pattern di riferimento (*reference pattern*) che rappresenta l'impronta digitale o firma della fotocamera. (Figura 11)

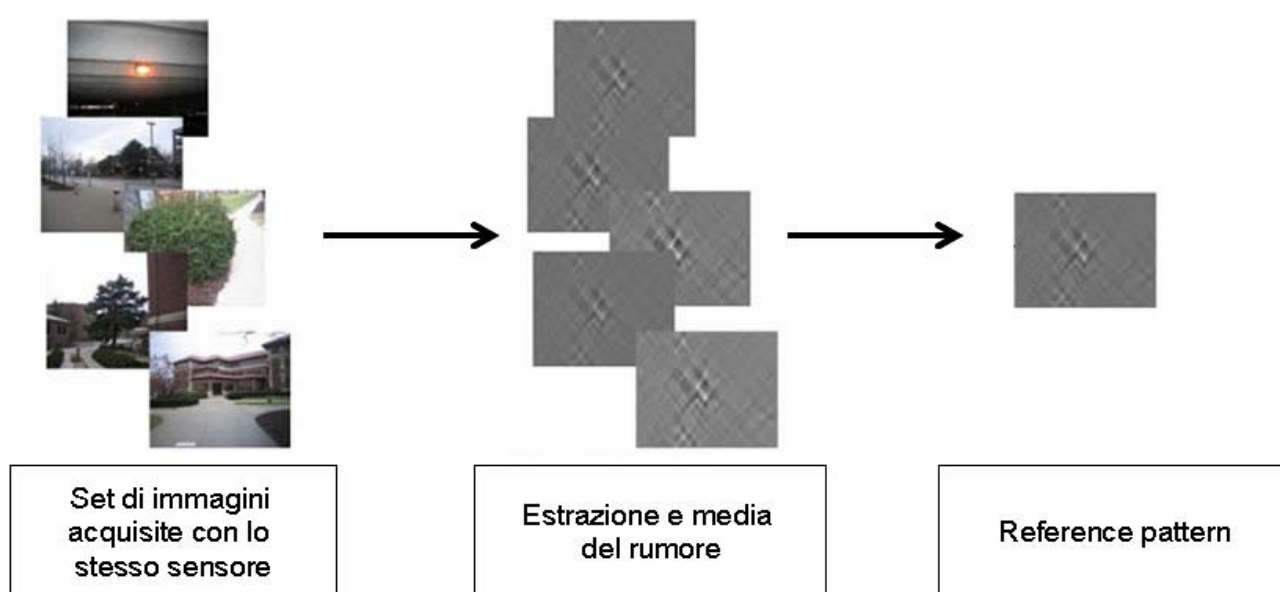


Figura 11 – Schema di estrazione del *reference pattern*.

La procedura di riconoscimento del sensore, data una qualsiasi immagine, consiste nell'estrazione del pattern noise e, attraverso un classificatore, nel riconoscimento del *reference pattern* che mostra una più alta correlazione col campione che stiamo analizzando. Ovviamente avere un buon numero di reference pattern rende il riconoscimento più facile ed affidabile (Figura 12).

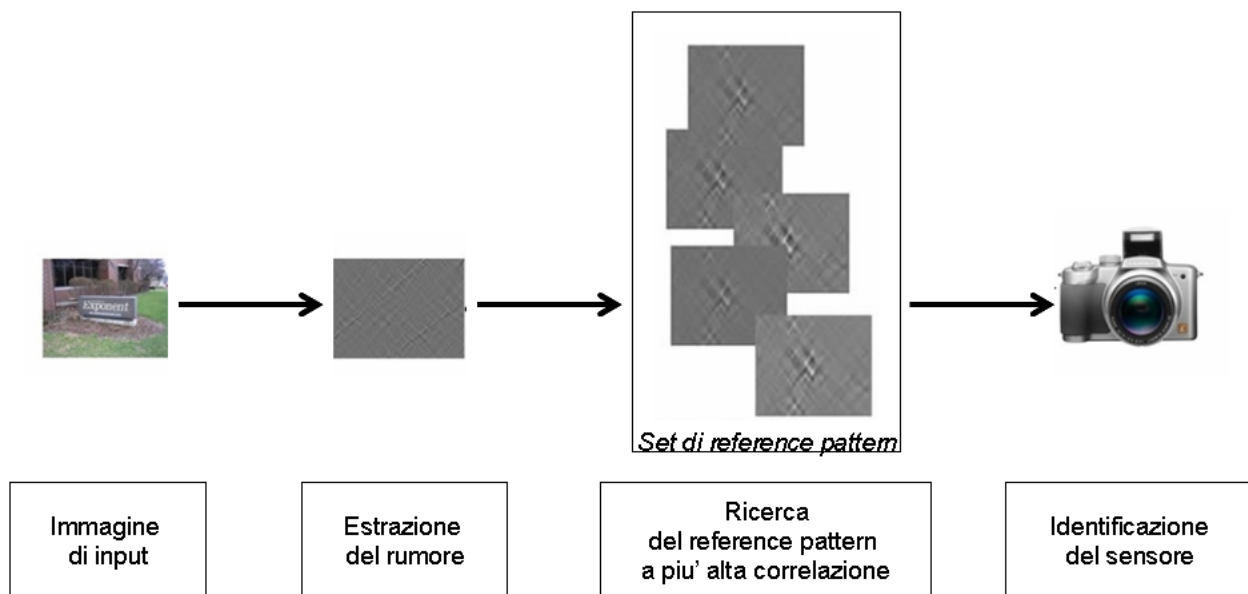


Figura 12 – Schema di riconoscimento del pattern.

La procedura appena descritta è la più semplice e nota. E' possibile leggere l'algoritmo nella sua forma estesa in [31].

Recentemente sono state proposte diverse migliorie e piccole varianti che rendono l'algoritmo di identificazione ancora più affidabile.

Alcuni autori hanno presentato delle tecniche attraverso le quali e' possibile migliorare la stima del reference pattern, che fanno uso di piccoli training set e utilizzano particolari procedure di classificazione.

In [32] e [33] sono descritti dei metodi di identificazione della fotocamera basata su stima e riconoscimento del PRNU dalle immagini. Una implementazione open source di questa tecnica è disponibile su <http://sourceforge.net/projects/prnucompare/>.

Operazioni di post-processing applicate ai reference pattern stimati, inoltre, possono ridurre la correlazione tra reference pattern di fotocamere della stessa marca e modello, riducendo quindi ulteriormente il numero di errori della procedura.

Evitare L'identificazione

Dato che le tecniche di identificazione del sensore sono tipicamente usate per analizzare prove in ambito giudiziario, è possibile pensare a possibili manomissioni destinate ad ingannare l'algoritmo di identificazione. Un malintenzionato potrebbe desiderare, infatti, non solo di rimuovere intenzionalmente il pattern noise per prevenire l'identificazione, ma anche di estrarre il rumore per copiarlo su un'altra immagine, per far credere che l'immagine sia stata acquisita con una fotocamera diversa.

Fortunatamente l'eliminazione del pattern noise, o la sovrapposizione dello stesso su un'immagine, sono operazioni abbastanza complesse, soprattutto per un non esperto. Se l'alterazione non è ben fatta, infatti, si potrebbe rischiare, di aggiungere artefatti che potrebbero far risaltare il tentativo di manomissione, e comunque di non riuscire ad ingannare l'algoritmo di identificazione.

D'altra parte, purtroppo, operazioni molto elementari sull'immagine, come un crop o una rotazione potrebbero rendere l'immagine irriconoscibile.

In rete, ad esempio, è possibile trovare siti come questo: <http://www.instructables.com/id/Avoiding-Camera-Noise-Signatures/> che spiegano come e cosa fare anche all'utente più sprovveduto.

Conclusioni

Le tecniche di Image Forensics costituiscono sicuramente un ulteriore strumento di indagine a disposizione degli investigatori per poter estrarre ed inferire, utili informazioni dalle immagini (e dai video) digitali. In questo documento ci si è soffermati sugli aspetti tecnici legati alla individuazione di manipolazioni (il cosiddetto "forgery") e all'identificazione della sorgente (camera) di acquisizione. Sono stati anche introdotti alcuni concetti di base, necessari per poter comprendere i dettagli tecnici degli algoritmi presentati.

Per essere in grado di recuperare o di inferire delle evidenze di prova è comunque necessaria una adeguata competenza specifica che richiede uno studio sistematico dei fondamenti della teoria dell'elaborazione delle immagini e dei video digitali. Gli stessi software oggi esistenti, che in qualche modo cercano di aiutare o quantomeno agevolare il lavoro degli investigatori, non riescono per forza di cose ad automatizzare in maniera sistematica ed efficiente tali operazioni e richiedono l'ausilio di utenti esperti.

Utili tools e Software

- Software opensource per l'analisi del segnale PRNU
<http://sourceforge.net/projects/prnucompare/>.
- AMPED Five (<http://ampedsoftware.com>)
- dTective di Avid e Ocean Systems ClearID
(<http://www.oceansystems.com/dtective/form/index.html>)
(<http://www.oceansystems.com/dtective/clearid/proposal/index.html>)
- Color Deconvolution (<http://www.4n6site.com>)
- LucisPro (<http://www.LucisPro.com>)
- Ikena Reveal di MotionDSP
(<http://www.motiondsp.com/products/IkenaReveal/form>)
- Video Focus di Salient Stills
(<http://www.salientstills.com/products/videofocus/purchase.html>)
- Impress di Imix (http://www.imix.nl/impress/impress_contact.htm)
- Video Investigator di Cognitech
(<http://www.cognitech.com/content/blogcategory/24/28/>)
- StarWitness di SignalScape (<http://www.starwitnessinfo.com/>)
- VideoAnalyst di Intergraph
(<http://www.intergraph.com/learnmore/cgi/public-safety/forensic-video-analysis.xml>)
- CrimeVision di Imagine Products (www.crimevision.net)

Bibliografia

- [1] Special Issue on Digital Forensics, Signal Processing Magazine, IEEE, Volume 26, Issue 2, March 2009;
- [2] G. Reis, "Analisi Forense con Photoshop", Apogeo - 2008 ISBN: 9788850327447
- [3] C. Baron, "Adobe Photoshop Forensics", Course Technology PTR, 2007, ISBN: 9781598634051;
- [4] The Lenna Story - www.lenna.org
- [5] R.C. Gonzalez, R.E. Woods, "Elaborazione delle Immagini Digitali" - Terza edizione - ISBN: 9788871925066 Pearson - Prentice Hall Italia, Ottobre 2008.
- [6] S. Battiato, F. Stanco - Fondamenti di Image Processing - ISBN: 8888659498 - EdiArgo 2006;
- [7] H. Farid, "Photo Tampering Throughout History",
<http://www.cs.dartmouth.edu/farid/research/digitaltampering/>
- [8] J. Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in Proc. Digital Forensic Research Workshop, Aug. 2003.

- [9] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
- [10] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 758–767, 2005.
- [11] H. Farid, "Detecting digital forgeries using bispectral analysis," AI Lab, Massachusetts Institute of Technology, Tech. Rep. AIM-1657, 1999.
- [12] T.-T. Ng and S.-F. Chang, "A model for image splicing," in Proc. IEEE Int. Conf. Image Processing, Singapore, 2004, vol. 2, pp. 1169–1172.
- [13] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection with binary similarity measures," in Proc. European Signal Processing Conf., Turkey, 2005.
- [14] H. Farid and S. Lyu, "Higher-order wavelet statistics and their application to digital forensics," in Proc. IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR), Madison, WI, 2003.
- [15] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Imaging, vol. 15, no. 4, p. 41102, 2006.
- [16] H. Farid, "Digital image ballistics from JPEG quantization," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006-583, 2006.
- [17] H. Farid, "Digital ballistics from jpeg quantization: A followup study," Dept. Comp. Sci., Dartmouth College, Tech. Rep. TR2008-638, 2008.
- [18] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," IEEE Trans. Image Process., vol. 12, no. 2, pp. 230–235, 2003.
- [19] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in Proc. IEEE Conf. Acoustics, Speech and Signal Processing, Honolulu, HI, 2007, pp. 217–220.
- [20] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006, pp. 48–55.
- [21] R. Lukac, "Single-sensor imaging in consumer digital cameras: a survey of recent advances and future directions". Journal Real-Time Image Processing 2006, Volume 1, pp.45–52.
- [22] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Trans. Signal Processing, vol. 53, no. 10, pp. 3948–3959, 2005.
- [23] Z. Lin, R. Wang, X. Tang, and H-V Shum, "Detecting doctored images using camera response normality and consistency," in Proc. Computer Vision and Pattern Recognition, San Diego, CA, 2005.
- [24] J. Fridrich, M. Chen, and M. Goljan, "Imaging sensor noise as digital x-ray for revealing forgeries," in Proc. 9th Int. Workshop on Information Hiding, Sant Malo, France, 2007, pp. 342–358.
- [25] P. Nilnius and J.-O. Eklundh, "Automatic estimation of the projected light source direction," in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2001, pp. 1076–1083.

- [26] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proc. ACM Multimedia and Security Workshop, New York, NY, 2005, pp. 1–10.
- [27] M. K. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye," in Proc. 9th Int. Workshop on Information Hiding, Saint Malo, France, 2007, pp. 311–325.
- [28] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inform. Forensics Security, vol. 3, no. 2, pp. 450–461, 2007.
- [29] M. K. Johnson and H. Farid, "Detecting photographic composites of people," in Proc. 6th Int. Workshop on Digital Watermarking, Guangzhou, China, 2007.
- [30] M. K. Johnson and H. Farid, "Metric measurements on a plane from a single image," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006-579, 2006.
- [31] J. Lukas, J. Fridrich, and M. Goljan, "Determining digital image origin using sensor imperfections," Proceedings of the SPIE International Conference on Image and Video Communications and Processing, A. Said and J. G. Apostolopoulos, Eds., vol. 5685, no. 1. SPIE, 2005, pp. 249–260.
- [32] M. Chen, J. Fridrich, and M. Goljan, "Digital imaging sensor identification (further study)," Proceedings of the SPIE International Conference on Security, steganography, and Watermarking of Multimedia Contents IX, E. J. D. III and P. W. Wong, Eds., vol. 6505, no. 1. SPIE, 2007.
- [33] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining Image Origin and Integrity Using Sensor Noise", IEEE Transactions on Information Forensics and Security , volume 3, no.1, pp.74-90, March 2008.
- [34] Z. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki and N. Saitoh, "Methods for Identification of Images Acquired with Digital Cameras" Proc. Of SPIE, Enabling Technologies for Law Enforcement and Security, vol. 4232, pp. 505–512, February 2001.
- [35] S. Bayram, H. T. Sencar, and N. Memon, "Improvements on source camera-model identification based on CFA interpolation" Proc. of WG 11.9 Int. Conf. on Digital Forensics, 2006.