ALMA MATER STUDIORUM - UNIVERSITA' DI BOLOGNA
CAMPUS DI CESENA
SCUOLA DI SCIENZE

CORSO DI LAUREA IN SCIENZE DELL'INFORMAZIONE

TITOLO DELLA RELAZIONE FINALE

Tecniche di rilevamento di alterazioni digitali di immagini

Relazione finale in
Basi di dati

Relatore
Prof.ssa Annalisa Franco

Presentata da
Laura Castellani

Sessione II Anno Accademico 2014/2015

a mia Mamma
medagliere nelle mie vittorie,
fazzoletto nelle mie sconfitte.

Indice

1. Introduzione

Il progresso nelle tecnologie digitali ha fatto nascere degli strumenti sempre più sofisticati e low-cost che fanno parte integrante del processo di informazione. Questo trend ha portato con sé dei cambiamenti rispetto all'integrità e all'autenticità dei documenti digitali, in particolare delle immagini. Dal momento che oggigiorno sono disponibili ad un pubblico sempre più vasto potenti tecnologie per generare e processare le immagini digitali, è necessario un concomitante sviluppo di tecnologie in grado di distinguere le immagini originali da quelle alterate.

Ciò si rende particolarmente necessario in ambito forense;spesso le immagini vengono utilizzate come prova legale e risulta quindi vitale avere degli strumenti in grado di riconoscere l'autenticità della prova.

Le possibili manipolazioni che si possono effettuare su di una immagine sono molteplici, tra le più note si ricordano il copia-incolla di un'immagine in un'altra, il ridimensionamento e il cambiamento dell'aspetto di un'immagine attraverso sfocature piuttosto che modifica del grado di luminosità. Una manipolazione su cui focalizzeremo l'attenzione in questa tesi è il Morphing di immagine, che consente, dati due volti, di unirne i tratti per creare una terza immagine che ne includa le caratteristiche di entrambi.

Come verrà esposto nel Capitolo 2 questa tecnica può essere utilizzata da “malviventi” per richiedere documenti di identità che non identifichino la loro persona ma un'altra a cui non risultano precedenti penali o che non compaia in una check-list, ponendo gli accenti anche sulle conseguenze che si hanno in termini di sicurezza.

Il Capitolo 3 è stato dedicato interamente a questa tecnica, il Morphing, analizzando le fasi che consentono la realizzazione di questa manipolazione digitale.

Nel Capitolo 4 vengono descritti alcuni metodi utilizzati per modificare il contenuto informativo di una foto; l'ultimo paragrafo mostra un breve excursus sulle immagini contraffatte più famose della storia.

Per comprendere la difficoltà della ricerca e dello sviluppo di algoritmi in grado di individuare immagini morphed o photoshopped, nel Capitolo 5 sono stati presi in esame alcuni studi sull'argomento i cui risultati mostrano che vi sono casi in cui i sistemi di

riconoscimento falliscono.

Infine nel capitolo 6 viene fatta una panoramica dei principali software che si trovano online in grado di autenticare immagini digitali contraffatte.

2. Documenti di identità e alterazioni digitali di immagini

Questo studio trae origine da una problematica in termini di sicurezza nata negli ultimi anni in seguito al processo di digitalizzazione che ha coinvolto i documenti di viaggio introducendo la possibilità di riconoscere automaticamente i viaggiatori sulla base di caratteristiche biometriche.

E' necessaria innanzitutto una premessa per descrivere meglio lo scenario : nel 2002, con la risoluzione di Berlino, l'ICAO (International Civil Aviation Organization) ha indicato il volto come la caratteristica biometrica primaria per gli eMRTD (electronic Machine Readable Travel Documents); come caratteristiche biometriche aggiuntive gli stati membri possono adottare le impronte digitali e l'iride.

A seguito di questa operazione l'ISO (International Standard Organization) ha definito alcuni standard di qualità che la foto deve soddisfare per poter essere inserito in un eMRTD, creando quindi un elenco di linee guida molto dettagliato.

In generale, sono possibili due metodi per poter inserire la foto nel proprio passaporto al momento della richiesta all'ufficio dedicato: il primo, e più banale, è quello di effettuare la foto del proprio volto direttamente nell'ufficio di richiesta del documento che, salvo eccezioni, dovrebbe avere a disposizione una macchina fotografica di alta qualità in modo tale che la foto rispetti gli standard di qualità ISO; il secondo metodo è quello in cui il cittadino porta direttamente la propria fotografia stampata che viene poi scannerizzata e inserita nel chip del documento.

In quest'ultimo caso è evidente che saranno necessari dei controlli accurati sull'autenticità della fotografia e sulla corretta corrispondenza foto/soggetto richiedente.

E' infatti noto che i software di manipolazione di immagini digitali sono oggigiorno facilmente disponibili per qualsiasi tipologia di utente ed è quindi diventato molto semplice manomettere immagini e renderle disponibile ad altri.

Assicurare l'integrità delle immagini digitali è diventato negli ultimi decenni una questione molto importante e delicata.

Apriamo una breve parentesi per confrontare la moderna fotografia digitale con la fotografia tradizionale analogica.

La fotografia tradizionale è una scienza; la luce entra nella fotocamera attraverso le lenti e l'immagine che la camera vede viene fedelmente registrata in un negativo. Questo negativo viene quindi stampato in un'immagine reale. Anche se le immagini rappresentate nella foto sono tipicamente fedeli all'immagine vista dalla fotocamera, esistevano anche in questo campo trucchetti fotografici e distorsioni.

Diverse variabili infatti influiscono su come possa risultare una fotografia e tutte queste possono impercettibilmente o drasticamente cambiare la “storia” che quella foto racconta. Uno scatto da un angolo più basso, ad esempio, può rendere un soggetto umano più alto di quanto sia in realtà. Spotting, cropping, bilanciamento del colore, aggiustamenti di luminosità e contrasto, messa a fuoco e modifica del tempo di esposizione sono metodi molto comuni per manipolare una fotografia. In ogni caso, finora, le fotografie analogiche hanno mantenuto la loro integrità poiché le alterazioni e le manipolazioni di una stampa analogica sono sempre stati facili da rilevare;ci basta pensare alla ricerca di diversi tipi di densità, alle linee di corrispondenza delle ombre o alla continuità dell'immagine per capire come diventa semplice smascherare una fotografia analogica contraffatta.

Ma la fotografia digitale è la nuova tecnica che ci permette di catturare immagini e le macchine digitali, a differenza delle sue corrispondenti analogiche, non memorizzano l'informazione in un mezzo continuo. L'informazione, invece, viene registrata in codice binario. Utilizzando quindi una serie di numeri, al posto di creste e depressioni continue caratteristiche dell'informazione analogica, la manipolazione di immagini digitali è più facile, economica e infinitamente più difficile da individuare rispetto all'alterazione analogica.

Abbiamo quindi capito come sia divenuto facile applicare delle alterazioni ad una fotografia, non tutte però vengono fatte con l'intento criminale di raggirare un sistema automatico di riconoscimento, alcune vengono fatte in modo non

intenzionale da strumenti di modifica, ad esempio, per rendere più bella una persona, migliorandone alcuni difetti estetici. In ogni caso in alcuni studi[4] che abbiamo preso in considerazione è stato dimostrato che gli algoritmi attuali di riconoscimento facciale sono in grado di scoprire un numero limitato di di alterazioni e che alcune di queste possono causare diversi problemi nel caso preso in considerazione ovvero di un sistema di riconoscimento automatico, come quello presente in alcune tipologie di varchi aeroportuali.

Sono infatti ormai presenti ormai nella maggior parte degli aeroporti i sistemi di Automatic Border Control (ABC), varchi non supervisionati che possono essere attraversati da alcune tipologie di viaggiatori con verifica automatica di identità;alcuni studi hanno mostrato che, in presenza di alterazioni delle immagini, i sistemi non sono in grado di riconoscere il proprietario dell' eMRTD così da rendere necessario l'intervento di un operatore umano.

Lo studio preso in esame in questo lavoro di tesi[1] analizza la fattibilità di un “attacco” a questi sistemi ABC, ovvero le possibilità che un ipotetico soggetto criminale presente in un elenco di ricercati in possesso di un documento con un'immagine facciale morphed ottenuta dalla combinazione di uno o più volti di soggetti senza precedenti penali riesca ad eludere i controlli. Ma come può accadere questo? Tutto questo può accadere se l'immagine memorizzata nell' eMRTD della persona sottoposta a verifiche è stata soggetta a *Morphing* ed ha tratti che possono corrispondere correttamente al volto di due o più soggetti; in questo caso quindi più persone possono condividere lo stesso documento eludendo i controlli ai gate. Esiste inoltre il rischio che una persona senza precedenti penali possa fare domanda per un eMRTD consegnando come foto di riconoscimento un'immagine sottoposta a *Morphing* e, se il personale dell'ufficio dedicato al rilascio di tale documento non dovesse riscontrare differenze tra l'immagine e la persona richiedente, potrebbe emettere un documento che non identifica univocamente una persona e che, nelle mani sbagliate, comporterebbe seri problemi di sicurezza.

Nello studio preso in considerazione vengono posti quindi gli accenti su due aspetti fondamentali: (i) la fattibilità di creare immagini facciali morphed ingannevoli e (ii) la robustezza dei sistemi di riconoscimento in commercio in

presenza di *Morphing*.

2.1 Fattibilità della creazione di immagini morphed

Come detto in precedenza il *Morphing* è un effetto digitale che cambia un'immagine in un'altra attraverso transizioni continue; spesso viene proprio utilizzato per raffigurare una persona cambiata in un' altra.
Nella relazione [1] che prendiamo in esame per analizzare questa tecnica di alterazione di immagine, vengono utilizzati 2 programmi di manipolazione di immagini per effettuare i test sul Morphing applicato a due immagini facciali: FREE GNU Image Manipulation Program v2.8 (GIMP) e GIMP Animation Package v.2.6 (GAP).
Dati due volti di persone distinte, attraverso alcune elaborazioni si ottiene un'immagine molto simile ad uno dei due soggetti (ipotizzando il richiedente del documento) ma che contenga anche dei tratti propri del volto dell'altro soggetto; come è facilmente intuibile, questa operazione risulterebbe sicuramente più facile nel caso di persone che presentano tratti somiglianti, ma questa non è una condizione necessaria affinché si generi il Morphing .
I passi che sono stati compiuti per effettuare il Morphing in modo semplificato sono i seguenti:

1. In uno dei due Software di manipolazione di immagini dichiarati nello studio [1] sono dapprima stati creati due livelli distinti di una stessa immagine in ognuno dei quali è stato inserito uno dei due volti;a questo punto si è proceduto manualmente all'allineamento delle immagini sovrapponendo gli occhi (Figura 1).

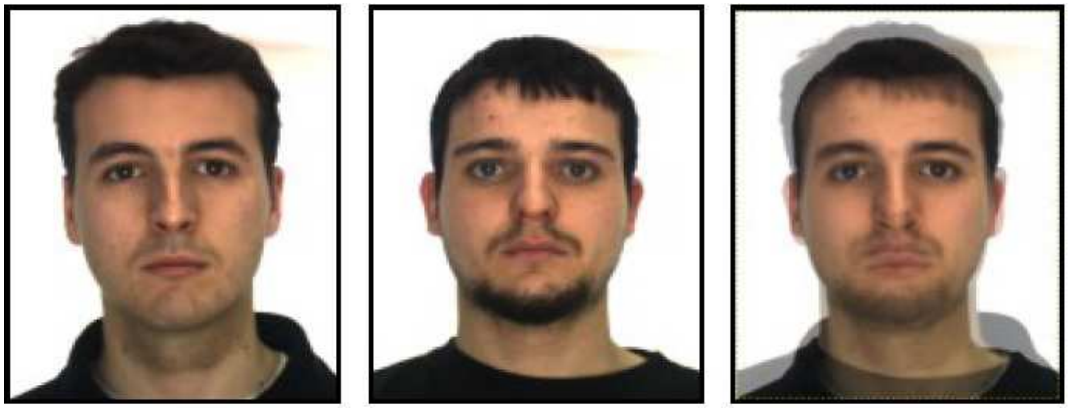


Figura 1: Primo step allineamento delle immagini

2. Utilizzando il tool GAP Morph sono stati segnati i “Control points” di cui avevamo parlato ad inizio capitolo,ovvero i punti di riferimento dell'immagine. Tra i punti scelti più frequentemente abbiamo ad esempio l'angolo degli occhi, le sopracciglia, la punta del naso e la fronte (Figura 2).

Figura 2: Secondo Step. Individuazione dei Control Points

3. Eseguite le operazioni precedenti è stata generata in modo automatico dal tool GAP Morph una sequenza di frame che mostranti la transizione da un viso all'altro (Figura 3).

4. A questo punto è stato scelto tra i frame creati quello che, partendo dalla foto del richiedente, otteneva un punteggio di confronto con il soggetto

per così dire “criminale”, maggiore.

Figura 3: Step 3.Frame ottenuti dalla procedura di Morphing

5. Effettuata la scelta del frame questi può essere stato sottoposto ad alcuni ritocchi per renderlo più realistico, così da potere essere scambiato per un'immagine originale (Figura 4).

Figura 4: Step 4/5.A sinistra il frame selezionato e a destra il frame sottoposto a ritocco.

2.2 Attacco ad un sistema ABC

Nello studio [1] sono stati eseguite alcune simulazioni di attacchi ai Sistemi ABC al fine di valutarne la robustezza in presenza di *Morphing*.

In questo paragrafo vengono quindi riportati e commentati i risultati sperimentali di questo articolo di ricerca [1], per dimostrare che, ad oggi, sono presenti alcune difficoltà nell'individuare questo tipo di alterazione in un'immagine digitale.

Gli strumenti commerciali su cui sono stati condotti gli esperimenti sono i seguenti: Neurotechnology VeryLookSDK 5.4[19] e Luxand FaceSDK4.0 [20].

Per rendere realistica la simulazione dell'attacco al sistema ABC, la soglia di riconoscimento facciale di entrambi i sistemi è stata impostata in accordo con le linee guida emesse da FRONTEX [21] (Agenzia Europea per la Gestione della Cooperazione Internazionale alle frontiere esterne degli Stati Membri dell'Unione Europea).

Più precisamente, per un sistema ABC che opera in modalità verifica, l'algoritmo deve garantire un livello di sicurezza in termini di FALSE ACCEPT RATE (FAR) almeno del 0,001%.

Per effettuare i test sono state selezionate dal AR Face database[22] coppie di immagini di volti di due persone con alcuni tratti somiglianti ma che sottoposte alla verifica di entrambi i sistemi SDK di riconoscimento non ottenevano un punteggio di corrispondenza rilevante.

L'AR Face Database contiene circa 4000 immagini a colori di volti(70 uomini e 56 donne), riprese in differenti espressioni facciali, condizioni di luce e occlusioni (ad esempio indossano occhiali da sole o altri elementi che ne oscurano parti del volto)(Figura 5).

Le immagini contenute nell'AR Face Database sono selezionate in modo da rispondere pienamente ai requisiti richiesti per i documenti eMRTD.

Queste coppie di immagini sono state sottoposte a Morphing ottenendo una terza immagine che include alcuni tratti di entrambi i volti di partenza.

Figura 5: AR Database: esempio di soggetto ripreso in diverse condizioni.

Infine con queste immagini è stata messa in atto la vera e propria simulazione.
I test della Relazione in esame[1] sono stati svolti su 5 coppie di persone di sesso maschile(Figura 6) e 5 coppie di sesso femminile (Figura 29). Oltre a questi sono stati simulati anche altri 2 tipi di attacchi: il primo mescolando un uomo e una donna(Figura 7) e il secondo mescolando tre uomini (Figura 8).
I test condotti nella relazione [1] mostrano come tutti gli attacchi di cui sopra abbiano avuto esito positivo, ovvero il Sistema ABC non ha rilevato alterazioni nelle immagini che aveva sottoposto a verifica.
I risultati sperimentali ottenuti nello studio considerato confermano che, in caso di immagine Morphed che include caratteristiche di somiglianza di due soggetti (source), ne il Sistema Automatico ne gli operatori umani sono in grado di rilevare con buon livello di accuratezza se il documento presentato appartiene realmente alla persona a cui appartiene .
In conclusione questo studio ha messo in luce come le contromisure presenti nei Sistemi di controllo Biometrici nei confronti di questi attacchi siano insufficienti.
Anche nel caso di controlli da parte di agenti di frontiera la percentuale di successo di un attacco è molto alta: è molto difficile non identificare una persona in un'immagine morphed se la stessa ha preso parte al processo di morphing.
Ad oggi l'acquisizione dell'immagine direttamente in un ufficio dedicato, con un'adeguata fotocamera ad alta risoluzione, rimane il modo più sicuro per rilasciare un Documento di viaggio valido e sicuro, evitando in questo modo che sia il cittadino a fornire la fototessera per il documento di viaggio.

Si rende quindi necessario studiare dei meccanismi per rilevare in modo automatico eventuali alterazioni digitali delle immagini in generale e in particolare le operazioni di Morphing.

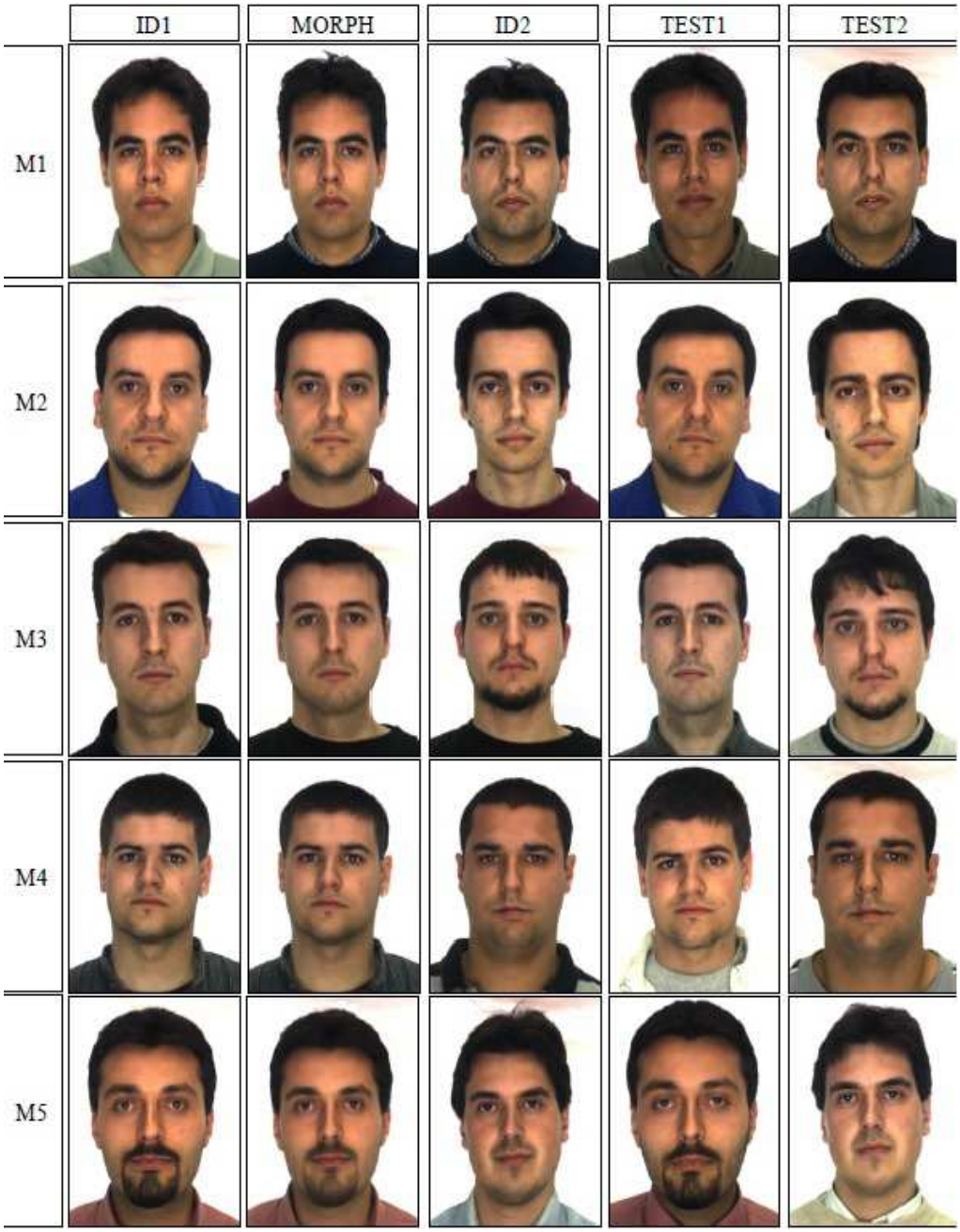


Figura 6: Esempi di immagini morphed ottenute da 5 coppie maschili. Nelle colonne ID1 e ID2 le immagini usate per il morphing, nella colonna MORPH il risultato del morphing e nelle colonne TEST1 e TEST2 le immagini utilizzate nei test.

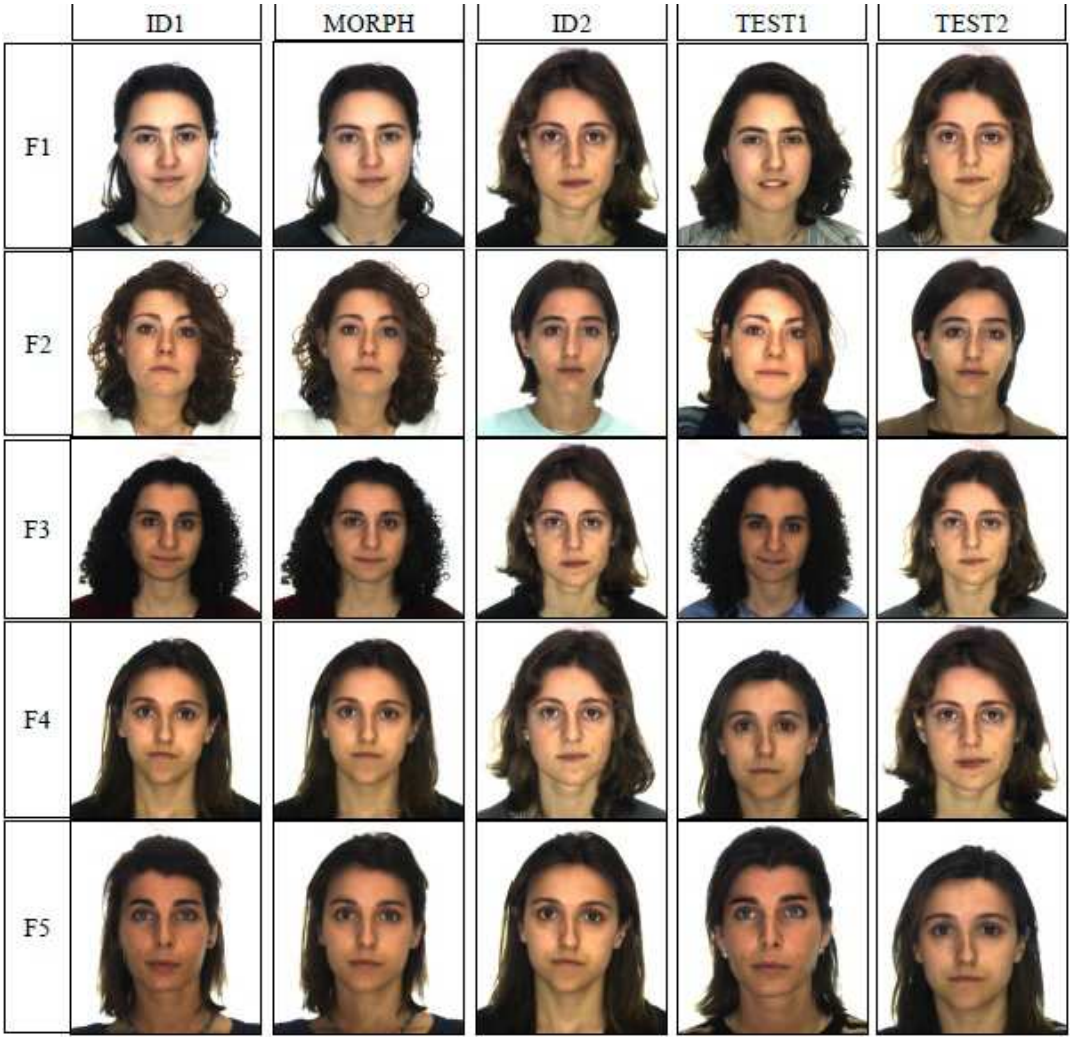


Figura 7: Esempi di risultati ottenuti da 5 coppie femminili

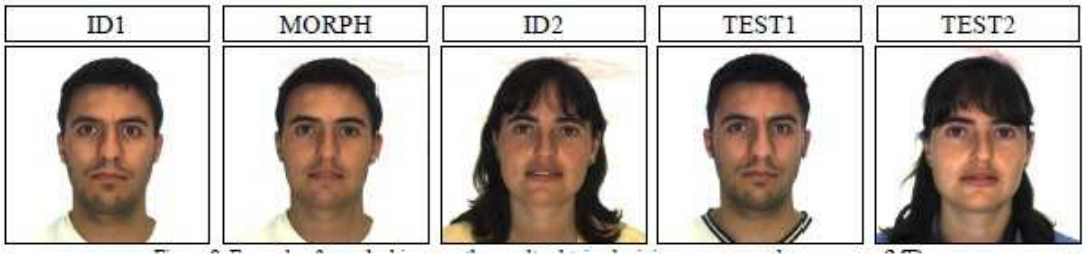


Figura 8: Esempio di risultato ottenuto utilizzando un volto maschile ed uno femminile

3. Morphing e riconoscimento del volto

Questo capitolo ha lo scopo di approfondire la tecnica di alterazione di immagini digitali che, come descritto nel Capitolo 2, rappresenta una delle principali problematiche che vengono affrontate quotidianamente ai gate di tutti gli aeroporti/porti internazionali: il Morphing.
Per introdurre questa breve trattazione viene innanzitutto definito in modo formale l'etimologia di Morphing e le sue prime applicazioni in ambito video. In seguito sono approfonditi gli effetti che portano a questa manipolazione e/o deformazione di immagini digitali.

3.1 Il Morphing

Le tecniche di animazione digitale subiscono una costante spinta a migliorare in termini di qualità e di creatività poiché i consumatori richiedono effetti speciali sempre più all'avanguardia, le aziende devono quindi sforzarsi per accontentare questo pubblico.
Gli appassionati dell'intrattenimento digitale non si accontentano più di semplici animazioni, ma desiderano una migliore qualità nelle transizioni di immagini e animazioni.
Proprio per questo sono stati introdotti diversi effetti speciali e uno dei più popolari tra questi è il Morphing di immagini che è stato utilizzato e migliorato nel corso degli anni per ottenere film, video, immagini, giochi di alta qualità ai fini di soddisfare e impressionare il pubblico.
Il termine Morphing significa metamorfosi di un'immagine e viene utilizzato per indicare le tecniche che permettono di creare un'animazione di trasformazione tra un oggetto ed un altro, o meglio, tra un'immagine digitale ed un'altra. Gli oggetti che subiscono la trasformazione possono essere di varia natura, fotogrammi, immagini, elementi tridimensionali e per ognuno di essi esistono software specifici in grado di realizzare le animazioni.

Uno dei primi esprimenti sul Morphing applicato nell'area cinematografica è stato condotto nel 1986 nella creazione del film “The golden child”.
Oltre che nella regia di film, la tecnica del Morphing di immagini è stata applicata nella realizzazione di video dal 1985 fino ad oggi.
Goodley & Crème, un famoso duo Rock inglese, è stato il primo ad introdurre l'effetto Morphing di dissolvenza incrociata nel loro video musicale “Cry”. Anche il famoso film di James Cameron “Terminator” e il video musicale della canzone “Black and White” di Micheal Jackson divennero famosi grazie all'implementazione del Morphing di immagine.
Oggigiorno il Morphing di immagini oltre ad essere applicato nei film, negli show televisivi, nei video e nei videogiochi viene implementato anche nei progetti multimediali come presentazioni o ebook illustrati.
Altre applicazioni note sono le tipiche trasformazioni da un volto ad un altro, utili per la generazione di ipotetici volti mancanti su un albero genealogico o per valutare come si possa alterare il volto di una persona al variare dell'età o dell'espressione del viso (creazione identikit).
Nella formulazione più comune, la generazione di un Morphing, consiste nel determinare un'immagine intermedia tra due immagini sorgenti: la prima immagine (*source*) viene deformata gradualmente e dissolta mentre la seconda immagine (*target*) aumenta gradualmente di intensità e passa in primo piano.
In definitiva l'intero processo consiste nel deformare due immagini in modo da portarle ad avere la stessa forma per poi dissolvere le immagini risultanti una dentro l'altra.
Il Morphing viene attuato applicando un algoritmo o una formula matematica alla mappa dei pixel di un'immagine di input fino ad ottenere una immagine di output.
Ci sono tre processi coinvolti nel Morphing di un'immagine e sono: F*eatures Specification* (la specifica dei tratti), W*arp Generation* (la generazione della deformazione) e *Transition Control* (il controllo della transizione).
E' bene specificare che in letteratura certe volte i termini *Morphing* e *Warping* sono usati quasi indistintamente, quando invece il primo comprende ulteriori fasi rispetto al secondo. La confusione nasce dal fatto che il *Morphing* include il

Warping e pertanto questi due processi condividono le medesime tecniche di base.

3.1.1 Features Specification

E' stato introdotto da Beier e Neely nel 1992 ed è chiamato anche *Feature-based Morphing* e si basa sulla definizione di primitive (punti o linee) di controllo. E' importante che in entrambe le immagini le linee di controllo corrispondano. Viene inoltre definita una regione di influenza per ogni primitiva di controllo.
I punti all'interno della regione di controllo si spostano (deformando l'immagine) secondo una trasformazione geometrica.
I punti che ricadono all'interno di più regioni di controllo vengono deformati combinando le diverse trasformazioni geometriche.
Nella maggior parte dei casi l'individuazione di questi tratti avviene manualmente ed è questo che rende il processo ancora più difficile. L'accuratezza del processo di "*Warping*" dipende dalla scelta e dal numero di questi punti di controllo. Uno svantaggio derivante da questa tecnica è il costo computazionale: per ogni pixel, occorre calcolare la quantità di spostamento per tutte le features. La scelta di questi punti deve essere fatta tenendo conto di alcune proprietà tra cui, per esempio, la distanza tra i punti scelti, i contorni e i tratti distintivi.
Rimane comunque una tecnica espressiva ed intuitiva per l'animatore, infatti le features sono dei tratti che caratterizzano la coppia di immagini come ad esempio la bocca, il naso, le sopracciglia (Figura 9).

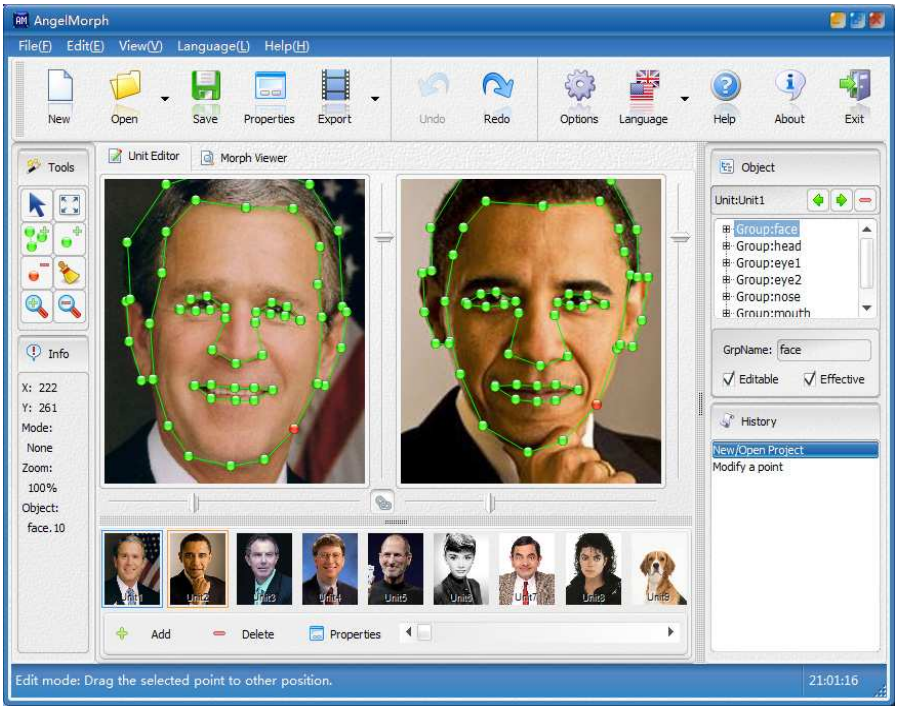


Figura 9: Esempio di selezione delle Features comuni a due volti

3.1.2 Warping generation e Mesh Warping

Il *Warping* consiste nel determinare una deformazione controllata dell'immagine sorgente utilizzando i punti di controllo o Landmarks (2.1.1.) la cui tipologia abbiamo visto che dipende dall'approccio utilizzato (di norma sono punti singoli ma possono anche essere linee o griglie).

Variando la posizione o l'orientamento di questi punti l'immagine deve deformarsi in modo coerente e intuitivo.

Dal punto di vista matematico il *Warping* può essere definito come una funzione $f: R^2 \rightarrow R^2$ che mappa i punti dell'immagine iniziale in quelli dell'immagine deformata: applicando *f* ad ogni punto *v* dell'immagine sorgente si ottiene l'immagine deformata.

Siano ora $S=\{s_1 , s_2 ,...s_n\}$ l'insieme dei punti di controllo nella loro posizione iniziale, e $D=\{d_1,d_2,..d_n\}$ i rispettivi punti nella posizione finale, allora la funzione *f* deve sottostare ai seguenti vincoli:

- *Interpolazione* : ogni punto di controllo deve essere mappato nel relativo punto di destinazione ($f(s_i)=d_i$ *per ogni i tra 1 e n*)

- *Continuità* : la deformazione ottenuta deve essere morbida e senza evidenti discontinuità

- *Identità* : se la posizione finale dei landmark è identica a quella iniziale, allora l'immagine non deve essere deformata (f(v) = v per ogni punto v dell'immagine).

La "*Warp generation*" consiste quindi nell'applicare un algoritmo che calcola e trasforma i pixel di un'immagine in una nuova posizione in un'altra immagine.
Ci sono molti algoritmi che si sono dedicati a fare il "*Warping*"; questo può essere definito come un metodo per deformare un'immagine digitale in diverse forme. Il "Mapping" dei pixel da un'immagine all'altra viene determinato proprio in questa fase di W*arping.*
Ci sono due step inclusi in questa seconda fase: il primo step è quello del calcolo di tutti i casi in cui è necessario rimpiazzare i pixel nella prima immagine, che coincide con l'immagine di partenza.
Il secondo step consiste nel ricampionamento dell'immagine per ottenere l'immagine finale o immagine di output.
Il *Mesh Warping* è una tecnica di *Warping* che si basa sulla costruzione di una mesh nell'immagine sorgente e destinazione.
L'immagine viene suddivisa in tante piccole aree rettangolari come vediamo nella Figura 10.
Ciascun rettangolo viene trasformato in un quadrilatero e i punti all'interno di ciascuna area seguono la trasformazione dettata dall'area di appartenenza (Figura 11).

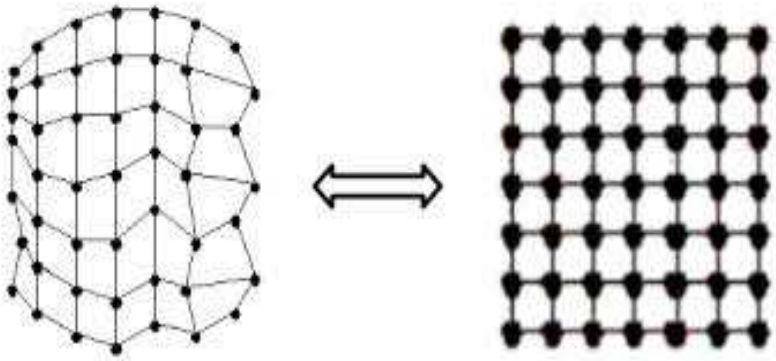


Figura 10:Griglia di riferimento per il Mesh Warping

Figura 11: Esempio di Mesh Warping applicato ad un'immagine

Nel processo di *Image Warping* interviene anche una fase di *Mapping,* che consiste nel determinare la funzione che stabilisce la corrispondenza tra la posizione (x,y) in un'immagine e la posizione (u,v) in un'altra. Sono possibili due approcci al problema:

1) *Forward mapping*: date *(u,v)* le coordinate di un pixel nell'immagine sorgente e *(x,y)* le coordinate nell'immagine destinazione:

$x = f_x(u,v)$

$y = f_y(u,v)$

Questo tipo di approccio è sconsigliato dal momento che si possono creare dei buchi nell'immagine destinazione.

Infatti se un pixel della sorgente corrisponde a più di un pixel nella destinazione, la precedente funzione riesce a trovare solo una corrispondenza, lasciando indeterminati gli altri pixel.

2) Reverse mapping: risolve il problema del Forward Mapping, ribaltando il modo di vedere le cose :

$u = f_x^{-1}(x,y)$

$v = f_y^{-1}(x,y)$

In questo modo si considerano le coordinate dell'immagine sorgente come funzione di quelle della destinazione.

Anche con questo approccio è possibile riscontrare un problema, chiamato Oversampling: più pixel della destinazione corrispondono allo stesso pixel della sorgente, ma in questo modo si risolve il problema dei “buchi”.

3.1.3 Transition control

L'Image Morphing combina la distorsione dell'immagine con un metodo che controlla la transizione dei colori nelle immagini intermedie prodotte dal processo.

Un Morphing contiene una sequenza di immagini intermedie dall'immagine

origine fino all'immagine che si vuole ottenere.

Per poter creare un “morph” di un'immagine in una nuova immagine è necessario determinare in ciascuna delle immagini della sequenza la posizione e la velocità di transizione di ciascun pixel che la compongono. Infatti la qualità del “morph” ottenuto dipende proprio da quest'ultima, la velocità di transizione.

Uno dei metodi per la fusione dei colori delle immagini è la dissolvenza incrociata in cui date due immagini, vengono generate immagini intermedie in cui il colore è una media pesata dei colori delle due immagini.

Uno degli svantaggi che spesso si riscontrano è il “ghost-busting”: in alcune regioni si genera una deformazione inaspettata .Si manifesta con la comparsa di parti dell'immagine originale, in posizioni sbagliate dell'immagine intermedia.

4. Caratteristiche delle immagini digitali

4.1 Costruzione di un'immagine digitale

Il procedimento (pipeline) che porta alla memorizzazione di una scena reale in un file immagine può essere suddiviso in tre fasi principali[15]: acquisizione, elaborazione e memorizzazione.

Nella fase di acquisizione la luce proveniente dalla scena attraversa il sistema di lenti che la indirizza verso il sensore della fotocamera (costruito con tecnologia CCD o CMOS) come si vede in Figura 12 . Quest'ultimo è composto da un alto numero di elementi fotosensibili che catturano l'energia della luce convertendola in corrente elettrica e che riescono in tal modo a determinare il valore di luminosità di ciascun pixel.

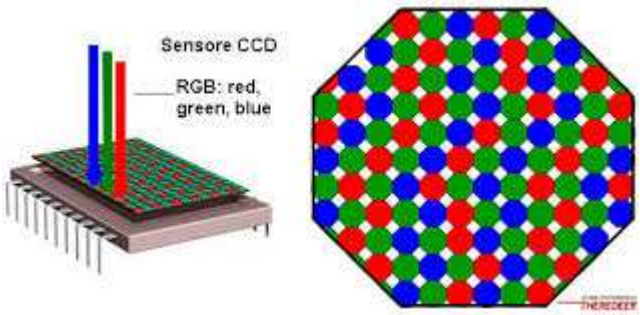


Figura 12: Esempio di sensore CCD(Charge-Coupled Device)

Per acquisire immagini a colori è necessario scomporre la luce visibile nelle tre componenti fondamentali, corrispondenti alla lunghezza d'onda del rosso, del verde e del blu. In linea di principio bisognerebbe avere un sensore per ognuno dei colori da catturare, facendo lievitare il costo delle fotocamere e introducendo svariate complicazioni tecniche.

I dispositivi in commercio invece adottano un'altra soluzione: sopra il sensore

viene applicata una sottile pellicola fotosensibile, detta CFA(Color Filter Array), che ha il compito di filtrare la luce e di separarla nei tre colori fondamentali in modo che ogni singolo pixel sia specializzato nella cattura selettiva di ciascuno di questi colori.
In questo modo si ottiene una griglia di valori in cui ogni pixel registra il segnale relativo ad una sola componente cromatica. L'utilizzo dei CFA permette di utilizzare un solo sensore per l'acquisizione a colori, ma richiede la ricostruzione delle due componenti mancanti mediante un algoritmo di interpolazione (Demosaicing) che approfondiremo nel paragrafo 5.3.1.
Di solito questa elaborazione viene eseguita dal processore della fotocamera prima della memorizzazione della foto, unitamente ad altre operazioni di post-processing quali: bilanciamento del bianco, l'elaborazione del colore, la correzione di pixel difettosi, la soppressione delle “dark currents”, il miglioramento del contrasto e la correzione gamma. L'immagine ottenuta viene quindi compressa in uno dei formati disponibili sul dispositivo secondo la configurazione dell'utente.
L'algoritmo utilizzato per la compressione dalla maggior parte delle fotocamere in commercio è il JPEG. Molti dispositivi, specie quelli di fascia medio/alta, permettono di salvare l'immagine in formato TIFF, oppure in formato RAW. Quest'ultimo è un formato definito in maniera indipendente per ogni produttore e salva i dati grezzi come acquisiti dal sensore, permettendo al fotografo un controllo assoluto e preciso su tutta la fase di sviluppo digitale dell'immagine.
E' importante sapere che ogni fase di formazione dell'immagine lascia un segno, una traccia. L'elenco di questi segni può essere suddiviso nel seguente modo[8]:

- Caratteristiche intrinseche della scena ripresa;
- Tracce durante l'acquisizione;
- Tracce dovute al software di elaborazione interno alla fotocamera;
- Tracce lasciate nella fase di elaborazione subita dall'immagine dopo la sua creazione e durante il salvataggio in memoria.

E' importante conoscere questi segni perché ogni manipolazione (malevola o meno) ha come conseguenza l'alterazione di almeno uno di questi.

4.1.1 Caratteristiche intrinseche della scena

Per semplificare e schematizzare il processo di creazione di un'immagine si adotta il modello “*Pinhole Camera Model”.*
Questo modello presuppone che tutti i raggi ottici che concorrono alla formazione dell'immagine, siano “transitati”, ad un certo tempo del cammino in un unico punto, detto centro di Proiezione CP , come si può vedere nella Figura 13.

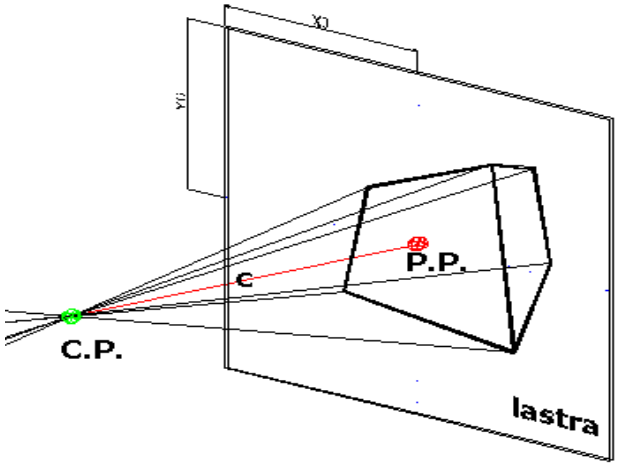


Figura 13: Pinhole Camera Model

Infatti il nome “Pin-Hole”, letteralmente “buco di spillo”, nasce proprio dal fatto che la luce che impressiona i sensori di una fotocamera digitale, attraversi un foro di piccole dimensioni, così piccolo da poter essere considerato un punto nell'accezione geometrica del termine.
Tracciando una retta ortogonale al piano del sensore e passante per il centro di Proiezione CP si individua un elemento di riferimento della prospettiva di

un'immagine che viene detto Punto Principale (P.P. In Figura 7).
La distanza tra i punti CP e PP è la focale della camera e viene evidenziata in figura 7 con la lettera c.
L'assunzione che tutti i raggi proiettivi passino per il punto CP è evidentemente solo un'approssimazione. Nella realtà questo non è un punto ma uno spazio di dimensioni finite. Questo produce una deformazione dell'immagine, che prende il nome di distorsione.
Vediamo quindi che la prospettiva ha come effetto quello di distorcere le dimensioni degli elementi presenti nella scena in maniera più o meno accentuata a seconda della loro distanza dal piano del sensore.
Ne deriva che data un'immagine sarà possibile ricavarne attraverso modelli matematici alcuni elementi caratteristici della scena ripresa come i punti e le linee di fuga, oltre al Punto Principale evidenziato precedentemente.
Anche luci e ombre sono elementi caratteristici molto importanti nell'analisi di una scena.
La luminosità di ciascun pixel che compone un'immagine digitale è proporzionale alla quantità di luce che la superficie a cui si riferisce quel determinato pixel riflette verso la fotocamera. Un modello semplificato prevede che la fonte di illuminazione in una scena esterna possa essere modellata come un punto infinitamente lontano. Questo permette di stimare la direzione della fonte di luce e, allo stesso tempo, di avere informazioni sulla scena basandosi sulle ombre prodotte dai soggetti rappresentati.

4.1.2 Tracce durante l'acquisizione

Ogni tipo di macchina fotografica monta un proprio sistema di lenti e queste possono introdurre dei difetti di ottica, come possiamo vedere nella Figura 14.
Questi difetti si possono suddividere principalmente in categorie: la distorsione geometrica radiale[12],visibile nelle immagini (a) e (b) della figura 14 e le aberrazione cromatiche[13], immagini (c)(d) della medesima figura.

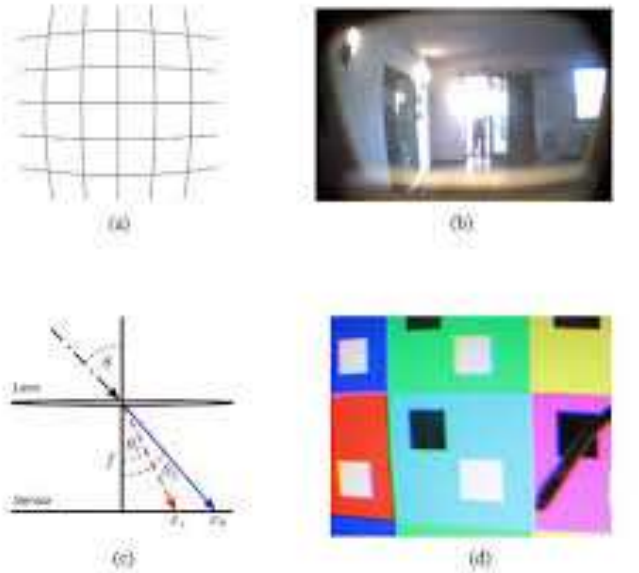


Figura 14: Esempi di difetti provocati dalle lenti di una fotocamera

La distorsione geometrica radiale è una deviazione della proiezione rettilinea che fa apparire le curve le linee mano a mano che si allontanano dal centro ottico dell'immagine.

L'aberrazione cromatica invece è un difetto nella formazione dell'immagine dovuta al diverso valore di rifrazione delle diverse lunghezze d'onda che compongono la luce che passa attraverso il mezzo ottico. Questo si traduce in immagini che presentano ai bordi dei soggetti aloni colorati.

Un ulteriore traccia distintiva è quella lasciata dalle imperfezioni di fabbrica del sensore montato nella macchina fotografica utilizzata. Queste imperfezioni producono delle disuniformità che si traducono in una differente sensibilità alla luce nelle diverse zone. In questo modo ogni sensore appone una propria firma (pattern), unica, che può essere identificata estraendo una componente specifica del rumore chiamata PRNU(Photo Response Non Uniformity), che trattato opportunamente può individuare diversi dispositivi.

4.1.3 Tracce dovute al software di elaborazione interno alla fotocamera

Sono tre i tipi di tracce che vengono rilasciate in un'immagine a causa del software utilizzato dalla fotocamera per l'elaborazione: la CFA Interpolation, i Metadati EXIF e Thumbnail e Preview.
Come già accennato all'inizio del capitolo, il compito dei sensori CFA (*color filter array)* è quello di filtrare la luce incidente la matrice di sensori lasciando passare solamente una certa lunghezza d'onda per sensore al fine di ottenere un'immagine RGB a risoluzione piena. I valori dei pixel di luminosità che mancano si ottengo attraverso una procedura che stima tali valori combinando quelli dei pixel vicini mediante una funzione di interpolazione.
La specifica di formato di file immagine utilizzato dalle fotocamere digitali, EXIF (Exchangeable Image File Format), utilizza i formati esistenti JPEG, TIFF e RIFF con l'aggiunta di specifiche etichette di metadati.
Questi tag di metadati definiti nello standard EXIF[31], di cui un esempio in Figura 15, includono una vasta gamma di informazioni nell'immagine,tra cui:

- Informazioni di data e ora. Le fotocamere digitali registrano la data e l'orario corrente in questi metadati.

- Includono informazioni statiche come il modello e il produttore della fotocamera, ed informazioni varie per ciascuna immagine come ad esempio l'orientamento, l'apertura, la velocità di scatto, la lunghezza focale, il bilanciamento del bianco e le informazioni di velocità ISO impostate.

- Una miniatura per visualizzare l'anteprima sul display LCD della fotocamera oppure nei software di fotoritocco.

- Descrizioni ed informazioni di copyright.

Figura 15: Esempio di Metadati EXIF

Inoltre la maggior parte dei dispositivi moderni salva all'interno dell'immagine principale una o due immagini secondarie, chiamate thumbnail (miniatura) e preview (anteprima). In pratica la Thumbnail è una versione a bassa risoluzione dell'immagine principale e può essere usata dalla macchina fotografica per presentare le immagini disponendole sotto forma di griglia nel display.

La preview invece è una miniatura dell'immagine principale ma con una risoluzione maggiore rispetto alla thumbnail e viene utilizzata per visualizzare velocemente l'immagine sul display.

4.1.4 Tracce lasciate dopo il salvataggio

Dopo le eventuali modifiche applicate ad una fotografia vi è sempre la necessità di salvare l'immagine dopo i cambiamenti. Questo salvataggio multiplo può essere individuato esaminando i relativi istogrammi riferiti ai valori dei coefficienti DCT (*Discrete Cosine Transform*). Non ci soffermiamo ulteriormente

sull'algoritmo di compressione JPEG, ma dopo avere effettuato gli opportuni controlli su questi coefficienti è possibile determinare se sono state fatte modifiche sull'immagine.

4.2 Modifiche al contenuto informativo dell'immagine

I Software di editing o manipolazione delle immagini, come detto in precedenza, sono divenuti facilmente disponibili nel mercato e divenuti sempre più facili da utilizzare.
Utilizzando i potenti tool di editing di questi software è possibile a ciascuna tipologia di utente di fare delle modifiche al contenuto delle immagini digitali e violarne l'autenticità.
Oggigiorno le immagini digitali vengono utilizzate in maniera sempre più diffusa anche in ambito legislativo quindi comprovarne l'autenticità e veridicità è diventato un ambito molto rilevante. In seguito vedremo alcuno delle operazioni principali a cui vengono sottoposte le immagini come ad esempio la rotazione, il ridimensionamento, l'allungamento, applicare uno zoom e varie tecniche di miglioramento.
Molto spesso è necessario capire se l'immagine è stata revisionata oppure no, invece di individuare quale specifico tipo di falsificazione è implicata.

4.2.1 Tecnica di taglia-incolla (splicing)

Questa tecnica si compone di 3 operazioni fondamentalmente:si copia una parte dell'immagine originale e la si incolla in un'altra immagine desiderata, come si vede nell'esempio in Figura 16. Questo tipo di editing aggiunge informazione all'immagine.

Figura 16: Esempio di immagine modificata con tecnica copia-incolla. L'immagine delle donna è stata tagliata e incollata su di una passerella.

4.2.2 Tecnica di ritaglio di parte dell'immagine (cropping)

Questa tecnica consiste nella selezione di una parte dell'immagine (detta ROI-Region of Interest), salvandola poi come immagine a se stante(Figura 17). Questo tipo di editing, a differenza dello *splicing* visto nel paragrafo precedente, rimuove informazione dall'immagine.

Figura 17: Esempio di ritaglio: il contenuto dell'immagine di sinistra è stato modificato togliendo la parte indesiderata; l'immagine risultante è visualizzata a destra

4.2.3 Tecnica Cloning (copia e incolla)

Il Cloning di un'immagine consiste di duplicare parti dell'immagine nell'immagine stessa. A seconda dell'operazione che si effettua sull'immagine, che può essere di "tagliare" o copiare una o più aree dell'immagine, si aggiunge o elimina informazione. (Figura 18)

Figura 18: Esempio di Cloning; in questo caso è stata fatta la scelta di copiare e incollare un'area dell'immagine,aggiungendo informazione

4.2.4 Tecnica del Retouching

La Figura 19 è un esempio di immagine sottoposta a Retouching, ovvero a “ritocco”. Il Retouching è visto come la tecnica meno dannosa nell'ambito della contraffazione di immagini digitali. Il ritocco modifica in modo significativo l'immagine e ne riduce alcune caratteristiche. Ormai moltissime riviste utilizzano la tecnica di Retouching per migliorare alcuni tratti di un'immagine, in modo da rendere il soggetto più attraente e vicino alla percezione comune di perfezione.

Figura 19: Esempio di Retouching applicato ad un volto femminile

4.3 Contraffazione: casi famosi e non

L'innocenza della fotografia è stata violata sin dagli albori della sua nascita. Nièpce creò la sua prima fotografia nel lontano 1826 e solo pochi decenni dopo, nel 1860 vennero individuate delle fotografie manipolate.

Macchine fotografiche digitali, videocamere e sofisticati software di editing fotografico hanno semplificato la possibilità di manipolare un'immagine.

Di seguito alcuni dei più noti casi di manomissione [16]:

1860 circa: Questo ritratto del Presidente Americano Abrahm Lincoln (sotto forma di Litografia) è composto dal volto del Presidente Lincoln e dal corpo del politico John Calhoun (Figura 20).

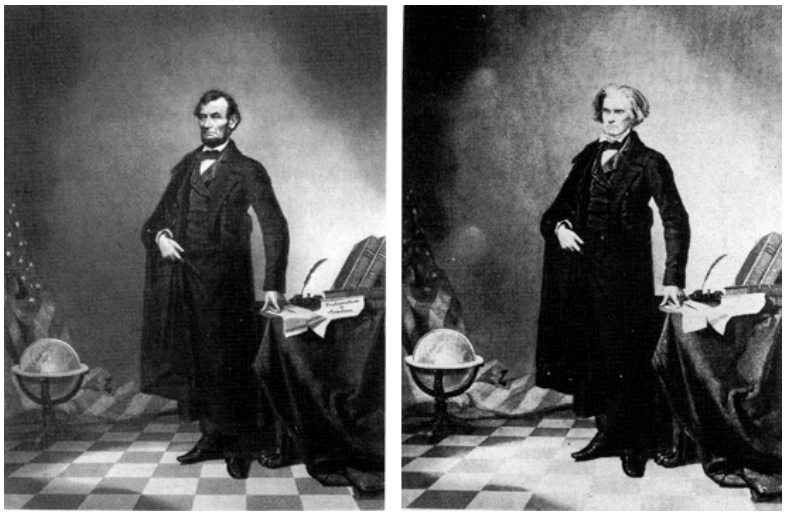


Figura 20: Lincoln's portrait. A sinistra l'immagine alterata e a destra l'immagine originale.

1930: Una delle routine di Stalin era quella di fare eliminare i suoi nemici dalle fotografie. In questa fotografia un Commissario è stato rimosso dalla documento originale (Figura 21).

Figura 21: Image of Stalin. Rimozione di un soggetto dalla foto.

1937: In questa fotografia ritoccata, Adolf Hitler ha fatto rimuovere Joseph Goebbels (secondo da destra). Non è chiaro il motivo che ha portato Hitler a prendere questa decisione (Figura 22).

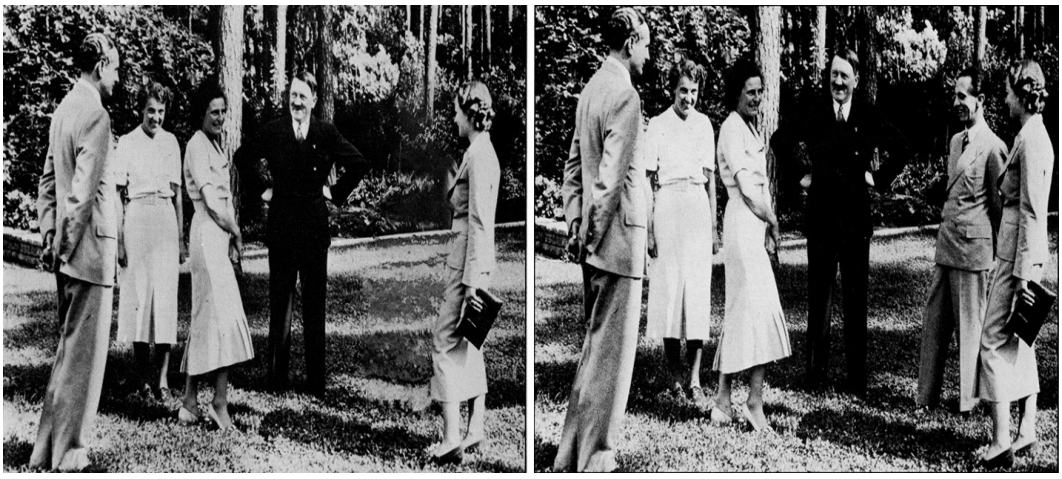


Figura 22: Hitler's photo.

1942: Al fine di creare un ritratto più eroico di se stesso, Benito Mussolini ha fatto rimuovere il ragazzo che teneva il cavallo (Figura 23).

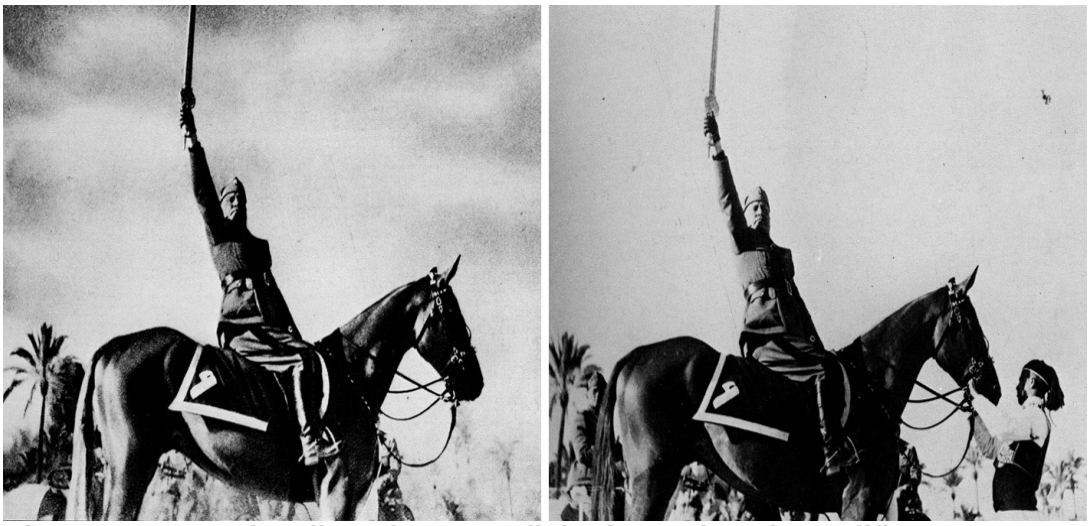


Figura 23: Immagine di Benito Mussolini prima e dopo la modifica.

1994: Questa fotografia manipolata di OJ Simpson è apparsa sulla copertina della rivista Time, poco dopo l'arresto di Simpson per omicidio.
La rivista Time è stata accusata di avere manipolato la fotografia per rendere Simpson più “minaccioso” e più “scuro” (Figura 24).

Figura 24: Copertine del Time e di Newsweek a confronto.

2003: La copia originale della copertina dei Beatles Abbey Road mostra Paul McCartney, terzo in linea, con una sigaretta. Le aziende pubblicitarie degli Stati Uniti hanno aerografato questa immagine per rimuovere la sigaretta dalla mano di McCartney (Figura 25).

Figura 25: Beatles Abbey Road

5. Algoritmi di Alteration Detection

5.1 Approcci generali sull'autenticazione di immagini

In generale possiamo identificare i possibili approcci che consentono l'autenticazione di un'immagine digitale in due tipologie: un approccio attivo o Non-Blind e uno passivo o Blind.

Un metodo di autenticazione di un'immagine digitale che si trova nel gruppo “approcci attivi” è quello che propone di inserire all'interno dell'immagine un “filigrana digitale”, in letteratura anglosassone si utilizza in genere la forma estesa “D*igital Watermarking*” [14].

Così come, ad esempio, nelle banconote viene inserito una filigrana come simbolo di copyright che ne verifica l'autenticità, in informatica si intende l'inclusione di informazioni all'interno di un file multimediale o di altro genere, che può essere successivamente rilevato o estratto per trarre informazioni sulla sua origine o provenienza.

Queste informazioni, lasciano il documento accessibile ma contrassegnato in modo permanente.

Esse possono essere evidenti per l'utente che visiona il file (per esempio in caso di indicazione di copyright applicata in sovrimpressione su una immagine digitale) o latenti (nascoste all'interno del file); in quest'ultimo caso il W*atermarking* può essere considerato una forma di steganografia.

Negli ultimi anni sono state proposte diverse tipologie di filigrane che, non solo possono essere utilizzate ai fini dell'autenticazione, ma anche come prova per individuare la falsificazione.

Lo svantaggio di questa tecnica è che è necessario inserire questa filigrana al momento dello scatto dell'immagine, cosa che limiterebbe questo approccio alle persone che posseggono una fotocamera attrezzata per questo scopo.

Un approccio diverso è quello cosi detto “passivo” che, in contrasto con gli approcci attivi sono realizzati senza l'applicazione di una filigrana o di una firma digitale.

Queste tecniche si basano sull'assunzione che anche se la contraffazione digitale potrebbe non lasciare tracce visibili, potrebbero però alterare le statistiche implicite di un'immagine.
Le tecniche forensi per l'individuazione di manipolazioni sono raggruppate in 5 categorie:

- **Tecniche Pixel-Based**: che individuano anomalie statistiche a livello di pixel;

- **Tecniche Format-based**: che fanno leva sulle correlazioni statistiche contenute nelle tecniche di compressione Lossy(con perdita di dati);

- **Tecniche camera-based**: che sfruttano gli artefatti introdotti dalla lente,dal sensore e dalla pipeline della macchina fotografica;

- **Tecniche Physically-based**: che generano un modello specifico delle anomalie mediante un'interazione nello spazio 3D degli oggetti, delle fonti di luce e dei sensori della fotocamera;

- **Tecniche Geometric-based**: che confrontano le misure fisiche degli oggertti reali e delle loro posizioni rispetto alla videocamera.

5.2 Rilevazione di manipolazioni con le Binary Similarity Measures

5.2.1 Cenni sulla rappresentazione di un'immagine

Nella rappresentazione di un'immagine ogni pixel rappresenta l'intensità nella corrispondente posizione della griglia di campionamento. Un pixel rappresenta in realtà non soltanto un punto dell'immagine, ma piuttosto una regione

rettangolare coincidente con una cella della griglia. Il valore associato al pixel deve pertanto rappresentare l'intensità media nella cella (Figura 26).

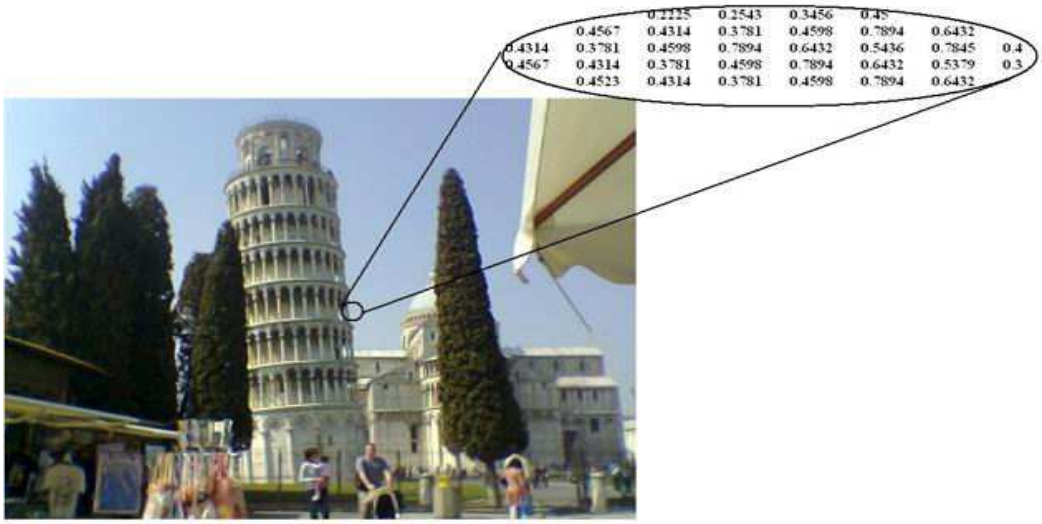


Figura 26: Rappresentazione numerica di un'immagine. Nel riquadro è riportato il valore dell'intensità dell'immagine.

La risoluzione spaziale è il più piccolo dettaglio distinguibile in un'immagine e viene normalmente espressa in elementi per unità di lunghezza, per esempio pixel per Inch. Quando non è necessaria una valutazione della risoluzione che metta in relazione il numero di pixel con il livello di dettaglio della scena originale, è di uso dire semplicemente che un'immagine di dimensione MXN ha una risoluzione MXN.

La dimensione dei pixel influisce sulla qualità visiva dell'immagine (Figura 27):con pixel di grandi dimensioni appaiono ben visibili le discontinuità di grigio mentre man mano che la dimensione dei pixel si riduce si ha l'impressione di un'immagine continua.

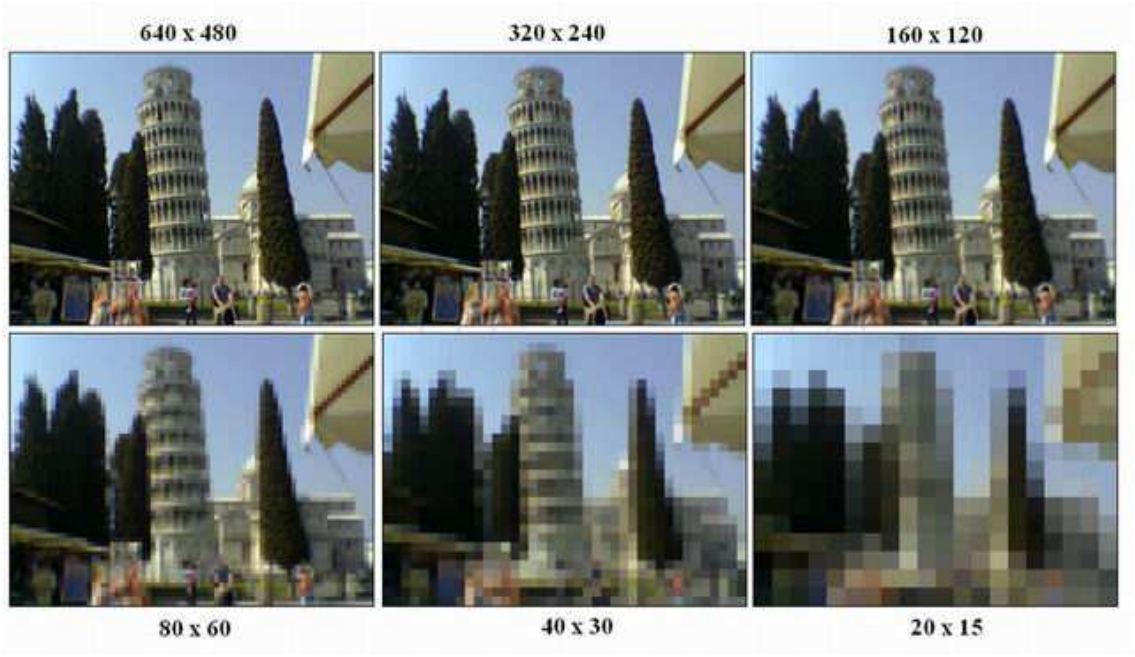


Figura 27: Esempio di rappresentazione di un'immagine modificando la dimensione dei pixel.

In realtà è la tecnologia dei sensori che determina la dimensione dei pixel e quindi la risoluzione dell'immagine.
La qualità dell'immagine dipende anche dal numero di livelli adoperati per la quantizzazione dei valori di intensità (risoluzione dei livelli di grigio)(Figura 28).
Un'immagine con un profondità colore di N bit può essere rappresentata da N piani di bit (bit planes), ciascuno dei quali può essere visto come un'immagine binaria.

Gray Level = 1 piano
True color = 3 piani (Red, Green, Blue)

In alcune applicazioni può essere utile evidenziare il contributo di specifici bit alla apparenza complessiva dell'immagine. Se per codificare i pixel di un'immagine si utilizzano 8 bit, si può considerare l'immagine costituita da 8 piani di 1 bit, dal piano 0 (che contiene il bit meno significativo di ogni pixel) al piano 7 (che contiene il bit più significativo).

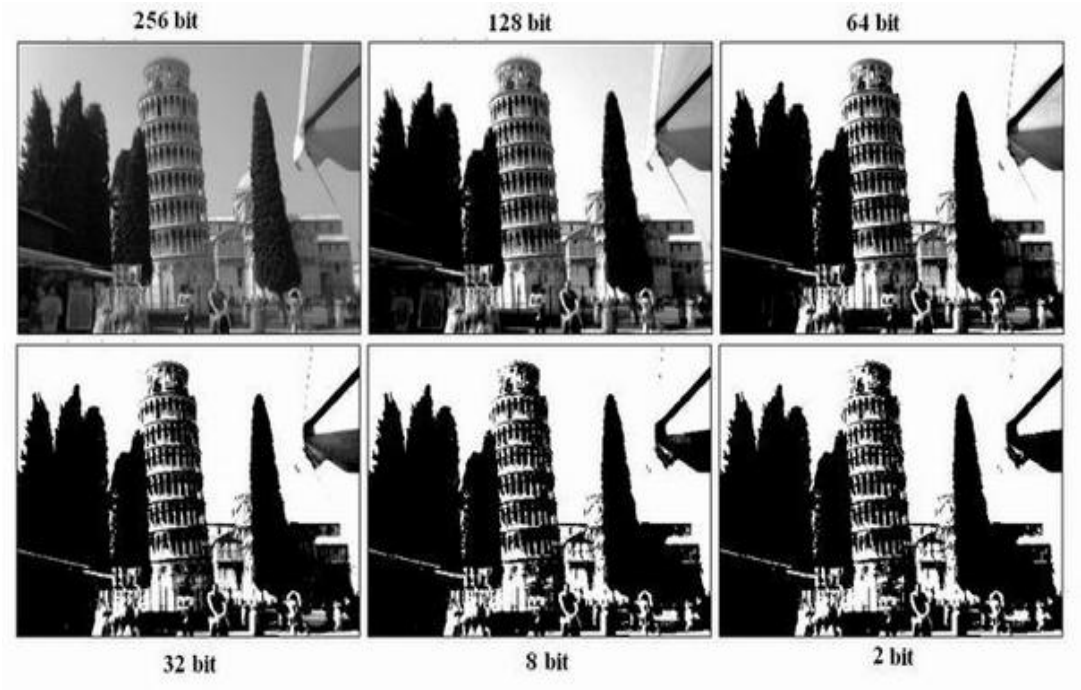


Figura 28: Esempio di rappresentazione di un'immagine modificando le dimensioni dei pixel a parità di dimensioni dell'immagine.

Se si considera il valore di ogni pixel dell'immagine espresso in binario, ovviamente il bit più significativo si trova nel piano 7, il bit di peso immediatamente inferiore si trova nel piano 6 e così via per tutti gli altri.

Il Bit-plane Slicing (Figura 29) consiste quindi nello scomporre un'immagine in otto immagini binarie, rappresentate da vari piani [17].

Figura 29: Scomposizione di un'immagine in otto immagini binarie (Bit-plane Slicing)

5.2.2 Binary Similarity Measures

Il metodo Binary Similarity Measures si basa sull'analisi dei piani a bit adiacenti di un' immagine utilizzando un insieme di misurazioni chiamate similarità binarie.

E' stato dimostrato che le classificazioni lineari basate sulle caratteristiche BSM sono in grado di individuare con soddisfacente veridicità la maggior parte delle manipolazioni effettuate tramite tool di Photoshop.

Le differenze nelle caratteristiche intrinseche dell'immagine possono essere monitorate attraverso le variazioni quantico-spaziali dei piani a bit; di conseguenza alcune caratteristiche statistiche estratte dai piani a bit dell'immagine possono essere utilizzate per rivelare la presenza di manipolazioni in un'immagine.

Dal momento che ciascun piano di bit è anche un'immagine binaria, si considera inizialmente il confronto tra le misure di due immagini binarie. Queste misure, chiamate appunto Binary Similarity Measures (BSM) erano state utilizzate in precedenza nel contesto della Steganalisi di immagini.

Nello studio [10] preso in considerazione in questa tesi per l'analisi del metodo

BSM, viene misurata la correlazione tra i piani di bit numerati 3-4, 4-5, 5-6, 6-7 per il canale rosso e i piani a bit 5-5 per i canali rosso e blu.

Le misurazioni classiche sono basate sul matching bit-a-bit tra le posizioni dei pixel corrispondenti nelle due immagini. Tipicamente, queste misure vengono ottenute dai punteggi basati su una tabella di contingenza calcolata su tutti i pixel dell'immagine.

Nello studio considerato è stato scoperto che è più rilevante effettuare dei confronti basati sulle *Binary Texture Statistics.*

I risultati sperimentali sono stati ottenuti calcolando le Binary Similarity Measures(Figura 29) come caratteristiche e utilizzando l'algoritmo Sequential Floating Forward Search (SFFS) per selezionare le migliori tra queste caratteristiche e utilizzando il Linear Regression Classifier per la classificazione.

L'esperimento è stato realizzato costruendo un database contenente 200 immagini, ottenute con una fotocamera modello Canon Powershot 200. Le immagini sono state acquisite tutte dalla stessa fotocamera in modo da poter rilevare le alterazioni a livello di informazione, e non quelle dovute alle proprietà della fotocamera. Le immagini campione erano precedentemente state sottoposte ad alterazioni utilizzando Adobe Photoshop, tra cui la rotazione, il ridimensionamento, la correzione della luminosità, la sfocatura e il miglioramento dei margini. La metà delle immagini è stata utilizzata per effettuare il training dell'algoritmo mentre le rimanenti sono state utilizzate per l'attività di testing vero e proprio. In questo studio è stato adottato un metodo appartenente a Farid [18] che ideò un modello statistico ad alto livello per discriminare le immagini naturali da quelle innaturali. Di seguito verranno riportati alcuni dei risultati dei test ottenuti dalla ricerca considerata sia sfruttando le *features di Farid* sia quelle della ricerca considerata, suddivisi per tipologia di alterazione.

Similarity Measure	*Description*
Sokal & Sneath Similarity Measure 1	$m_1 = \frac{a}{a+b} + \frac{a}{a+c} + \frac{d}{b+d} + \frac{d}{c+d}$
Sokal & Sneath Similarity Measure 2	$m_2 = \frac{ad}{\sqrt{(a+b)(a+c)(b+d)(c+d)}}$
Sokal & Sneath Similarity Measure 3	$m_3 = \frac{2(a+d)}{2(a+d)+b+c}$
Sokal & Sneath Similarity Measure 4	$m_4 = \frac{a}{a+2(b+c)}$
Sokal & Sneath Similarity Measure 5	$m_5 = \frac{a+d}{b+c}$
Kulczynski Similarity Measure 1	$m_6 = \frac{a}{b+c}$
Ochiai Similarity Measure	$m_7 = \sqrt{\left(\frac{a}{a+b}\right)\left(\frac{a}{a+c}\right)}$
Binary Lance and Williams Nonmetric Dissimilarity Measure	$m_8 = \frac{b+c}{2a+b+c}$
Pattern Difference	$m_9 = \frac{bc}{(a+b+c+d)^2}$
Binary Minimum Histogram Difference	$dm_{10} = \sum_{n=1}^{4} min(p_n^{\beta}, p_n^{\beta+1})$
Binary Absolute Histogram Difference	$dm_{11} = \sum_{n=1}^{4} \left\| p_n^{\beta} - p_n^{\beta+1} \right\|$
Binary Mutual Entropy	$dm_{12} = -\sum_{n=1}^{4} p_n^{\beta} \log p_n^{\beta+1}$
Binary Kullback Leibler Distance	$dm_{13} = -\sum_{n=1}^{4} p_n^{\beta} \log \frac{p_n^{\beta}}{p_n^{\beta+1}}$
Ojala Minimum Histogram Difference	$dm_{14} = \sum_{n=1}^{N} min(S_n^{\beta}, S_n^{\beta+1})$
Ojala Absolute Histogram Difference	$dm_{15} = \sum_{n=1}^{N} \left\| S_n^{\beta} - S_n^{\beta+1} \right\|$
Ojala Mutual Entropy	$dm_{16} = -\sum_{n=0}^{15} S_n^{\beta} \log S_n^{\beta+1}$
Ojala Kullback Leibler Distance	$dm_{17} = -\sum_{n=1}^{N} S_n^{\beta} \log \frac{S_n^{\beta}}{S_n^{\beta+1}}$

Figura 29: Binary Similarity Measures

Scaling-up	Method	False Positive	False Negative	Accurancy(%)
%50	BSM	2/100	0/100	99
	Farid	4/100	11/100	92,5
	Farid	5/100	11/100	92
%10	BSM	18/100	3/100	89,5
	Farid	4/100	17/100	89,5
%5	BSM	25/100	4/100	85,5
	Farid	4/100	14/100	91
	Farid	8/100	21/100	85,5
%1	BSM	32/100	8/100	80
	Farid	17/100	12/100	85,5

Tabella 1:Performance di un "attacco" di ridimensionamento di immagine

Nella Tabella 1 sono mostrati i risultati dei test che classificano se un'immagine è originale o alterata tra quelle che erano state sottoposte a diverse percentuali di ridimensionamento.

La Tabella 2 invece mostra i risultati delle Performance dei due metodi su immagini sottoposte a diversi gradi di rotazione.

Rotation	Method	False Positive	False Negative	Accurancy(%)
%50	BSM	2/100	0/100	99
	Farid	4/100	11/100	92,5
%25	BSM	7/100	0/100	96,5
	Farid	5/100	11/100	92
%10	BSM	18/100	3/100	89,5
	Farid	4/100	17/100	89,5
%5	BSM	25/100	4/100	85,5
	Farid	4/100	14/100	91
%2	BSM	27/100	7/100	83
	Farid	8/100	21/100	85,5

Tabella 2: Performance di un "attacco" di rotazione dell'immagine

La Tabella 3 mostra i risultati corrispondenti alla modifica del gradi di luminosità.

Brightness Adjustment	Method	False Positive	False Negative	Accurancy(%)
%40	BSM	17/100	27/100	78
	Farid	60/100	28/100	58
%25	BSM	13/100	32/100	77,5
	Farid	61/100	26/100	56,5
%15	BSM	19/100	28/100	76,5
	Farid	67/100	27/100	53,5
%5	BSM	18/100	45/100	68,5
	Farid	59/100	39/100	51

Tabella 3: Performance di un "attacco" di regolazione della luminosità

Come mostrato dalle tabelle riportate i ricercatori hanno effettuato i test con più di un classificatore per ciascun tipo di alterazione di immagini e variando le impostazioni del grado di variazione applicato all'immagine.

Tuttavia si è dimostrato poco pratico utilizzare un classificatore specifico per ciascun tipo di impostazione, è stato scelto di creare un solo classificatore per tipo di alterazione che operi in un specifico range di valori.

Per testare questo classificatore è stato generato un gruppo di immagini ridimensionate a diverse percentuali.

Vediamo nelle Tabelle seguenti i risultati ottenuti.

Per testare un'immagine con un unico classificatore si è creato un set di immagini aggiungendo un egual numero di immagini ingrandite con scala del %50, %25, %10, %5 , scalate di dimensioni inferiori con percentuali del %50, %25, %10, %5, ruotate con gradazioni di 45°, 30°, 1 5°, 5°, con aumento di contrasto di scale 25, 15, 5 , luminosità modificata in scala di 15, 25 ,sfuocata con scala di 0.3, 0.5.

Nuovamente la metà delle immagini sono state usate come set di training e le rimanenti come test. In questo articolo[10] è stato denominato il classificatore di queste categorie come classificatore generico-generico.

Image Alteration Type	Method	False Positive	False Negative	Accurancy (%)
Ingrandimento	BSM	12/100	3/100	92,5
	Farid	6/100	17/100	88,5
Riduzione	BSM	29/100	13/100	79
	Farid	17/100	18/100	82,5
Rotazione	BSM	13/100	45/100	71
	Farid	16/100	14/100	85
Aumento contrasto	BSM	1/100	48/100	75,5
	Farid	79/100	13/100	54
Regolazione luminosità	BSM	3/100	17/100	75,5
	Farid	76/100	12/100	53,5
Messa a fuoco	BSM	6/100	18/100	88
	Farid	80/100	4/100	58

Tabella 4: Performance di classificatori generici

Per rendere i risultati più realistici, sono stati indirizzati i test verso delle immagine “falsate”; queste immagini sono state truccate inserendo dei contenuti extra o rimpiazzando il contenuto originale. Per renderle il più simili al naturale possibile ed evitare qualunque sospetto, il contenuto inserito è stato ridimensionato, ruotato o aggiustato di luminosità prima di essere incollato nell'immagine.

Sono stati quindi presi due blocchi non manomessi e un solo blocco manomesso da ciascuna immagine (40 totali) e testati con i classificatori generici.

Riportiamo nella Tabella 5 i risultati di questo test.

Method	False Positive	False Negative	Accurancy (%)
BSM	9/40	2/20	81,67
Farid	40/40	0/20	33,3

Tabella 5: Performance di un generico classificatore per blocchi di immagini

Gli stessi blocchi sono poi stati sottoposti anche al classificatore generico-generico.

I risultati sono riportati in Tabella 6.

Method	False Positive	False Negative	Accurancy (%)
BSM	8/40	4/20	80
Farid	9/40	8/20	71,67

Tabella 6: Performance di un generico-generico classificatore per blocchi di immagini

Infine sono state selezionate 100 immagini da Internet che potevano facilmente essere manomesse. Sono state testate sia con un generico classificatore sia con un classificatore generico-generico.

Nelle tabelle 7 e 8 i risultati ottenuti.

Method	False Negative	Accurancy (%)
BSM	9/100	91
Farid	0/100	100

Tabella 7: Performance di un generico classificatore per blocchi di immagini catturate da Internet

Method	False Negative	Accurancy (%)
BSM	48/100	52
Farid	47/100	53

Tabella 8: Performance di un generico-generico classificatore per blocchi di immagini prese da Internet

I risultati riportati mostrano che i classificatori progettati sono in grado di discriminare un'immagine manomessa dalla sua originale con una ragionevole accuratezza.

Dal confronto con il metodo del Dott. Farid emerge che questo studio ha

ottenuto prestazioni migliori specialmente nelle alterazioni di messa a fuoco e regolazione della luminosità. D'altro canto però , mentre sono stati ottenuti buoni risultati ai livelli più forti di manipolazione, il metodo del Dott. Farid ottiene prestazioni migliori con livelli più piccoli di manipolazione. In conclusione questo studio ha mostrato che i due metodi possono essere definiti complementari. Di conseguenza è obbligatorio un uso misto dei modelli di analisi forense per avere un alto livello di accuratezza.

5.3 Rilevazione di alterazioni utilizzando tecniche di analisi avanzate

Nel corso di anni sono stati proposti diversi metodi per accertare l'autenticazione di un'immagine osservando le tracce di possibili operazioni effettuate sull'immagine.

Farid [23] suggerì una metodologia in cui venivano studiate le tracce di ridimensionamento nascoste in ogni porzione di un'immagine.
Gallagher [24] creò una tecnica di rilevamento del ridimensionamento in cui sfrutta la periodicità nelle immagini interpolate per ricercare tracce di modifica alla dimensione dell'immagine.
Ma gli studi [23] e [24] rilevano solo operazioni di ridimensionamento e rotazione nelle immagini falsate e questo non è sufficiente.
Nell'articolo [9] viene proposto un sistema per rilevare la rotazione, il ridimensionamento, l'aumento del contrasto e il livello degli istogrammi.
L'idea di rilevare il mapping dei valori dei pixel viene attribuita a Stamn e Liu[25].
Infatti il mapping del valore dei pixel lascia dietro di sé alcune tracce statistiche chiamate impronte intrinseche nell'istogramma dei valori dei pixel.
Rilevando queste impronte intrinseche si possono determinare le operazioni di mapping dei pixel fatte sull'immagine.

Ma un'impronta statistica non rileva le operazioni di rotazione e ridimensionamento, per cui non sarà efficace al 100% nell'individuare immagini falsificate. Ecco perché in questo articolo viene proposto un processo per la validazione delle immagini che combini diverse tecniche e che sia in grado di individuare le modifiche possibili su di una immagine per superare questi limiti.
Anche la combinazione di diverse tecniche non supera un limite, quello relativo alla falsificazione chiamata copy-move.
Le limitazioni del copy-move sono dovute al fatto che il primo approccio (Farid) tiene conto solo dell'operazione di shifting delle regioni di un'immagine.
Nell'articolo di ricerca [9] viene fatta una analisi di come è possibile combinare i singoli algoritmi che rilevano specifiche alterazione di immagini per ottenere un algoritmo combinato in grado di rilevare tutte queste alterazioni.
Nelle immagini falsificate, le alterazioni possono essere sull'intera immagine (global) o solo su una porzione di essa (local). L'algoritmo che viene descritto è in grado di rilevarle entrambe.

5.3.1 Metodo per rilevare il ri-campionamento

Per generare una contraffazione convincente, come detto precedentemente, si ricorre spesso ad operazioni di ridimensionamento, rotazioni, oppure deformazioni di porzioni di immagine. Per esempio quando si crea un fotomontaggio con due persone, una delle due deve essere manipolata, ad esempio, per essere impostata con le stesse proporzioni dell'immagine in cui andrà aggiunta.
Per rilevare il ricampionamento nelle immagini digitali vengono usati gli algoritmi descritti in [24] e [25]; gli step di questo metodo vengono riportati in Figura 30.
Nella fase di Preprocessing, l'immagine in input viene dapprima convertita nello spazio colore YcbCr in cui Y rappresenta le componenti luma dell'immagine e Cb ,Cr rappresentano le componenti di crominanza.

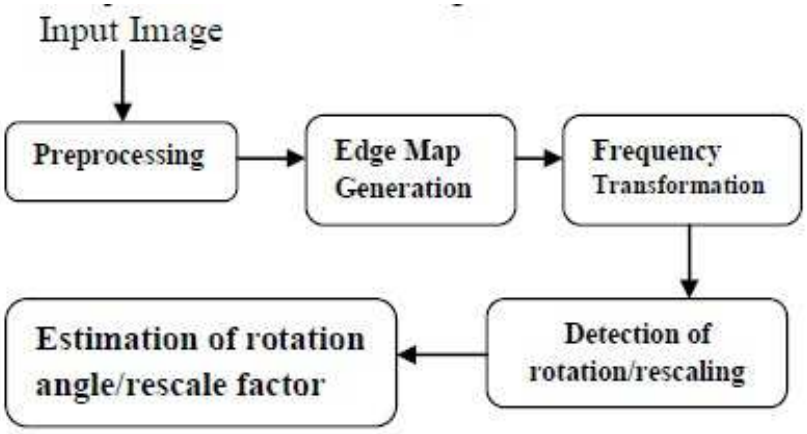


Figura 30: Step nel metodo di rilevamento del ri-campionamento

Il simbolo Y' serve per distinguere il luma dalla luminanza (Y), significa che l'intensità della luce non è codificata in base ai colori RGB primari.

Y'CbCr non è uno spazio colore assoluto, ma è un modo di codificare l'informazione RGB e i colori realmente visualizzati dipendono dai coloranti usati dal mezzo di visualizzazione.

La Edge Map Generation dell'immagine in input viene realizzata piegando la componente della luminanza (Y) dell'immagine di input con 3*3 operatori Laplacian.

Per calcolare la Frequency Transformation (DFT -Dimensional Frequency Transformation) ci sono due metodi: DA (DFT + Averaging) e AD (Averaging +DFT).

Nel metodo DA, per avere lo spettro orizzontale viene calcolata per ogni riga della edge map la magnitudine della DFT, e poi viene fatta la media per tutte le righe [26].

Nel metodo AD, viene calcolata la media di tutte righe della Edge Map per formare una riga orizzontale e poi viene calcolata la magnitudine della DFT per ottenere lo spettro di frequenza orizzontale.

Seguono a queste fasi quella di rilevamento e di stima dell'angolo di

rotazione;senza entrare nel dettaglio vengono riportate qui di seguito la formula che stima l'angolo di rotazione (Figura 31) e il fattore di ridimensionamento della formula (Figura 32).

$$f_{root1} = \begin{cases} 1-\cos\Theta, & 0° < \Theta \le 60° \\ \cos\Theta, & 60° < \Theta < 90° \end{cases}$$

And

$$f_{root2} = \begin{cases} \sin\Theta, & 0° < \Theta \le 30° \\ 1-\sin\Theta, & 30° < \Theta < 90° \end{cases}$$

Figura 31: Formula che stima l'angolo di rotazione. froot1 e froot2 sono i picchi di frequenza dovuti alla rotazione

$$f(res) = (1/R) - 1,\ R < 1$$

Figura 32: Fattore di ridimensionamento(R) e f(res) è il picco di frequenza indotto dovuto alla rotazione

5.3.2 Rilevamento di rotazioni e ridimensionamenti consecutivi

Sia la rotazione che il ridimensionamento sono spesso combinati nella maggior parte delle immagini falsificate.

Le quattro possibilità di combinazioni sono :DOUBLE ZOOMING (DZ), ROTATION ZOOMING (RZ), ZOOMING ROTATION (ZR) e DOUBLE ROTATION (DR).
In tutte queste operazioni consecutive i picchi indotti dalla prima operazione non appaiono mentre appaiono nei grafici i picchi dovuti alla seconda operazione. In alcuni casi i picchi appaiono a frequenze composte proprio a causa della combinazione di queste operazioni.

5.3.3 Rilevamento dell'aumento di contrasto

Il metodo per individuare l'aumento di contrasto nelle immagini, sia esso globale o locale, viene anche chiamato Intrinsic Fingerprint Detection Technique.
Nella Figura 33 vengono mostrati gli step necessari ad individuare l'aumento del contrasto nelle immagini.
Prima di tutto viene scelta l'immagine test che può essere a colori oppure in scala di grigi.
Se la scelta ricade su di una immagine RGB, vengono dapprima separate le componenti Red, Green e Blue e viene calcolato l'istogramma del valore dei pixel per tutte le componenti.
Infine viene calcolata la magnitudine del DFT (Dimensional Frequency Transformation) dell'istogramma.
La magnitudine ottenuta viene poi messa nel grafico con la frequenza per ottenere il grafico della frequenza.
Punti di zero o picchi improvvisi presenti nel grafico si riferiscono alle Intrinsic Fingerprints e se sono presenti allora si può dire che l'immagine è stata alterata con aumento del contrasto.

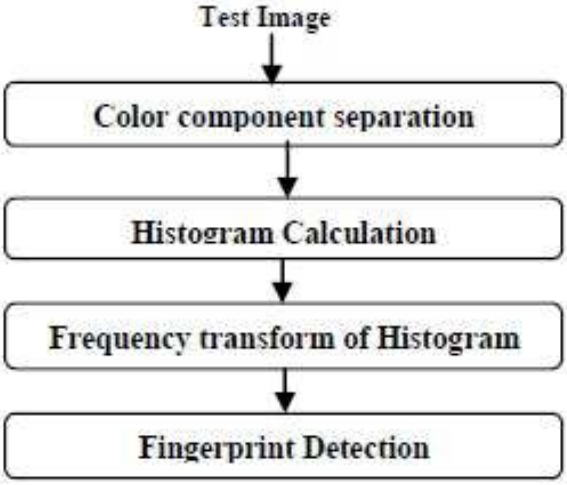


Figura 33: Fasi per individuare l'aumento di contrasto nelle immagini

5.3.4 Rilevamento equalizzazione dell'istogramma

L'Istogramma di un'immagine è un tipo di istogramma che rappresenta in modo grafico la variazione tonale di un'immagine digitale. Traccia il numero di pixel per ogni variazione tonale. L'asse orizzontale del grafico rappresenta le variazioni tonali, mentre l'asse verticale rappresenta il numero di pixel di quel particolare tono (Figura 34).

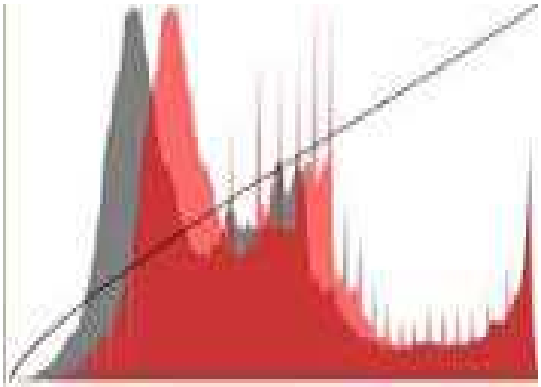


Figura 34: Esempio di un istogramma di immagine

L'Equalizzazione di un Istogramma invece è una trasformazione matematica che consente di ottenere un'immagine con un istogramma di distribuzione dei grigi più uniforme (Figura 35).

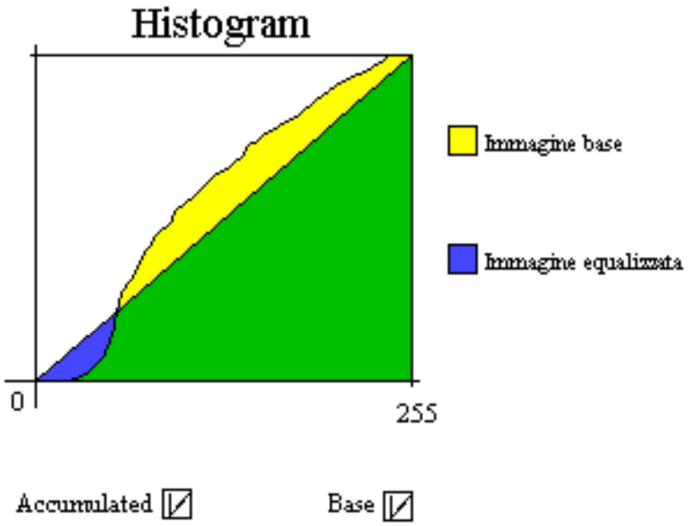


Figura 35: Esempio di equalizzazione di un istogramma di un'immagine

In pratica anche l'equalizzazione di un istogramma è una forma di aumento del contrasto. Infatti per il rilevamento dell'equalizzazione di un istogramma vengono utilizzati gli stessi metodi che si usano per il rilevamento delle Intrinsic Fingerprint.

5.4 Individuazione di immagini sottoposte a Morphing

Rispetto al passato, il *Morphing* viene utilizzato molto al giorno d'oggi. Anche se l'effetto che ebbe inizialmente fu quello di novità, nell'epoca attuale i *Morphing* sono spesso creati in modo da essere nascosti, invisibili agli occhi. Sebbene si tenti di rendere queste manipolazioni impercettibili all'occhio umano, esse si ripercuotono sulle statistiche dell'immagine che ha subito alterazione, ecco perché uno dei metodi possibili per individuare queste falsificazioni è l'individuazione di pixel alterati.

Il procedimento di rilevazione di Image Morphing può includere diverse tecniche. Queste tecniche includono, ma non sono limitate solo a questo, la

valutazione di problemi alla struttura dell'immagine come la scoperta di artefatti dovuti alla manipolazione o alla degradazione, l'analisi dei metadati e l'indicazione della provenienza dell'immagine. Analizzando lo studio [11] sarà presentato uno dei metodi per individuare il Morphing.

5.4.1 Demosaicizzazione e Interpolazione

Per permettere alla fotocamera di restituire un'immagine a colori è necessario registrare le diverse lunghezze d'onda presenti nella scena che si cattura,partendo da un'immagine RAW. Come visto nel paragrafo 4.1 il sensore da solo non è in grado di svolgere questo compito, ovvero di discriminare i colori; è quindi necessario eseguire una sorta di “specializzazione cromatica” dei pixel in modo che possano misurare distintamente le componenti cromatiche primarie che compongono un colore:Rosso, Verde e Blue. Questo si ottiene ponendo davanti ad ogni pixel un filtro colorato: il più utilizzato è il Filtro di Bayer (Figura 36).

Il Filtro di Bayer è composto da una matrice di punti colorati della stessa dimensione del sensore e con una disposizione ben precisa. Il rapporto è di 2 punti ogni punto rosso o blu, perché l'occhio umano è più sensibile al colore verde. Quindi la luce attraversa il filtro, colpisce il sensore ed esso registra il valore di luminosità di un solo colore. Se eliminassimo il Filtro di Bayer, il sensore registrerebbe immagini in bianco e nero.

In questo modo la scena ripresa verrà scomposta in pixel, ognuno dei quali fornirà l'intensità luminosa di una sola componente di colore.

Questo però non basta per ottenere l'immagine finale a colori (RGB), perché è necessario che per ogni pixel siano presenti tutte e tre le componenti di colore primarie. Per calcolare il valore dei canali mancanti per ogni pixel subentra la funzione di Demosaicizzazione che utilizza tecniche di interpolazione. La tecnica di interpolazione più semplice è la “nearest neighbor”, che ripete il valore del pixel più vicino.

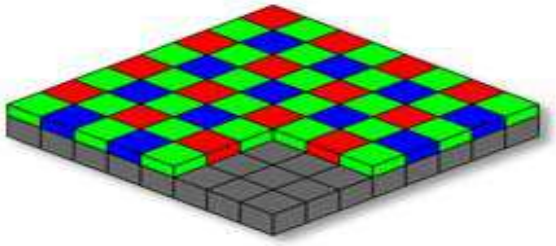


Figura 36: Matrice di Bayer usata sui singoli pixel del sensore

Una seconda tecnica è l'interpolazione bilineare che consente di rilevare i valori mancanti di canali di un punto, partendo dai punti adiacenti.
L'interpolazione è un processo che sulla base di curve e modelli matematici complicati, genera i pixel mancanti in un 'immagine. I processi di interpolazione più diffusi sono:

- **Bicubica**: Questa tecnica ricalcola ogni pixel utilizzando un campo di 4x4 pixel adiacenti; in questo modo lo strumento in uso verifica 16 pixel e calcola un valore medio di colore per quello nuovo. L'aspetto negativo è che spesso le immagini mostrano un alone in prossimità dei contorni.

- **Bilineare:** agisce in modo analogo alla tecnica bicubica ma utilizza un algoritmo che si basa su un'area di 2x2 pixel.

5.4.2 Individuazione di Image Morphing localizzando Pixel Alterati con Algoritmo di Demosaicizzazione

Ghatol, Paigude e Shirke [11] esplorano il processo di interpolazione CFA per determinare la correlazione tra la struttura presente in ogni banda di colore, che può essere utilizzata per la classificazione delle immagini.

L'assunzione principale è che l'algoritmo di interpolazione e la progettazione del pattern CFA di ogni produttore di fotocamere digitali sono gli uni differenti dagli altri e quindi risultano correlazioni tra le strutture distinguibili nell'immagine catturata, introducendo dei pattern periodici nel segnale dell'immagine.

Il Flow Diagram della tecnica proposta per il Photo Morphing Detection nello studio[11] è riportato in Figura 37.

Il primo passo è quello della scelta di immagini catturate da una fotocamera digitale o da un computer.

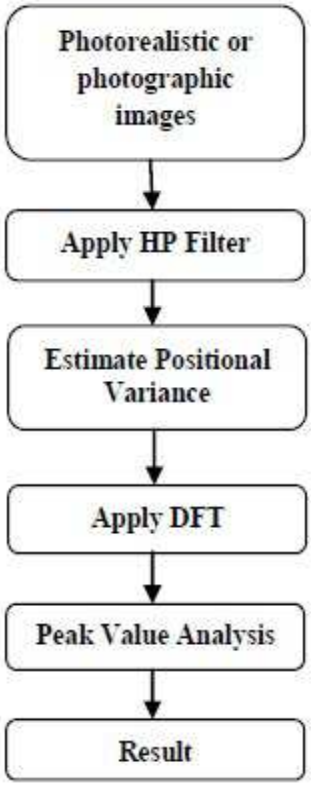


Figura 37: Flow Diagram for Photo Morphing Detection

Dopo questo passaggio viene calcolata la stima della varianza di ciascuna diagonale utilizzando un metodo chiamato Maximum Likelihood Estimation (MLE). Combinando i valori dei pixel adiacenti, viene generato il valore di un pixel interpolato. La varianza viene condizionata dal peso dei pixel adiacenti che produce un valore di pixel interpolato.

Questo forma il modello delle varianze che può essere rilevato e viene quindi utilizzato come idea di base per individuare la demosaicizzazione.

Per trovare la periodicità viene poi calcolato il DFT.

Un picco di frequenza relativamente alto indica che l'immagine non è morphed e si tratta di una caratteristica della demosaicizzazione.

6. Software per la rilevazione di alterazioni di immagini in commercio

In questo capitolo vengono introdotti alcuni dei Software sviluppati e commercializzati per l'individuazione e autenticazione di immagini digitali.
L'autenticazione forense di immagini è l'applicazione delle competenze scientifiche alle immagini con l'obiettivo di distinguere,secondo alcuni criteri, se l'immagine o il video in questione è un'accurata rappresentazione dei dati originali[27].

6.1 Fotoforensics

Fotoforensics [28] è un Web Service che consente di identificare immagini morphed o photoshopped utilizzando alcuni algoritmi in grado di individuare eventuali alterazioni eseguite sulle immagini.
La schermata inziale della pagina Web del servizio è la seguente (Figura 38):

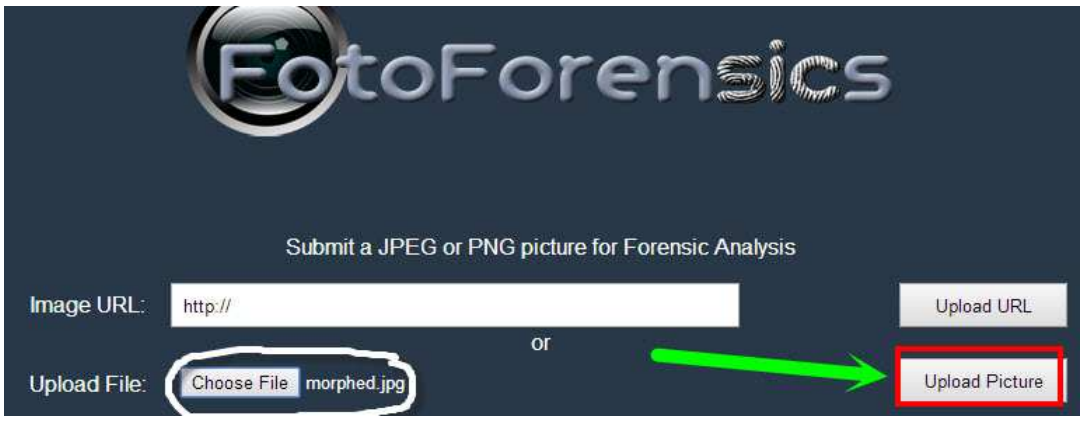


Figura 38: Home page FotoForensics

Si esegue prima di tutto l'upload dell'immagine e dopo alcuni secondi di elaborazione vengono mostrate due immagini: una è l'originale e l'altra è l'immagine analizzata (Figura 39).

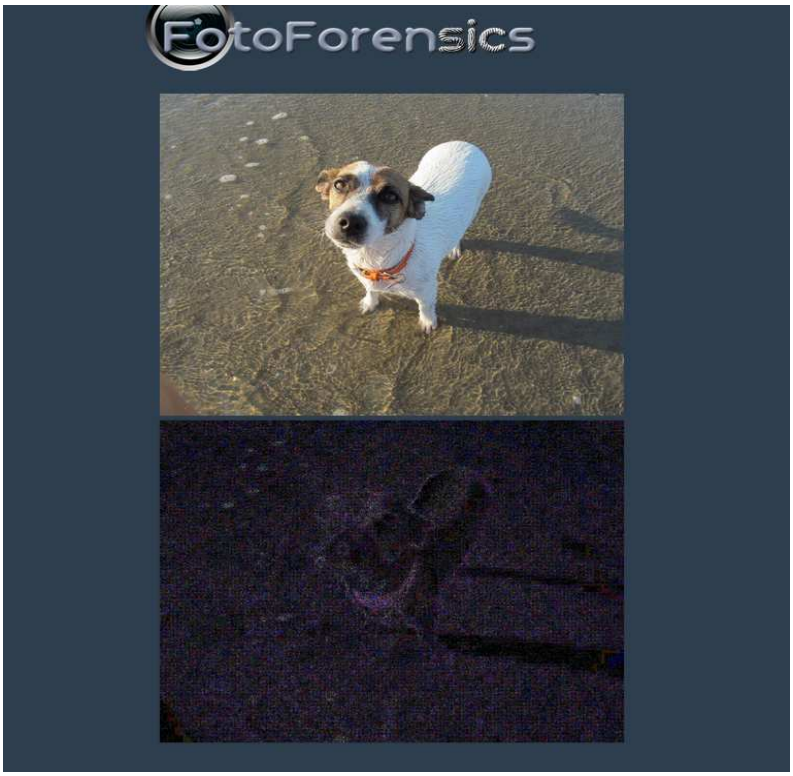


Figura 39:Esempio di immagine analizzata

Come vediamo nella Figura 40, il Software ci fornisce 4 tipi di informazioni utili per capire se l'immagine caricata è stata sottoposta a Morphing o ritoccata con Adobe Photoshop.

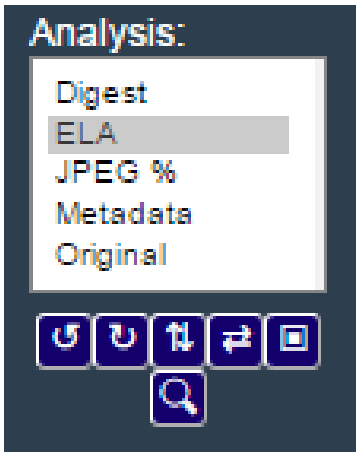


Figura 40: Informazioni restituite.

ELA significa Errore Level Analysis, ovvero mostra gli errori di livello dell'immagine. Se l'immagine sottoposta a verifica è modificata o morphed allora vengono mostrati alcuni colori nell'analisi dell'immagine. Come si vede infatti nella Figura 39 compaiono alcune sfumature colorate, indicazione (corretta) che l'immagine è stata alterata.

JPEG (%) individua invece la percentuale dell'Image Morphing. Mostra la qualità dell'immagine al momento dell'ultimo salvataggio. Se la percentuale di qualità risulta diminuita allora l'immagine è stata sicuramente modificata (Figura 41).

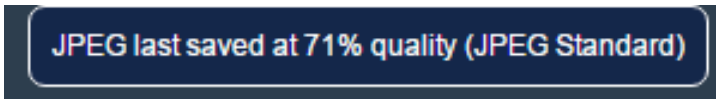
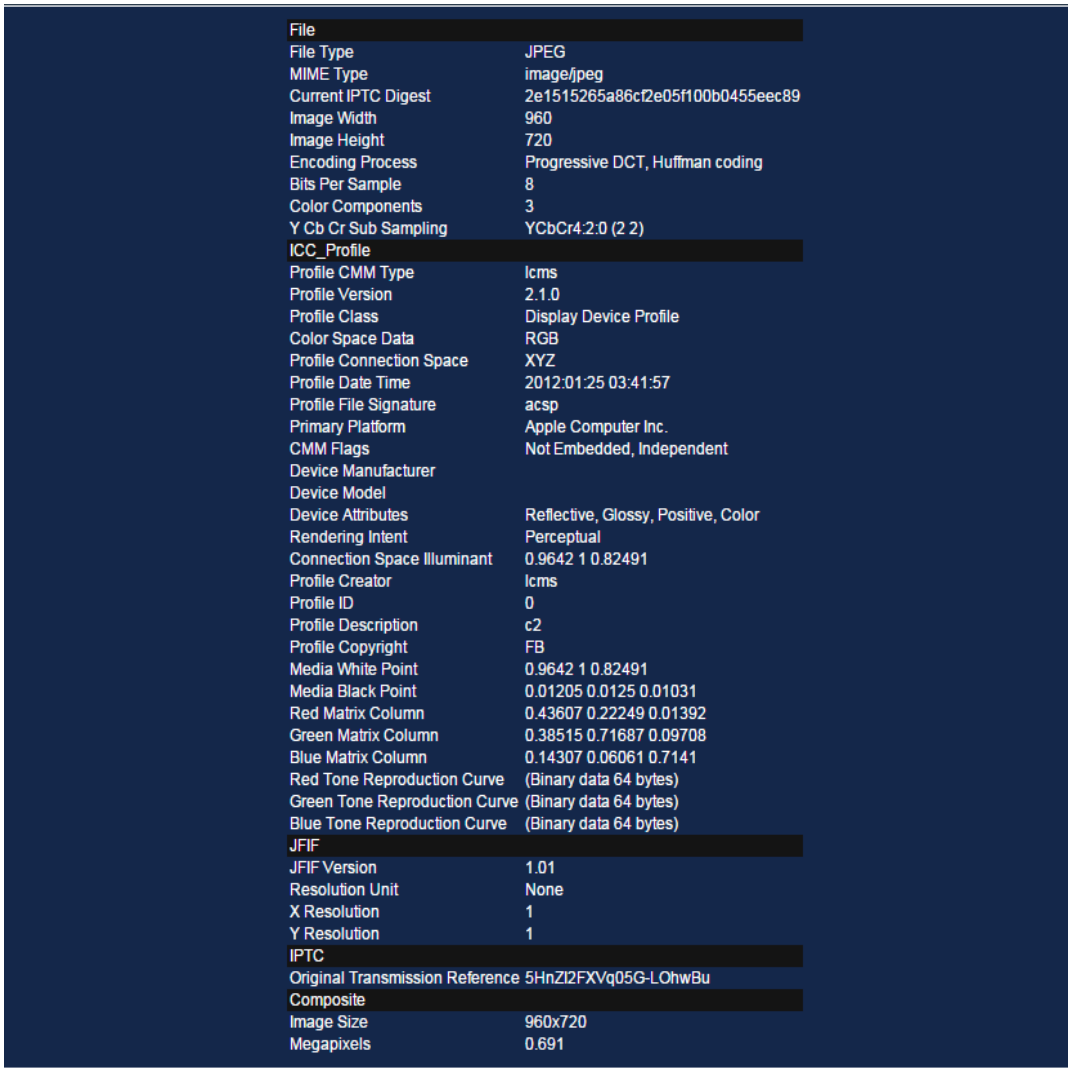


Figura 41: Esito JPEG % dell'immagine test

Sebbene molti utenti siano in grado di eliminare i MetaData dalle immagini, rimangono sempre alcune informazioni nella sezione dedicata.

METADATA è la funzione che visualizza le informazioni disponibili sulla foto quali ad esempio la data di creazione, la data dell'ultima modifica e quale

macchina fotografica è stata utilizzata (Figura 42).



File	
File Type	JPEG
MIME Type	image/jpeg
Current IPTC Digest	2e1515265a86cf2e05f100b0455eec89
Image Width	960
Image Height	720
Encoding Process	Progressive DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)
ICC_Profile	
Profile CMM Type	lcms
Profile Version	2.1.0
Profile Class	Display Device Profile
Color Space Data	RGB
Profile Connection Space	XYZ
Profile Date Time	2012:01:25 03:41:57
Profile File Signature	acsp
Primary Platform	Apple Computer Inc.
CMM Flags	Not Embedded, Independent
Device Manufacturer	
Device Model	
Device Attributes	Reflective, Glossy, Positive, Color
Rendering Intent	Perceptual
Connection Space Illuminant	0.9642 1 0.82491
Profile Creator	lcms
Profile ID	0
Profile Description	c2
Profile Copyright	FB
Media White Point	0.9642 1 0.82491
Media Black Point	0.01205 0.0125 0.01031
Red Matrix Column	0.43607 0.22249 0.01392
Green Matrix Column	0.38515 0.71687 0.09708
Blue Matrix Column	0.14307 0.06061 0.7141
Red Tone Reproduction Curve	(Binary data 64 bytes)
Green Tone Reproduction Curve	(Binary data 64 bytes)
Blue Tone Reproduction Curve	(Binary data 64 bytes)
JFIF	
JFIF Version	1.01
Resolution Unit	None
X Resolution	1
Y Resolution	1
IPTC	
Original Transmission Reference	5HnZI2FXVq05G-LOhwBu
Composite	
Image Size	960x720
Megapixels	0.691

Figura 42: Metadata immagine test

ORIGINAL è la sezione dove viene mostrata l'immagine test al momento dell'upload sul sito.

6.2 Image Edited?

Image Edited [29] è un altro tool molto utile nell'individuazione di immagini ritoccate.

Questo Web Service a differenza di Fotoforensics fornisce all'utente una risposta diretta ad una ipotetica domanda “L'immagine è stata modificata?” rendendolo quindi facilmente comprensibile da tutti, come è intuibile dalla pagina Home (Figura 43) .

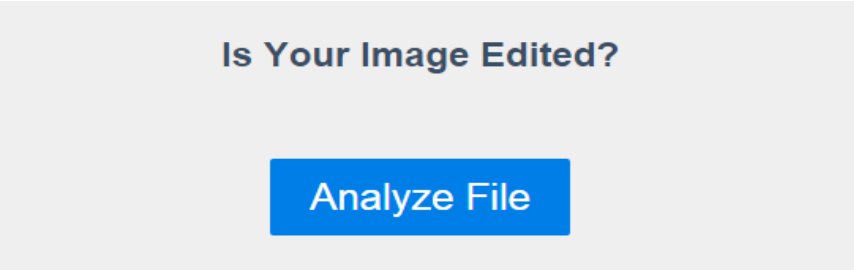


Figura 43: Home page

Ad esempio, se viene fatto l'upload di una foto completamente Photoshopped, si ottiene la risposta “Yes” e alcune importanti informazioni come i MetaData e gli EXIF data. Inoltre è in grado di capire con quale Software sono state fatte le modifiche all'immagine. Come si vede infatti dalla Figura 44, l'immagine caricata è stata alterata utilizzando Adobe Photoshop CC.

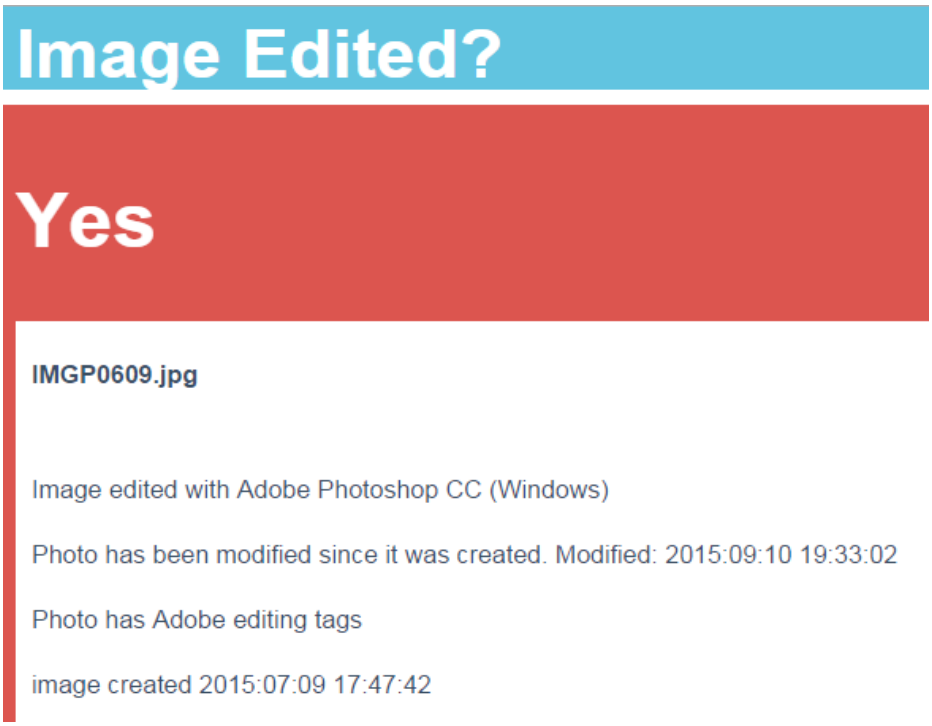


Figura 44: esito analisi immagine test

Un ulteriore funzione disponibile è quella di fornire, in caso, l'identificazione di un'immagine presa da Facebook (Figura 45).

Figura 45: Esito in caso di foto scaricata da Facebook

6.3 Fotoforensics vs Image Edited

In questo paragrafo vengono riportati i risultati di alcuni test eseguiti sui Software Fotoforensics e Image Edited per verificare il grado di accuratezza di entrambi i software a fronte di immagini alterate e non.

Test 1

Il primo test eseguito è stato fatto scegliendo una delle immagini utilizzate proprio in questa tesi come esempio di immagine alterata, la Figura 16.
L'esito restituito dai Software è il seguente:

Figura 46: Test1 - Esito Fotoforensics JPEG%

Figura 47: Test 1 - Esito Image Edited?

Risultati : Mentre la percentuale JPEG della qualità dell'immagine al 62% restituita da Fotoforensics permette di capire che questa immagine è stata alterata, Image Edited non è in grado (“Can't tell”) di fornire una risposta utile ai fini dell'autenticazione dell'immagine.

Test 2

Il secondo test è stato eseguito utilizzando una delle immagini proposte tra i casi di contraffazione famosi nel Paragrafo 4.3, la copertina del Time del 1994 (Figura 24).
Di seguito sono riportate le risposte dei Software a confronto:

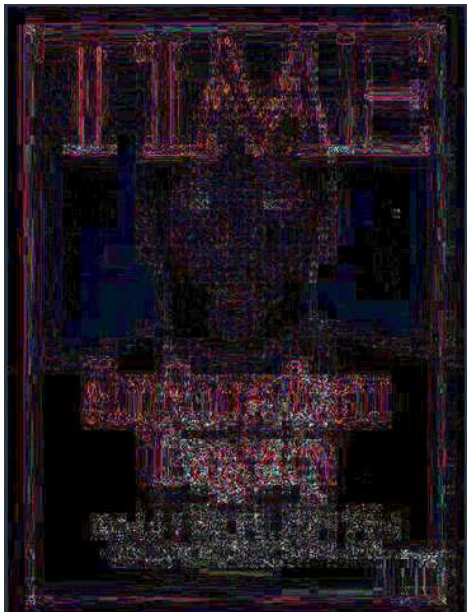


Figura 48: Test2 - Esito Fotoforensics ELA

Figura 49: Test2 - Esito Image Edited?

Risultati : In questo caso entrambi i Software hanno rilevato la presenza di alterazioni nell'immagine. Fotoforensics restituisce un'immagine analizzata che evidenzia con tratti colorati i punti che potrebbero avere subito variazioni (ELA), mentre Image Edited conferma in modo più semplificato che l'immagine non è autentica.

Test 3

Verifichiamo adesso il comportamento dei due Software con un'immagine che non ha subito alterazioni (Figura 49).

Figura 49: Immagine test non modificata

I Software hanno restituito i seguenti esiti:

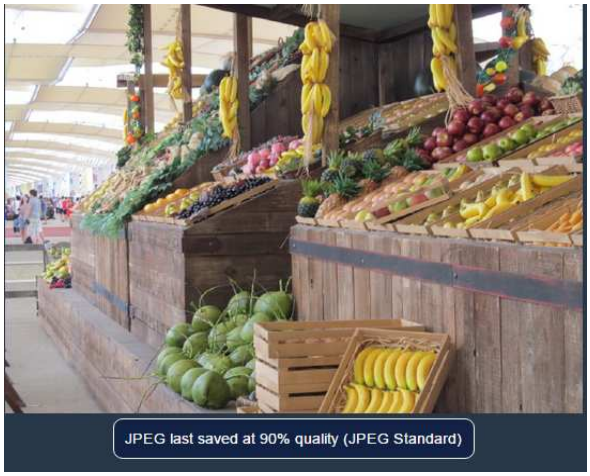


Figura 50: Test3 – Esito JPEG% Fotoforensics

Figura 51: Test3 - Esito Image Edited

Risultati : In questo test Fotoforensics ci restituisce una percentuale di qualità dell'immagine al 90%, ovvero che l'immagine è autentica, mentre Image Edited anche in questo caso non rileva elementi sufficienti per fornire all'utente una risposta certa sull'originalità dell'immagine.

Test 4

Infine cofrontiamo gli esitit restituiti da questi due Software in presenza di Morphing.
I campioni che utilizziamo sono le immagini dei due volti esempio del paragrafo 2.1, uno dei quali è un'immagine originale (Figura 52) e l'altro (Figura 53) è un volto ottenuto dal Morphing tra l'immagine in Figura 52 ed un altra.

Figura 52: Immagine originale

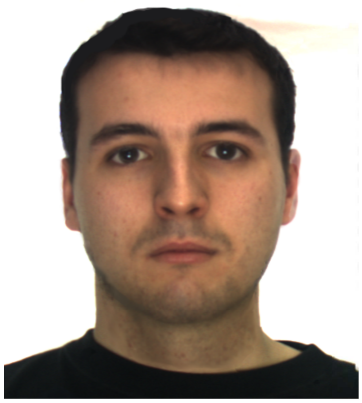


Figura 53: Immagine Morphed

a) L'analisi dell'immagine originale (Figura 52) da parte dei Software ha restituito i seguenti esiti :

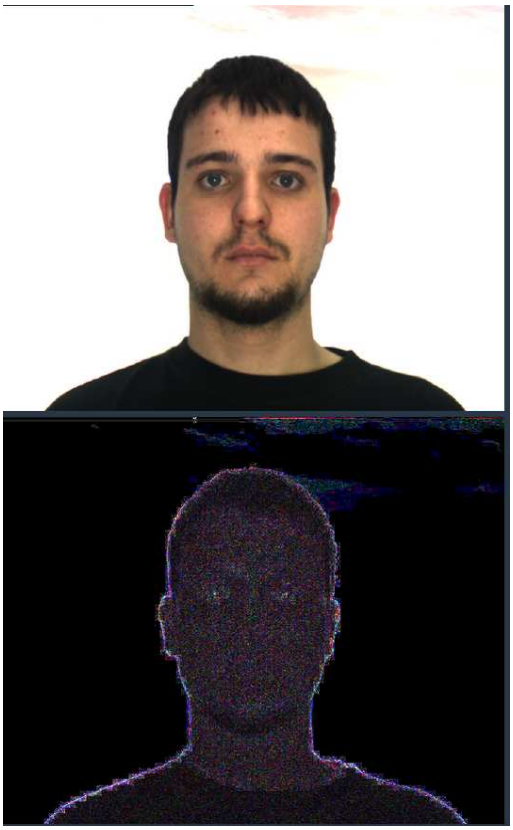


Figura 54: Test4a - ELA Fotoforensics

Figura 55: Test4a - Risposta di ImageEdited?

Risultati: In questo caso gli ELA di Fotoforensics hanno indicato che l'immagine è originale, diversamente da Image Edited? che fornisce una risposta incerta.

b) Infine vediamo i test eseguiti sull'immagine sottoposta a Morphing (Figura 53):

Figura 56: Test4b - ELA Fotoforensics

Figura 57: Test4b Risposta di ImageEdited?

Risultati: nessuno dei due software è stato in grado di rilevare il Morphing in questa immagine. Fotoforensics ha classificato l'immagine come originale mentre Image Edited? ha fornito la stessa risposta del punto (a), ovvero non ha dati sufficienti per classificare l'immagine.

Quest'ultimo test dimostra che i Software di individuazione di alterazioni di immagini, in particolare in presenza di Morphing, hanno un livello di precisione piuttosto limitato in quanto le variabili che possono fare attribuire ad una immagini l'etichetta di “falsificata” sono molteplici e non sempre facilmente rilevabili.

Ci sentiamo in ogni caso di affermare che, limitatamente ai risultati dei test svolti in questa tesi, il Software Fotoforensics presenta un livello di precisione nell'individuazione di immagini modificate più alto rispetto al concorrente Image Edited?.

6.4 PhotoPolice

PhotoPolice [30] è la nuova App proposta nel Mac Apple Store che permette di individuare eventuali modifiche apportate ad un'immagine.
A seguito della scansione di un'immagine da analizzare, l'App mostra un'immagine aggiornata che ne evidenzia i tratti sospetti. (Figura 46).

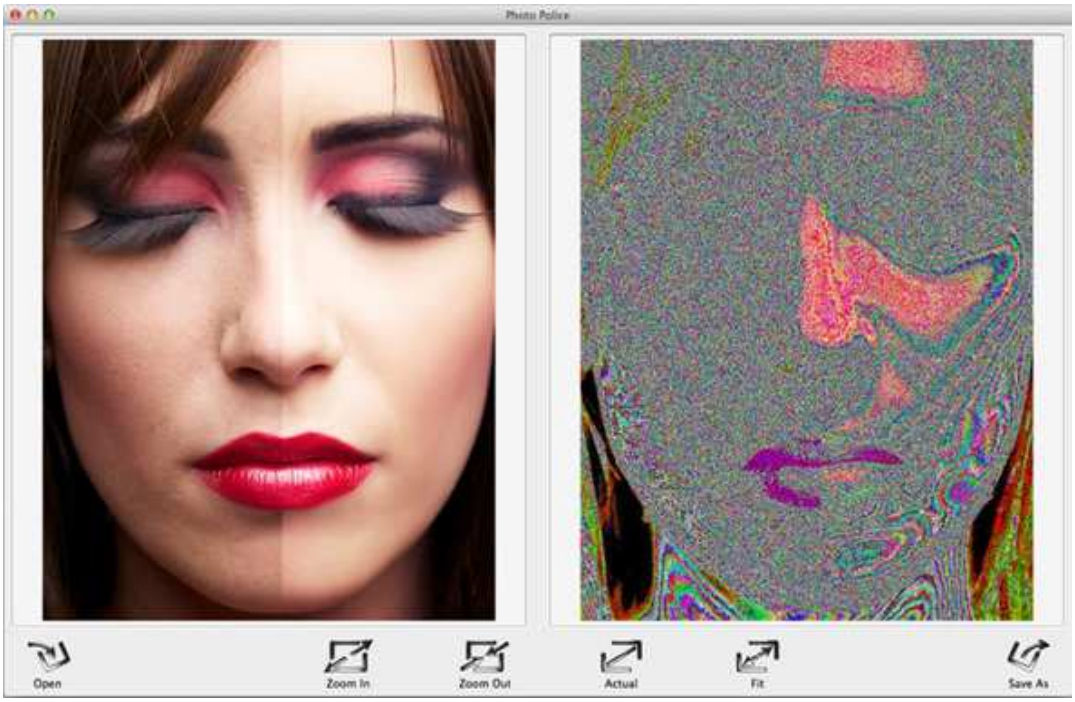


Figura 58: Esempio di analisi di un'immagini di PhotoPolice

Il processo di analisi dell'Applicazione include la rilevazione delle seguenti tecniche:

- La tecnica di sfocatura utilizzata per nascondere le imperfezioni del viso, esempio l'acne
- Le modifica di singole regioni di una fotocamera
- Le sezioni nascoste di una fotocamera
- Tutti i dati dei low-pixel

Alcuni critici hanno notato che questa applicazione non è particolarmente precisa nell'individuare immagini Photoshopped ed è inoltre limitato ad un unico formato di immagine (.JPEG) che, considerando la moltitudine di formati disponibili, limita molto l'utente.

Conclusioni

L' obiettivo di questa tesi è stato quello di studiare le tecniche di rilevamento di alterazioni digitali nelle immagini, a fronte di un problema sempre più importante e tangibile come quello della contraffazione di immagini digitali a fini criminali.
Per poter comprendere queste tecniche sono stati approfonditi alcuni dei moltissimi argomenti inerenti le immagini digitali a partire dalla vera e propria formazione di una fotografia digitale, facendo alcuni cenni sulla tecnologia che consente l'acquisizione di una foto da parte delle macchine fotografiche. Abbiamo visto come quest'ultima fase lasci delle tracce sull'immagine utili allo scopo di individuare eventuali modifiche.
La tecnica di alterazione digitale sulla quale è stata focalizzata l'attenzione è il Morphing, che consente di creare un'immagine di un volto con componenti del viso di altre due persone in modo tale che, inserita questa immagine in un documento di identità di viaggio, i sistemi di riconoscimento ABC presenti nei terminali aeroportuali non siano in grado rilevare l'alterazione ma anzi, riscontrando tratti del volto della persona fisica nell'immagine, ne consentano il passaggio.
La ricerca di questa tesi si è quindi concentrata sugli algoritmi proposti per evitare queste situazioni di forte rischio per la sicurezza, che hanno il compito di smascherare un'immagine sottoposta a Morphing.
L'analisi di questi algoritmi ha portato alla luce il fatto che non è sufficiente un unico algoritmo per discriminare un'immagine autentica da una falsificata, ma è necessario combinare più metodi, ognuno specializzato nella ricerca di una o più alterazioni, per migliorare il livello di precisione durante il processo di verifica di un'immagine digitale.
A seguito dello studio di questi algoritmi mostra l'esistenza di una discreta possibilità di successo di riuscire ad ingannare i Sistemi di Sicurezza ABC, in concomitanza al fatto che un agente di sorveglianza non sarebbe in grado ad occhio nudo di rilevare alterazioni di questo livello.
Per terminare la panoramica sono stati illustrati anche i metodi più generali per individuare alcune delle forme più comuni di alterazione di immagini e alcuni dei

Software online presenti in commercio che svolgono questa funzione di verifica di immagini digitali.

Per fare una verifica diretta dell'accuratezza di due tra i Software mostrati sono state utilizzate cinque tipi di foto:due alterate e due originali e una Morphed.

I risultati ottenuti evidenziano che il livello di precisione nell'individuazione di immagini alterate è piuttosto vulnerabile. In particolare modo abbiamo dimostrato che i Software di rilevamento di alterazione digitali non individuano il Morphing di immagini, ma è necessaria l'implementazione di algoritmi specifici.

In conclusione l'autenticazione forense di immagini presenta ancora alcuni ostacoli e saranno necessari ulteriori studi per lo sviluppo di algoritmi con una buon livello di accuratezza .

Ringraziamenti

Vorrei ringraziare prima di tutti la Prof.ssa Annalisa Franco per la sua costante disponibilità, l'aiuto e le conoscenze che mi ha trasmesso, non solamente nello svolgimento di questa tesi ma anche nel mio percorso formativo.
Un particolare ringraziamento va soprattutto alla mia famiglia: a mia mamma, senza il cui sostegno ed esempio di costante determinazione e coraggio non avrei potuto conseguire questo importante traguardo, a mia sorella Sara, ai miei nonni Ivan e Graziella colonne portanti della mia vita, alle mie cugine Giulia, Giada e Giorgia per avermi spronata in ogni momento e ai miei zii tutti. Vorrei ringraziare anche chi purtroppo non può essere presente, mio padre Alessandro, la mia Nonna Bisa e miei nonni la cui presenza spirituale mi ha accompagnata in questo percorso e confortata nei momenti difficili.
Ringrazio il mio compagno Loris per avere percorso questo cammino al mio fianco ed essermi stato vicino in ogni momento incoraggiandomi.
Ringrazio inoltre i mie suoceri Oscar e Graziella, per l'immenso affetto e supporto che mi hanno dato in questi anni di formazione accademica,.
Grazie infine a tutti gli amici vicini e lontani.

Laura Castellani

Bibliografia e Sitografia

[1] M.Ferrara, A.Franco, D.Maltoni - “The Magic Passport”

[2] Galphade, M.N., Suresh Khule ,Sumit Sharma and Rohit Khose - “Photo Morphing Detection

[3] Sabihah Binti Shamsuddin, Siti Norasyikin Binti Mohd Razali and Nur Adila Binti Salehuddin - “Review of Image Mnorphing Methods and Techniques” (2012-2013)

[4] Martin Bichsel - “Automatic Interpolation and Recognition of Face Images by Morphing

[5] Ian Craw, David Tock and Alan Bennett - “Finding Face Features”

[6] M. Bichsel, A.P. Pentland - “Human Face Recognition”

[7] Lee S., Chwa K.-Y., Hahn J., Shin S. - “Image morphing using deformation techniques” - The Journal of Visualization and Computer Animation – 1996.

[8] S.Battiato,F. Galavan, M.Jerian, M.Salcuni - “Linee Guida per l'Autenticazione Forense di Immagini”

[9] M. Mahipati Patil, S.P. Rangdale ,S.A. Nalawade - “Digital Image Alteration Detection using Adavance Processing”, International Journal of Computer Application – 2015

[10] S. Bayram, I.Avcibas, B. Sankur, N.Memon - “Image Manipulation Detection with Binary Similarity Measures”

[11] N. P. Ghatol, R. Paigude, A. Shirke - “Image Morphing Detection by Locating Tampered Pixels with Demosaicing Alghoritms”, International Journal of Computer Applications –2013

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

[13] M. K. Johnson, H. Farid - “Exposing digital forgeries through chromatic aberration”.

[14] https://en.wikipedia.org/wiki/Digital_watermarking

[15] R. Ramanath, W.E. Snyder, Y. Yoo and M.S Drew - “Color image processing pipeline”, Signal Processing Magazine, IEEE Volume:22, Issue: 1, (2005).

[16] H. Farid - “Photo Tampering Throughout History”
http://www.fourandsix.com/photo-tampering-history/

[17] https://en.wikipedia.org/wiki/Bit_plane

[18] Farid, H. , S. Lyu -”Higher-Order Wavelet Statistics and their Application to Digital Forensics, IEEE Workshop on Statistical Analysis in Computer Vision, Madison, Winsconsin, 2003

[19] Neurotechnology Website - “http://www.neurotechnology.com/”

[20] Luxand Website - “http://www.luxand.com/”

[21] FRONTEX Website - “http://www.frontex.europa.eu/”

[22] A. M. Martinez and R. Benavente - “The AR face database”, Technical Report

[23]Farid H. - ” Image Forgery Detection”

[24]Gallagher - “Detection of linear cubic interpolation in JPEGcompressed images”

[25]Stamn MC, Liu KJ. - “Forensic detection of image manipulation using statistical fingerprints”

[26] S. Devi Mahalakshmi, K. Vijayalakshmi, S. Priyadharsini - “Digital image forgery detection and estimation by exploring basic image manipulations”. Digital Investigation.

[27]https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2008/index.htm/standards/2008_04_standards02.htm

[28] http://fotoforensics.com/

[29] http://imageedited.com/

[30] https://itunes.apple.com/it/app/photo-police/id486614091?mt=12

[31] http://www.photometadata.org/meta-resources-metadata-types-standards-exif